Cyberthreat forecast for 2012

Cyber weapons

2011 was the year that virtually all global players signaled their readiness to develop and deploy cyber weapons. The mass hysteria sparked by the discovery of the Stuxnet worm in 2010 led a number of states to start treating the use of cyber weapons against them as an act of war. However, by doing so, they are losing sight of some very important aspects of this type of threat. Take, for instance, Stuxnet. It was a unique phenomenon, designed exclusively for use at a specific time and at a specific place. And there was no readily available military solution to combat it. This is why we believe that the use of cyber weapons like Stuxnet will continue to be limited to isolated incidents. Their appearance will depend primarily on the relationship between specific states. Basically, to facilitate the creation of a cyber weapon of this standard there needs to be both an assailant and a victim. For the assailant, the problem needs to have become so serious that it can no longer be ignored, but the option of military action is out of the question. Analysis of current interstate conflicts can help predict similar incidents in the future.

This may well be true for cyber weapons such as Stuxnet, designed to carry out acts of sabotage. However other cyber weapons, used to destroy data at a given time, are likely to be more widely used. Programs such as kill switches, logic bombs etc., can be developed on a regular basis and deployed systematically. Moreover, the creation of these programs can be outsourced to private contractors used by the military, or law enforcement and intelligence agencies. In many cases the outsourcer will never know the identity of the actual client.

It is safe to say that the main cyber conflicts in 2012 will revolve around traditional confrontations: the US and Israel versus Iran, and the US and Western Europe versus China.

Mass targeted attacks

In 2011 we witnessed the emergence of new sources of malware and targeted cyber attacks. In the New Year we expect to see a significant increase in the number of new players and threats as well as high-profile incidents.

A far more effective detection process will also play a role in boosting the number of recorded attacks. An entirely separate field of the IT security industry has sprung up as a result of the problems associated with detecting and combating targeted attacks, and large companies are increasingly approaching small private firms for help in dealing with them. The growing competition in the market offering this kind of protection service will shed more light on incidents. As a result of the enhanced level of protection and the number of vendors offering help, the attackers will be forced to drastically change their methods.

At present many of the groups behind targeted attacks often don't even bother creating specialized malware and instead use someone else's ready-made programs. A good example is the Poison Ivy Trojan, originally created in Sweden but which has become a firm favorite with Chinese hackers. In contrast is the Duqu Trojan, a harbinger of things to come that can be modified to achieve specific aims and which makes use of dedicated command servers.

The effectiveness of traditional attack methods – the use of documents in email attachments that contain exploits for vulnerabilities – will gradually diminish. Attacks will increasingly be launched from browsers. Of course, the effectiveness of this approach will depend on the number of vulnerabilities found in popular software such as browsers, office applications and multimedia systems.

The range of companies and areas of the economy that will come under attack will expand. The majority of incidents currently affect companies and state organizations involved in arms manufacturing, financial operations, as well as hi-tech and scientific research activities. In 2012 companies in the natural resource extraction, energy, transport, food and pharmaceutical industries will be affected, as well as Internet services and information security companies. The geographic range of the attacks will increase considerably, spreading out beyond Western Europe and the US to affect countries in Eastern Europe, the Middle East and South-East Asia.

Mobile threats

Android

The unwanted attention that the Android platform has received from virus writers will intensify. In 2012 cybercriminals targeting mobile platforms will focus heavily on creating malware for Google Android. The dramatic growth in malicious programs for Android in the second half of 2011 saw Google's operating system rank first among mobile platforms in terms of the number of threats, and there is little to suggest that the virus writers will shift their focus in the near future.

We also expect an increase in attacks making use of vulnerabilities. 2012 will see cybercriminals making active use of a variety of exploits to spread malware as well as malicious programs containing exploits that can be used to escalate privileges and gain access to a device's operating system. Virtually all the attacks that made use of exploits in 2011 were attempts to elevate privileges to the operating system. However, in 2012 we are very likely to see the first attacks that will use exploits to infect the operating system itself. In other words, we'll see the first mobile drive-by-download attacks.

There will be an increase in the number of malicious programs finding their way into app stores, especially Android Market. The fact that Google's policy of checking new apps has changed very little, despite numerous malicious programs being discovered at Android Market, means the virus writers are unlikely to refrain from uploading malware to official stores.

There is a high probability that the first mass worm for Android will appear, capable of spreading itself via text messages and sending out links to itself at some online app store. We're also likely to see the first mobile botnet on the same platform.

The activities of several virus writer groups specializing in mobile applications evolved into the wholesale manufacture of malware in 2011 – a process that will continue to develop in 2012. It means we are likely to face a full-blown mobile malware industry next year.

Other mobile platforms

- **Symbian.** For a long time the most popular platform among users and virus writers. Now losing ground on the mobile OS market and among cybercriminals. Therefore, we don't expect to see significant amounts of malware for this platform.

