National Security Cyberspace Institute NSCI

CyberPro

October 6, 2011

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Nikolay Grebennikov, Kaspersky Lab

Nikolay was appointed Chief Technology Officer of Kaspersky Lab at the beginning of 2009. He joined the company in 2003 as a system analyst for the Kaspersky Anti-Virus for Windows Workstation 5.0 project team and within six months was heading the Kaspersky Anti-Virus 6.0 team. Then Nikolay was deputy director of innovative technologies in charge of all new research including proactive defense, heuristic detection, and defense against information leaks, keyloggers and rootkits. Before his current role, Nikolay was Vice President of Research and Development since 2008.

Before joining Kaspersky Lab, Nikolay worked as a device driver developer, database programmer, general software programmer and project manager for several IT companies based in Moscow.

Nikolay has a Ph.D in Computer Science from Bauman Moscow State Technical University for his work on information security.

NSCI: First, can you tell us a little bit about Kaspersky Lab and the area(s) of cybersecurity you are focused on?

GREBENNIKOV: Kaspersky Lab is a leading developer of user-centric IT security solutions that provides effective protection against all Internet threats, including viruses, spyware, crimeware, hackers, phishing and spam to its users, be they consumers or corporate clients. Kaspersky Lab products provide superior detection rates and one of the industry's fastest outbreak response times for home users, SMBs, large enterprises and the mobile computing environment. Our technology is also used worldwide inside the products and services of the industry's leading IT security solution providers. Currently the company is ranked among the world's top four vendors of security solutions for endpoint users. According to the company's 2010 financial results, Kaspersky Lab's global revenue grew by 38% compared to the previous year and exceeded US $500 million.

Over 300 million people worldwide are protected by Kaspersky Lab products and technologies. Kaspersky Lab's corporate client-base exceeds 200,000 companies located around the globe, ranging from small and medium-sized businesses, all the way up to large governmental and commercial organizations.

Kaspersky Lab was the first to develop many technological standards in the antivirus industry, including full-scale solutions for Linux, Unix and NetWare, a new-generation heuristic analyzer designed to detect newly emerging viruses, effective protection against polymorphic and macro viruses, continuously updated antivirus databases and a technique for detecting viruses in archived files. This is reflected in many respected security software developers choosing the Kaspersky Anti-Virus engine to drive their own products, including Blue Coat, D-Link, IBM, Juniper, LANDesk, Microsoft, M86, Netgear and ZyXEL etc.

The company's product range covers all of the main information security requirements that users, businesses and large state organizations have to adhere to, including: excellent protection levels, adaptability to changing circumstances, scalability, compatibility with different platforms, high performance, high fault tolerance, ease of use and high value. One of the primary advantages of Kaspersky Lab's corporate range is the easy, centralized management provided by Kaspersky Administration Kit 8.0 that extends to the entire network regardless of the number and type of platforms used.

Kaspersky Lab's tightly integrated solutions provide agile and efficient malware protection solutions against contemporary security threats. Kaspersky Lab empowers secure businesses worldwide with:
- Tightly integrated protection leveraging deep anti-malware solutions and simplified, centralized management solutions.

- Powerful tools ensure security and control over an array of applications, devices and web content.
- Simple deployment, optimized for complex IT environments with limited staff resources.
- Streamlined architecture minimizes system impacts.

The range of products for business includes applications for the protection of file servers and data storage systems running Windows, Linux and Novell NetWare operating systems, Microsoft Exchange and IBM Lotus Domino groupware servers. It also covers Sendmail, qmail, Postfix and Exim mail servers, Microsoft ISA Server/Forefront TMG, and various Linux proxy servers, workstations and laptops running Windows, Linux and Mac operating systems, as well as smartphones using the BlackBerry, Windows Mobile and Symbian platforms.

NSCI: How are we doing in preventing malware from spreading, and minimizing its impact when it does spread?

GREBENNIKOV: Our flagship product Kaspersky Internet Security 2012 includes the state of the art HIPS (Host Intrusion Prevention System) which together with the new System Watcher works against malware that is trying to infect the system and spread further. These technologies limit the impact of unknown malicious program, which can otherwise escape conventional detection strategies, such as those that are signature-based. It is extremely important for a computer network for instance, or actually the for cyber ecosystem at a global level to limit the spread of malware – this is why such technologies can really make a difference when deployed on many computers.

Additionally, Kaspersky Lab constantly monitors the malware threat and situation at a global level, engaging in malicious websites shutdown, cooperating with ISPs to limit malware spread and working together with non-profit security organizations such as CERTs in order to provide intelligence on how to effectively fight against malware. Currently, cybercrime has become an explosive, huge phenomenon and stopping it will require a lot of efforts, cooperation at the highest levels between law enforcements, governments and private security companies and of course, the help of the media to educate the users about the threat.

