SOPHOS

simple + secure

IT Security Year in Review: 2011

Top trends of 2011 and predictions for key developments in 2012

By **James Lyne**, Director of Technology Strategy

The year 2011 was characterized by highly visible cyber attacks and cybercriminals targeting new platforms, as business use of mobile devices accelerated. We witnessed governments placing a heavy focus on the importance of cyber security. And we saw a number of high-profile "hacktivist" groups, without the financial motives of previous years, make uncomfortable headlines for targeted companies.

Cyber attacks are becoming more professionalized with commercial tools shared among cybercriminals. These products and services simplify mass generation of new malicious code campaigns and exploits. The net result has been significant increases in the volume of malware and more infections. In the coming year, businesses will be challenged to manage these threats alongside new ways of accessing applications and data, like cloud services, which will see a resurgence of interest.

2011: Looking back at seven top trends

1. A throwback to hacktivism

Financial motives have driven the majority of malicious code and attacks for some time. This year saw an increase in hacktivist activity ranging from some very basic attacks to serious data breaches. The media widely covers distributed denial of service or SQL injection attacks, sometimes leading organizations to focus on mitigating hacktivist attacks rather than the basics. This distorts true security priorities.

2. Continued massive escalation in the volume of malicious code

SophosLabs now sees over 150,000 new malware samples every day, an increase of more than 60% since 2010. More and more, cybercriminals create and distribute malware generation engines and toolkits. And a significant portion of this malicious code features back doors, meaning detecting the payload of malware is increasingly difficult.

3. Mobile malware: just the beginning but still stuck in the 1990s

Some in the security industry have preached for years that mobile devices would become the next significant target, but nothing ever really happened. This began to change in 2011, with a greater volume of malicious code and attacks on key platforms, such as Android. At the moment these attacks are still somewhat simple, much like '90s PC malware. But it's a warning of what may come.

4. Control systems and critical national infrastructure

The bad guys have diversified their traditional targets and hackers have started to pay more attention to these systems. While the threats were perhaps over-hyped, there are real issues in this area and it's vital to keep these critical systems fully protected.

5. We got to talk to the bad guys

Cybercriminals in 2011 constantly tried to trick people into giving up information and clicking on links. We even saw examples of social engineering where cybercriminals called businesses by phone in order to extract information. Attacks via social media platforms, VOIP and other channels were also widespread.

6. High-profile targeted attacks

We saw a number of high-profile targeted attacks, including those against RSA and defense contractors. These high-profile attacks showed us a different class of attackers—the rumored "state sponsored" and corporate espionage hackers—as opposed to mainstream threats. In many cases, the attack techniques and capabilities are identical to traditional malware.

7. The basics still go wrong

Some unusually traditional threats like Morto demonstrated how basics like good password management are still a significant challenge to IT security. Infections from the browser, brought about by a failure to patch vulnerabilities in PDF, Flash or the browser itself, remained commonplace.

Some in the security industry have preached for years that mobile devices would become the next significant target, but nothing ever really happened. This began to change in 2011, with a greater volume of malicious code and attacks on key platforms, such as Android.

2012: The year ahead

1. Continued growth in malware spread by social media and the web

The mass malware generation techniques of 2011 will remain effective and we can expect them to continue in 2012. Cybercriminals will continue to launch attacks using new social media platforms and integrated apps.

2. Cybercriminals further diversify targets

Security really is about more than just Microsoft Windows. Over the past 18 months the bad guys have increased attacks on other platforms like Mac OS X. It's likely we'll continue to see more targeted attacks on other platforms in 2012 and 2013. You need better user education and controls to make sure other platforms don't present an easy back door for cybercriminals.

3. Mobile devices in the spotlight

We've learned many lessons from Microsoft, and the architecture of mobile devices is more robust as a result. But we've also seen a lack of progress on password security, patching and encryption. IT security professionals will need to deal with rapidly evolving mobile platforms, each with a unique set of risks. This could also mean the bad guys will focus on the ARM platform, given its widespread use in mobile.

4. New web and networking technologies force us to learn some lessons

Web technologies are undergoing interesting changes now, from add-ons like Flash or Silverlight to the funky new HTML5. These new technologies introduce some impressive new capabilities for rich web applications (for examples, see http://www.apple.com/html5/). But they could also introduce new attack vectors.

Many languages or environments provide more access to local computing power and resources to enhance the web experience, but could allow the bad guys to find new ways of stealing data. IPv6 (the replacement for the major protocol that drives our networks and the Internet) brings security challenges and benefits. Mass migration in 2012 to IPv6 is somewhat unlikely. But given the shrinking number of IP addresses remaining, we're likely to see an uptick in consideration of this issue.

5. Casual consumerization causes backsliding

More of us are trying to directly embrace consumerized devices in the workplace. However, the casual shift to use of these devices without appropriate controls will cause backsliding in security capabilities, opening up holes that have to be fixed. IT will once again struggle to deploy basic controls and reliable measures for the environment.

6. Trend of targeted attacks continues

Given the low cost of producing relatively high quality malware it's likely we'll see more targeted attacks in 2012. With rising awareness of cybercrime as a means of IP theft or intelligence gathering, these attacks will continue to be a priority issue for certain businesses and organizations.

More of us are trying to directly embrace consumerized devices in the workplace. However, the casual shift to use of these devices without appropriate controls will cause backsliding in security capabilities, opening up holes that have to be fixed.

7. Continued hacktivism and high-profile threats focusing on control systems

As we embed technology more and more into our lives and homes (e.g., initiatives like smart grid), we may see new attack vectors or privacy breaches opening up. These attacks won't be the largest block of threats, but will likely be high profile. We also have to consider the security of embedded systems in devices like cars, since cybercriminals are likely to continue to look beyond the traditional PC-based platform. We can count on cybercriminals to find creative ways to extort information or money.

8. Convenience technologies could become new vectors for fraud

In 2011 we saw interesting new examples of fraud, like some of the illicit activities conducted with BitCoin. We're eagerly waiting for the widespread availability of technologies like near field communication (NFC) in mobile devices. We'll be able to make easy payments and begin to transition away from cash and potentially credit cards. But expect cybercriminals to target these integrated platforms, as they hold all of your life and your money.

9. Cloud services back on the list

Cloud service adoption dropped off the agenda for many businesses given the challenging economic conditions and a host of unanswered questions. But many are now starting to use these services. That means more focus on securing data wherever it flows, rather than just protecting the device or the network. Cybercriminals will target cloud service providers as they grow more popular.

The road ahead

The big challenge for businesses in 2012 will be to keep their security capabilities from backsliding as they adopt new technologies and the cybercriminals expand their focus. As we continue to mobilize and access information in different ways and from more locations, security tools will need to keep up. For example, keeping users protected even when they are roaming outside the traditional VPN.

Keeping your devices healthy by identifying missing patches in areas commonly targeted by the bad guys will help significantly. You should evaluate your use of cloud services and consider how to protect data as it flows to a wider range of devices and partners. Technologies like file and folder encryption will aid cloud and new device adoption.

As we enter 2012, your focus should be on getting the basics covered in the new deployment models and devices you use. And you'll need to upgrade your organization's security tools to solve more of these problems.

James Lyne, Director of Technology Strategy  @jameslyne

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK

A Sophos Article 12.11v1.dNA

SOPHOS