- **J2ME.** We will continue to see quite a few malicious programs (more precisely, SMS Trojans) for Java 2 Micro Edition. However, their number will either remain at the same level or decrease.
- **Windows Mobile.** A platform that has never attracted much attention from virus writers and 2011 was no different. It will hardly be surprising if the number of malicious programs for this platform can be counted on the fingers of one hand.
- **Windows Phone 7.** Quite likely that the first proof-of-concept malware will appear for this platform.
- **iOS.** Since its arrival in 2009 two malicious programs have been detected that target cracked devices running iOS, and not much else. Don't expect any changes in 2012, unless Apple changes its software distribution policy.

In 2012 a considerable amount of non-Android-based malware will most probably be used in targeted attacks. A typical example is the attack using ZitMo and SpitMo (Zeus- and SpyEye-in-the-Mobile).

Mobile espionage – data theft from mobile phones and the tracking of subjects using their telephones and geolocation services – will become widespread, going well beyond the traditional use of such technologies by law enforcement agencies and private investigation companies.

Attacks on online banking

In 2012, attacks on online banking systems will be one of the most widespread methods of stealing money from rank and file users. The number of crimes committed in this area is rising rapidly all over the world in spite of all the technical measures taken by banks.

In the near future, it is likely that there will be more cases of unauthorized access to online banking systems in Asian countries. That is because these services are rapidly developing in South-East Asia and China, while the region's abundant cybercrime expertise has so far been focused on other types of attacks (including attacks on online gamers). Apart from online games, Asian cybercriminals have gained a reputation for their phishing attacks on clients of European and US banks. Now that local e-payment and banking services are developing in line with the rising standards of living in Asian countries, there will be an ever increasing number of attacks performed on local banks and users, employing dedicated, locally-focused phishing and Trojan programs.

Such attacks will most probably be targeted on mobile device users as well as PC users. Apart from South-East Asia and China, attacks may be performed on mobile payment services in East African countries.

Users' private lives

The problem of protecting users' confidential data is gradually becoming one of the hottest topics in IT security. Russian users have seen data leak from cellphone operators and e-commerce sites, there were the stories about the mobile software from CarrierIQ and the storing of geolocation data in iPad/iPhone, data thefts from tens of millions of clients of various systems in South Korea, the hacking of Sony PlayStation Network – to name just a few a few of the high-profile events that took place in the last year. Although these incidents varied in their causes as well as the amount and type of data stolen, they all had the same aim.

Increasingly companies all over the world are trying to collect as much information as they can about their clients. Unfortunately, this is not often supported by sufficient measures to protect the information that is gathered. The continuing development of "cloud technologies" also contributes to potential data losses: there is now an extra target for the cybercriminals to attack, i.e. the data centers where various companies' data are stored. Data leaks

from cloud services could deal a serious blow to the perception of the technology itself and the idea of "cloud storage" that largely rely on users' trust.

As for the systems collecting user data, similar to CarrierIQ, we are convinced there will be more instances of them being exploited in 2012. Mobile providers, software and web-service manufacturers do not intend to throw away the business opportunities that arise from holding users' data.

Hacktivism

Hacktivism, or hacker attacks as a form of protest, is now experiencing a revival and reaching new levels. Multiple attacks on various government institutions and businesses will continue in 2012 despite all the efforts of authorities arresting high-profile hacktivists. Hacktivism will increasingly have political implications, and this will be a more serious trend than in 2011 when most attacks targeted corporations or were carried out just for lulz.

However, hacktivism can also be used to disguise other attacks by distracting attention from them or setting up a false trail, thus creating an opportunity to "securely" hack an object of interest. In 2011, a number of hacktivist attacks have led to leaks of sensitive information which is undoubtedly the purpose of classic targeted attacks both in terms of commercial espionage and national interests. In these cases, hacktivists have greatly (and perhaps involuntarily) assisted other groups which can take advantage of their methods to steal information in attacks of a very different kind.

Conclusions

In summary, we expect to see the following events and trends next year in the field of cybercriminal activities:

- Cyber weapons like Stuxnet will be tailor-made for specific cases only. Cybercriminals will increasingly use simpler tools, such as kill switches, logic bombs etc. to destroy data at a required time.
- The number of targeted attacks will continue to grow. Cybercriminals will begin using new infection methods, as the effectiveness of existing methods diminishes. The range of targeted businesses and areas of economic activity will expand.
- 2012 will see cybercriminals writing mobile malware that primarily targets Google Android. We expect to see an increasing number of attacks exploiting vulnerabilities as well as the first mobile drive-by attacks.
- There will be more and more cases where malware is uploaded to official app stores, primarily to Android Market. Mobile espionage will become widespread; this will include stealing data from mobile phones, and tracking people using their telephones and geolocation services.
- In 2012, attacks on online banking systems will be one of the most widespread methods used to steal money from users. South-East Asia, China and East Africa are particularly at risk.
- Multiple attacks on various government institutions and businesses will be carried out all over the world. Hacktivism may also be used to conceal other types of attacks.

KASPERSKY lab