Also Kaspersky Lab is in ongoing assault against botnet operators and the hosting companies that allow anonymous domain registrations which facilitate them. For example, Kaspersky Lab, Microsoft and Kyrus Tech have successfully worked together in September’2011 to take out the Kelihos botnet , originally named Hlux by Kaspersky Lab. Kelihos was used for delivering billions of spam messages, stealing personal data, performing DDoS attacks and many other criminal activities, via an estimated 40,000 computers.

Kaspersky Lab has played a pivotal role in taking down the botnet, tracking it since the beginning of 2011, when it started collaborating with Microsoft in tackling Kelihos, including sharing its live botnet tracking system with the US company. Kaspersky Lab has also taken care that the botnet cannot be controlled anymore, and continues to make sure that this is the case. Its specialists reversed-engineered the code used in the bot, cracked the communication protocol, discovered the weaknesses in the peer-to-peer infrastructure, and developed the corresponding tools to counteract it. What’s more, since the offending domains used in the botnet have gone offline via court orders Microsoft had secured, Kaspersky Lab has been “sinkholing” the botnet - where one of its computers has gotten inside the botnet’s complex internal communications to bring it under its control.

NSCI: With Kaspersky Lab's main office in Moscow and regional offices in numerous countries, you obviously bring an international perspective to the fight against malware. What key international steps do you think need to be taken to ensure a more secure cyberspace? What progress have we made in the last few years?

GREBENNIKOV: The main problem of dealing with internet threats is that the Web has no borders, and neither do the cybercriminals who operate on the Internet. Today a cybercriminal robs Brazilian user, tomorrow – German user, and the day after tomorrow – American user. And all this time this cybercriminal is in China. Thereby law enforcement agencies have jurisdictional limits, and are unable to conduct investigations across the globe. Current policing methods are ineffective due to a lack of information-sharing between national police and other law enforcement agencies. That’s why we need Internet police to investigate international crime – a kind of Internet Interpol. Also I suggest creating a unified law on cybercrime.

One more problem solution is in introducing regulation in the form of Internet passport, which will identify users and allow them the same kinds of digital identification as a real-world passport. But don’t confuse it with the end of the Internet Anonymity – these are different things. Without this Internet ID users won’t have a possibility to have an online banking access or to vote for the next President. But without passport they will connect to the Internet, chat with their friends, use social networks – act as they usually do.

NSCI: Can you share a few cybersecurity best practices with our readers?

GREBENNIKOV: One of the most important suggestions is to review the security policy and make sure it's up to date. Actually, very few companies have a security policy at all! Secondly, I'd suggest companies to get rid of old hardware and use modern computer systems that run Windows 7 64 bits or Windows 2008 R2 64 bits. In general, older versions of Windows provide much less security than these two modern variants and can be hacked a lot easier. It's also important to update the operating system and any third party software on a regular basis. This includes Microsoft Office, Adobe Reader, Adobe Flash, JAVA and so on. Finally, it's very important to run a security software suite which protects against malware, hackers and spam.

Most attacks against consumers at the moment happen through the web or pirate software. As a first line of defense, we recommend to also update the operating system and any third party software on a regular basis. This includes Microsoft Office, Adobe Reader, Adobe Flash, JAVA and so on.

To browse the internet, Chrome and Firefox are more secure than Internet Explorer which is a primary target of hackers. Chrome especially has a very good history of security and due to its sandboxing architecture has better security than Firefox.

Recently, a lot of incidents are related to weak passwords on online resources. Make sure you have strong passwords (containing lowercase, uppercase, numbers and special signs) and that you have a different password for each online resource. This way, even if one system gets hacked (eg. Sony PSN) your Yahoo account is still secure.

Finally, it's very important to install and run an internet security suite, such as Kaspersky Internet Security 2012 – which provides complete protection again the different kind of threats that exist in today's digital world.

NSCI: What are the keys to the cyber community at large becoming more proactive in addressing cybersecurity threats?

GREBENNIKOV: Through education, training, better cybercrime laws, cooperation between governments, awareness, the cybercrime situation on the Internet can be slightly improved. Unfortunately, it's unlikely that it can also be solved forever; but, I'm afraid that without education and awareness, the situation can go wrong very quickly.

The more information about threats and variety of malware is spread the more people will know about it. Experts from Kaspersky Lab regularly participate in major international events such as IT security conferences and exhibitions. The Company puts a lot of effort into raising public awareness about IT security issues and uniting the efforts and knowledge of the IT industry's key players in the daily struggle against cybercrime. Moreover Kaspersky Lab regularly holds media events in all parts of the world in order to keep the media world updated on all possible security threats and ways of struggling against them. Also Kaspersky Lab runs Securelist.com , a computer security portal devoted to educating the general public about different aspects of Internet security and various threats existing in the Internet.

NSCI: Kaspersky Lab has significant cybersecurity experience and knowledge. Do you think there are enough cybersecurity professionals to go around when it comes to national and international needs, the private sector and government sector, etc?

