
There have been a lot of cyber-attacks against security agencies and by governments this year, according to Costin Rau from Kaspersky Lab.


Nazir Kazi, from e-Scan says that amongst the IT-related crimes, hacktivism is gaining momentum.


Anas Alnaqbi, senior security consultant from eHosting DataFort says that these attacks have serious global ramifications.

The top 10 cyber-threats of 2012

The regions top cyber-security experts from Kaspersky Lab, e-Scan and e-Hosting Datafort outline the threats enterprises have to be most aware of

1. THE RISE OF HACKTIVISM

Hacktivism has increased in 2012. Anonymous, LulzSec and TeaMp0i-soN are just a few hacktivist groups. Throughout 2011, hacktivist groups were actively involved in various operations against law enforcement agencies, banks, governments, security companies or major software vendors. Sometimes working together, these groups emerged as one of the main actors of 2012, through security breaches of networks belonging to the UN, Stratfor, IRC Federal, ManTech and the CIA website

2. TARGETED ATTACKS AND THE ADVANCED PERSISTENT THREAT

Incidents of this incldue the RSA security breach or imposing-sounding incidents such as operation Night Dragon, Lurid, or Shady Rat. Many of these attacks were directed at US targets, notably companies working with the US military or government. These attacks confirm the emergence of powerful nation-state actors and the establishment of cyber-espionage as common practice. Additionally, many of these attacks seem to be connected and have major global ramifications.

3. CRYPTOGRAPHIC ATTACKS AND MISUSE OF TRUST IN CAs

One of the affiliates of Comodo, a company known for its SSL digital certificates, was hacked. The attacker used the existing infrastructure to generate fake digital certificates, for web sites such as mail.google.com, login.yahoo.com, or login.skype.com. The DigiNotar breach was bigger. Hackers accessed the infrastructure and generated over 300 fraudulent certificates. The attacks show that we already have the loss of trust in the certificate authorities (CA), and, in the future, CA compromises may become even more popular.

4. NATION STATE SPONSORED MALWARE ATTACKS

Stuxnet, Duqu, Flame and Gauss are probably just a few of the multitude of malware created by nation states to spy on each other. The common problem with self replicating malware is that sometimes they get out of hand. For instance, besides its designated target, Stuxnet infected 150,000 PCs around the world.

Corporations can be caught up in this digital cross-fire and get infected with extremely advanced malware that uses zero-days and 'God mode' exploits such as Flame.

5. THE HACKING OF CLOUD SERVICES

The implementation of the cloud c introduces new issues with regard to security and privacy for data at rest and in motion. The Sony PSN hack pointed out several main things – first of all, in the cloud era, Personally Identifiable Information is nicely available in one place, over fast internet links, ready to be stolen. 77 million usernames and 2.2 million credit cards can be considered normal booty"in the cloud era.

The cloud is a great concept to host and share file, but has its drawbacks. Hosting sensitive information in the cloud should be a BIG NO for any organisation.

6. THE RISE OF ANDROID MALWARE

In August 2010, the first Trojan for the Android platform appeared masquerading as a media player app. In under a year, Android malware exploded and became the most popular mobile malware category. In Q2 2012 alone, the number of Trojans targeting the Android platform nearly tripled from the first quarter of the year. The popularity of Android malware can be attributed to the wild growth of Android itself, the documentation available on the Android platform making the creation of malware for Android quite trivial, and, there are many who blame the Google Market for its weak app screening.

7. SOCIAL ENGINEERING ATTACKS

No threat is small enough to be taken lightly. It could be in the form of an eMail Spoof or DoS Attack or even a Packet Sniffer – all of which can lead to data loss. But what seems to be inching its way into the corporate world is the rise in social engineering attacks. Hence, the need to look beyond the basics of policy and procedure development to more advanced technologies such as network monitoring, data leakage prevention, and log file analysis. Social engineering tactics on social media drive users to disclose sensitive information and download malware and these attacks are skyrocketing.

8. PATCHING AND UPDATES

Operating systems and applications have always been a target for hackers. Rarely is there an application developed which does not need any correction, upgrade or modification. With every new release, researchers trace vulnerabilities that can be exploited. Also, many enterprises rely on very old versions of operating systems such as Windows NT or Win 2000. Even Windows XP, an outdated OS, is still widely used. These older operating systems do not offer the same degree of security as, let's say, Windows 7 64 bits. The big challenge for corporations is updating these older OSes.

9. INSIDER THREATS

Insider threat always exists in some form or the other. Many of the successful attacks have got assistance from an insider, either accidently by opening a infected email, or on purpose after being lured with promises of financial gain. These insiders can include unhappy employees or previous employees of the company that posses enough information to be able to pose a threat to the infrastructure. Humans as a threat to computer security is here to stay.

RSA was hacked, due to an employee being unable to recognise the threat in from of a PDF which was lying inside the Junk folder.

10. MOBILE THREATS

More than 50 apps on the Android Marketplace were infected with a Trojan designed to gain administrative privileges over a smartphone without the user's permission. It could download more malicious programmes to your phone without your knowledge and steal data. It will only be a matter of time before it occurs again. A recent Android malware outbreak in China spread through apps distributed on forums and alternative app markets. Long URLs have already proved to be excellent USP for phishing syndicates, QR codes for long URLs won't be much far behind.