Top 10 Security Issues That Will Destroy Your Computer In 2013

Hacktivism. Depending on which side you're on, hactivism either gets better or worse. If your government or your company is deemed villainous by the "hactivistas" out there, look out. They're coming in droves.

Here's one for you. In October, I traveled to Russia. Nice hotel. Six stars, let's say. Pretty Moscow views. Beautiful women. Bentleys in the lobby. Hush-hush restaurants. Too expensive. Okay, last month I discover that someone had hacked into an ATM machine there, got my pin number from my Santander debit card and stole a few hundred bucks from my account. I had to cancel the card, you all know the routine. I still don't have a debit card.

Three years ago, I was the victim of identity theft. Someone, somehow, got my ID through my Best Buy credit card and subsequently took $8,000 chunks out of my bank account until it was all gone. They forged my signature. They forged my checks, all made out to some New Jersey automotive shop that did not exist.

Luckily, I got it all back, two months later. I thought it would never happen again. But it did. And it does. It never ends.

Cyber security guys say it will only get worse in 2013.

Senior researchers at Russian-based Kaspersky Lab, one of the world's top three internet security software companies, came out with their list of ominous predictions on Wednesday.

Whether you're paying credit card bills on an Android or running the IT network for a Fortune 500 company, here is what Kasperky Lab says you can expect baring down on you next year.

1. Targeted Attacks

While the threat landscape is still dominated by random, speculative attacks designed to steal personal information from anyone unlucky enough to fall victim to them, targeted attacks have become an established feature in the last two years. Such attacks are specifically tailored to penetrate a particular organization and are often focused on gathering sensitive data that has a monetary value in the 'dark market'. Targeted attacks can often be highly sophisticated. But many attacks start by 'hacking the human', i.e. by tricking employees into disclosing information that can be used to gain access to corporate resources. Any organization can become a victim. All organizations hold data that is of value to cybercriminals; and they may also be used as 'stepping-stones' to reach other companies."

2. More Hactivism

Last year's attacks included the DDoS attacks launched by Anonymous on government websites in Poland, following the government's announcement that it would support ACTA (the Anti-Counterfeiting Trade Agreement); the hacking of the official Formula 1 website in protest against the treatment of anti-government protesters in Bahrain; the hacking of various oil companies in protest against drilling in the Arctic; the attack on Saudi Aramco; and the hacking of the French Euromillions website in a protest against gambling. Society's increasing reliance on the Internet makes organizations of all kinds potentially vulnerable to attacks of this sort, so 'hacktivism' looks set to continue into 2013 and beyond."

3. Cyber Espionage & Warfare

Stuxnet pioneered the use of highly sophisticated malware for targeted attacks on key production facilities. However, while such attacks are not commonplace, it's now clear that Stuxnet was not an isolated incident. We are now entering an era of cold 'cyber-war', where nations have the ability to fight each other unconstrained by the limitations of conventional real-world warfare. Looking ahead we can expect more countries to develop cyber weapons."

4. Big Brother Watching Even More

(This will include) using technology to monitor the activities of those suspected of criminal activities. This is not a new issue – consider the controversy surrounding 'Magic Lantern' and the 'Bundestrojan'. More recently, there has been

debate around reports that a UK company offered the 'Finfisher' monitoring software to the previous Egyptian government and reports that the Indian government asked firms (including Apple, Nokia and RIM) for secret access to mobile devices. Clearly, the use of legal surveillance tools has wider implications for privacy and civil liberties. And as law enforcement agencies, and governments, try to get one step ahead of the criminals, it's likely that the use of such tools – and the debate surrounding their use – will continue."

5. Increase in Malware

The wide use of mobile devices, while offering huge benefits to a business, also increases the risk. Cloud data can be accessed from devices that may not be as secure as traditional endpoint devices. When the same device is used for both personal and business tasks, that risk increases still further."

6. Privacy Rights Eroding

The value of personal data – to cybercriminals and legitimate businesses – will only grow in the future, and with it the potential threat to our privacy increases."

7. Cyber Extortion

This year we have seen growing numbers of ransomware Trojans designed to extort money from their victims, either by encrypting data on the disk or by blocking access to the system. Until fairly recently this type of cybercrime was confined largely to Russia and other former Soviet countries. But they have now become a worldwide phenomenon, although sometimes with slightly different modus operandi. In Russia, for example, Trojans that block access to the system often claim to have identified unlicensed software on the victim's computer and ask for a payment. In Europe, where software piracy is less common, this approach is not as successful. Instead, they masquerade as popup messages from law enforcement agencies claiming to have found child pornography or other illegal content on the computer. This is accompanied by a demand to pay a fine. Such attacks are easy to develop and, as with phishing attacks, there seem to be no shortage of potential victims."

8. Apple Under Attack

Attacks on the Mac OS has been growing steadily over the last two years; and it would be naive of anyone using a Mac to imagine that they could not become the victim of cyber crime. It's not only generalized attacks – such as the 700,000-strong Flashfake botnet – that pose a threat; we have also seen targeted attacks on specific groups, or individuals, known to use Macs. The threat to Macs is real and is likely keep growing."

9. Android, Even Worse

Mobile malware has exploded in the last 18 months. The lion's share of it targets Android-based devices – more than 90 per cent is aimed at this operating system. The appearance of the 'Find and Call' app earlier this year has shown that it's possible for undesirable apps to slip through the net. But it's likely that, for the time being at least, Android will remain the chief focus of cyber criminals. The key significance of the 'Find and Call' app lies in the issue of privacy, data leakage and the potential damage to a person's reputation: this app was designed to upload someone's phone book to a remote server and use it to send SMS spam."

10. Un-Patched Exploits In Java

One of the key methods used by cyber criminals to install malware on a computer is to exploit un-patched vulnerabilities in applications. This relies on the existence of vulnerabilities and the failure of individuals or businesses to patch their applications. Java vulnerabilities currently account for more than 50 per cent of attacks, while Adobe Reader accounts for a further 25 per cent. cyber criminals will continue to exploit Java in the year ahead. It's likely that Adobe Reader will also continue to be used by cyber criminals, but probably less so because the latest versions provide an automatic update mechanism."

Source: Kaspersky Lab researchers Costin Raiu and David Emm. For full explanations of security threats, and a look at 2012 threats, see the Kaspersky Security Bulletin 2012.