Kaspersky Lab outlines key security trends in 2012; predicts core threats for 2013

MOSCOW, RUSSIA: Kaspersky Lab's experts have outlined key security trends of 2012 and presented their views on the core threats of 2013. The most notable predictions for the next year include the continued rise of targeted attacks, cyber-espionage, and nation-state cyber-attacks, the evolving role of hacktivism, the development of controversial "legal" surveillance tools, and the increase in cybercriminal attacks targeting cloud-based services.

Quick facts:

Important cyber security stories of 2012:
• Sophisticated malware targeting Mac OS X
• Explosive growth of Android threats
• Flame and Gauss as the sign of continued state-sponsored cyber warfare operations
• Notable password leaks from popular web services, such as LinkedIn and Dropbox
• Theft of Adobe certificates
• New 0-day vulnerabilities in Java and other popular software
• Attacks on network devices (namely DSL routers)
• DNSChanger shutdown
• Destructive Shamoon and Wiper malwares
• Madi cyber-espionage campaign

Predictions for 2013:

• Continued rise of targeted attacks
• Ongoing march of "hacktivism"
• More nation-state sponsored cyber-attacks
• Government-backed use of "legal" surveillance tools in cyberspace
• Attacks on cloud-based infrastructure
• Deterioration of digital privacy
• Continued problems with online trust and digital authorities
• Continued rise of Mac OS X malware and mobile malware
• Vulnerabilities and exploits continue to be key attack methods for cybercriminals
• Wide deployment of Ransomware and cryptoextortion malware

Key predictions overview:

Targeted attacks on businesses have only become a prevalent threat within the last two years. Kaspersky Lab expects the amount of targeted attacks, with the purpose of cyber-espionage, to continue in 2013 and beyond, becoming the most significant threat for businesses. Another trend that will likely impact companies and governments is the continued rise of "hacktivism" and its concomitant politically-motivated cyber-attacks.

State-sponsored cyber warfare will undoubtedly continue in 2013. In fact, during 2012, Kaspersky Lab discovered three new major malicious programmes that were used in cyber warfare operations: • Flame, • Gauss and • miniFlame.

While Flame was the largest and most sophisticated of the cyber-espionage programmes, its longevity was its most prominent characteristic. Being at least a five-year-old project, Flame was an example of a complex malicious programme that could exist undetected for an extended amount of time while collecting massive amounts of data and sensitive information from its victims.

Kaspersky Lab's experts expect more countries to develop their own cyber programmes for the purposes of cyber-espionage and cyber-sabotage. These attacks will affect not only government institutions, but also businesses and critical infrastructure facilities.

In 2012 an on-going debate took place on whether or not governments should develop and use specific surveillance software to monitor suspects in criminal investigations. Kaspersky Lab predicts that 2013 will build on this issue as governments create or purchase additional monitoring tools to enhance the surveillance of individuals, which will extend beyond wiretapping phones to enabling secret access to targeted mobile devices.

Government-backed surveillance tools in the cyber environment will most likely continue to evolve, as law-enforcement agencies try to stay one step ahead of cybercriminals. At the same time, controversial issues about civil liberties and consumer privacy associated with the tools will also continue to be raised.

Development of social networks, and, unfortunately, new threats that affect both consumers and businesses have drastically changed the perception of **online privacy** and trust. As consumers understand that a significant portion of their personal data is handed over to online services, the question is whether or not they trust them. Such confidence has already been shaken following the wake of major password leaks from some of the most popular web services such as Dropbox and LinkedIn. The value of personal data - for both cybercriminals and legitimate businesses - is destined to grow significantly in the near future.

2012 has been the year of the explosive growth of **mobile malware**, with cybercriminals' primary focus being the Android platform, as it was the most popular and widely used. In 2013 we are likely to see a new alarming trend - the use of vulnerabilities to extend "drive-by download" attacks on mobile devices. This means that personal and corporate data stored on smartphones and tablets will be targeted as frequently as it is targeted on traditional computers. For the same reasons (rising popularity), new sophisticated attacks will be performed against owners of Apple devices as well.

As vulnerabilities in mobile devices become an increasing threat for users, computer application and programme vulnerabilities will continue to be exploited on PCs. Kaspersky Lab named 2012 the year of Java vulnerabilities, and in 2013 Java will continue to be exploited by cybercriminals on a massive scale. However, although Java will continue to be a target for exploits, the importance of Adobe Flash and Adobe Reader as malware gateways will decrease as the latest versions include automated update systems for patching security vulnerabilities.

Says Costin Raiu, director of Global Research & Analysis Team at Kaspersky Lab: "In our previous reports we categorised 2011 as the year of explosive growth of new cyber threats. The most notable incidents of 2012 have been revealing and shaping the future of cyber security. We expect the next year to be packed with high-profile attacks on consumers, businesses and governments alike, and to see the first signs of notable attacks against the critical industrial infrastructure. The most notable trends of 2013 will be new example of cyber warfare operations, increasing targeted attacks on businesses and new, sophisticated mobile threats."

Read the Kaspersky Security Bulletin 2012: Top ten security stories and Security Forecast report.

Useful links: Kaspersky Security Bulletins

- Malware Evolution 2011
- IT Threat Evolution Q1 2012
- IT Threat Evolution Q2 2012
- IT Threat Evolution Q3 2012.