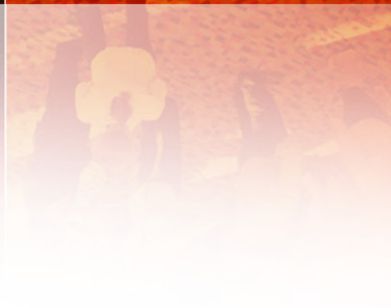# 12 SECURITY PREDICTIONS FOR 2012

TREND MICRO™

This time every year, I sit down with my research teams and we talk about what we think the coming year will hold in terms of threats to our customers. It's an important discussion that helps us not only share with you what we think you need to be prepared for, but also to help guide our direction as we continue to build products and services to help protect you from these threats.

This year, as we look ahead, we've come up with 12 predictions for 2012 that fall into four main categories:

- Big IT trends
- Mobile landscape
- Threat landscape
- Data leaks and breaches

In looking at these predictions, what we see in common are trends toward ever more sophisticated attackers and away from the PC-centric desktop. Our hope that new OSs make the world a safer place didn't work out. This means that our customers in 2012 will need to continue moving toward a more data-centric model for effective security and privacy as they embrace consumerization, virtualization, and the cloud. And we here at Trend Micro need to continue our work in these key areas to help enable our customers to meet and protect against these threat trends in 2012.

At Trend Micro, we are always working to understand not just the threats of today, but also the trends of tomorrow; it's in our company name. That helps us to help you better protect your data and assets.

I hope that you find this year's predictions to be not only interesting, but helpful in making 2012 a safe and secure year.

Raimund

Raimund Genes
CTO, Trend Micro

BIG
IT
TRENDS

1

Though many organizations are still uncomfortable with consumerization, security and data breach incidents in 2012 will force them to face BYOD-related challenges.

The Bring-Your-Own-Device (BYOD) Era is here to stay. As more and more corporate data is stored or accessed by devices that are not fully controlled by IT administrators, the likelihood of data loss incidents that are directly attributable to the use of improperly secured personal devices will rise. We will definitely see incidents of this nature in 2012.

The real challenge for data center owners will be dealing with the increasing complexities of securing physical, virtual, and cloud-based systems.

2

While attacks specifically targeting virtual machines (VMs) and cloud computing services remain a possibility, attackers will find no immediate need to resort to these because conventional attacks will remain effective in these new environments. Virtual and cloud platforms are just as easy to attack but more difficult to protect. The burden will thus fall on IT administrators who have to secure their company's critical data as they adopt these technologies. Patching a big array of virtualized servers is a challenge, allowing hackers to hijack servers, to fork traffic, and/or to steal data from vulnerable systems.

MOBILE LANDSCAPE

3 Smartphone and tablet platforms, especially *Android*, will suffer from more cybercriminal attacks.

As smartphone usage continues to grow worldwide, mobile platforms will become even more tempting cybercriminal targets. The *Android* platform, in particular, has become a favorite attack target due to its app distribution model, which makes it completely open to all parties. We believe this will continue in 2012 although other platforms will also come under fire.

4 Security vulnerabilities will be found in legitimate mobile apps, making data extraction easier for cybercriminals.

To date, mobile platform threats come in the form of malicious apps. Moving forward, we expect cybercriminals to go after legitimate apps as well. They will likely find either vulnerabilities or coding errors that can lead to user data theft or exposure. Compounding this further is the fact that very few app developers have a mature vulnerability handling and remediation process, which means the window of exposure for these flaws may be longer.

THREAT LANDSCAPE

5 Even though botnets will become smaller, they will grow in number, making effective law enforcement takedowns more difficult to realize.

Botnets, the traditional cybercrime tool, will evolve in response to actions taken by the security industry. The days of massive botnets may be over. These may be replaced by more, albeit smaller but more manageable, botnets. Smaller botnets will reduce risks to cybercriminals by ensuring that the loss of a single botnet will not be as keenly felt as before.

6

Hackers will eye nontraditional targets so flawed Internet-connected equipment, ranging from SCADA-controlled heavy industrial machinery to medical gadgets, will come under attack.

Attacks targeting supervisory control and data acquisition (SCADA) systems as well as other equipment accessible via networks will intensify in 2012 as certain threat actors go beyond stealing money and valuable data. STUXNET and other threats in 2011 highlighted how SCADA has become an active target. Proof-of-concept (POC) attacks against network-connected systems, including medical equipment, are expected to ensue.
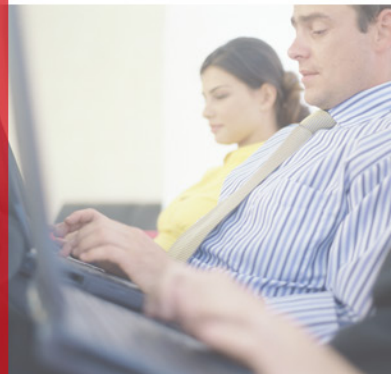
7

Cybercriminals will find more creative ways to hide from law enforcement.

Cybercriminals will increasingly try to profit by abusing legitimate online revenue sources such as online advertising. This will help them hide from the eyes of both law enforcement and antifraud watchdogs hired by banks and other financial agencies.

DATA
LEAKS AND
BREACHES

8 More hacker groups will pose a bigger threat to organizations that protect highly sensitive data.

Online groups such as Anonymous and LulzSec rose to prominence in 2011, targeting companies and individuals for various political reasons. These groups are likely to become even more motivated in 2012. They will become more skilled both at penetrating organizations and at avoiding detection by IT professionals and law enforcement agencies. Organizations will have to deal with this new threat and to increase their efforts to protect vital corporate information.

9 The new social networking generation will redefine "privacy."

Confidential user information is ending up online, thanks in large part to users themselves. The new generation of young social networkers have a different attitude toward protecting and sharing information. They are more likely to reveal personal data to other parties such as in social networking sites. They are also unlikely to take steps to keep information restricted to specific groups such as their friends. In a few years, privacy-conscious people will become the minority—an ideal prospect for attackers.

10

As social engineering becomes mainstream, SMBs will become easy targets.

To date, the craftiest social engineering ploys have been directed against large enterprises. However, cybercriminals are now so adept at social engineering that the effort to target companies individually–big or small–is becoming less costly. This and the greater volume of personal information available online will allow cybercriminals to launch more customized and fine-tuned attacks against small and medium-sized businesses (SMBs). As in previous attacks against SMBs, cybercriminals will continue focusing on gaining access to companies' online banking accounts.

11 New threat actors will use sophisticated cybercrime tools to achieve their own ends.

Targeted attacks will continue to grow in number in 2012. Cybercriminals will not be the only ones using these attacks, however. As the effectiveness of advanced persistent threats (APTs) becomes more obvious, other parties such as activist groups, corporations, and governments will find themselves using similar cybercrime tools and tactics to achieve their goals.

12 More high-profile data loss incidents via malware infection and hacking will occur in 2012.

High-profile attacks will continue to hit major organizations in 2012. Important and critical company data will be extracted through malware infection and hacking. As a result, significant data loss incidents will ensue, potentially affecting thousands of users and their personal information. These incidents can result in significant direct and indirect losses to concerned parties.

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years of experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products, and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com.**

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com

Securing Your Journey to the Cloud