GREBENNIKOV: Currently, every nation in the world is facing the growing threat of cybercrime, which is already affecting home users, SMBs, corporations and is starting to affect governmental institutions as well. We can think of it this way – the number of threats has been growing at an exponential rate during the past ten years, however, the number of security experts has stayed pretty much the same. This is why there is currently a huge need for cybersecurity experts at all levels, in the private sector, governmental and of course, law enforcement. Particularly the need is probably the highest in the Large Enterprises (LE) sector, where faced with the growing trend of cybercrime, many police departments find themselves effectively drowned in the huge number of cases. The solution here which has been already tested successfully in the USA is for the LE agencies to start special qualification programs in which cybersecurity experts can be trained to work with LE in certain cases. Unfortunately, this is a slow process which can take as much as 10 years and it will be a while until we see it happening globally.

NSCI: Can you share some of the trends in malware you are seeing? What does the future look like when it comes to malware threats?

GREBENNIKOV: The defining feature of the next decade will be the end of Windows' domination of user operating systems. Though Microsoft's brainchild will remain the primary business platform, everyday users will have access to an ever-expanding variety of alternative operating systems. Notably, even now the number of devices accessing the Internet via Windows and non-Windows platforms are almost the same, with the latter even occasionally exceeding their Microsoft counterparts.

The growing number of new operating systems will affect the process of threat creation: cybercriminals will not be able to create malicious code for large numbers of platforms. This leaves them with two options: either target multiple operating systems and have many individual devices under their control, or specialize in Windows-based attacks on corporations. The second variant will probably appeal to them more – by 2020, targeting individual users will become much more complex because the emerging trend of making payments electronically and using online banking will continue, but biometric user identification and payment protection systems will become the norm.

The coming changes in operating systems and their specifications will affect virus writing techniques as these new systems evolve. Many cybercriminals who used to target Windows devices will have to become adept at exploiting the new-generation operating systems. To retain their 'place in the sun', today's cybercriminal will need to enlist the help of members of the younger generation who are capable of writing malicious code for the new platforms. However, this state of the affairs cannot prevail forever and we may well see 'turf wars' between different hackers and hacker groups.

Cybercrime in 2020 will almost assuredly divide into two groups. One group will specialize in attacks on businesses, sometimes to-order. Commercial espionage, database theft and corporate reputationsmearing attacks will be much in demand on the black market. Hackers and corporate IT specialists will confront each other on the virtual battlefield. State anti-cybercrime agencies will probably be involved in the process too and will have to deal predominantly with Windows platforms, in addition to the latest versions of traditional *nix systems.

The second group of cybercriminals will target those things that influence our everyday lives, such as transport systems and other services. Hacking such systems and stealing from them, making free use of them and the removal and changing of personal data about customers' activities will be the main focus of attention of the new generation of hackers, who will make a living this way.

The trend that has seen the Internet become both a popular resource for communication, entertainment and news, and a specially designed tool for Internet commerce and online payments, etc. will continue. The 'online user-base' will expand to include many mobile and smart devices capable of using the web to exchange or transfer information without the need for human intervention.

Botnets, one of today's most potent IT threats, will evolve dramatically. They will incorporate more and more mobile and Internet-enabled devices, and zombie computers as we know them will become a thing of the past.

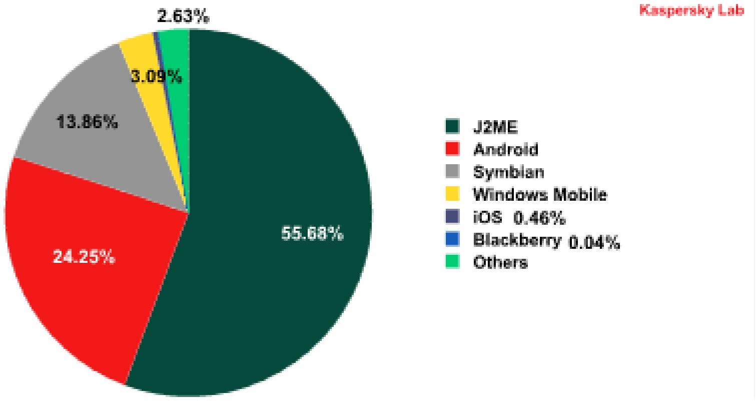
The tools and technologies used in the field of communications will undergo massive change. These changes will see greatly increased data transfer rates and enhancements that will make the virtual communication experience much closer to that of real-life: by 2020, communication via the Internet with the help of a keyboard will be the stuff of old movies, meaning spammers will need to seek out new ways of delivering their unwanted correspondence to addressees across the globe. The first step the spammers will take is to change from targeting desktops to mobile devices. The volume of mobile spam will grow exponentially, while the cost of Internet-based communications will shrink due to the intensive development of cellular communication systems. As a result, users will be less likely to worry about unwanted advertising material.

The old adage 'Knowledge is power' will be more relevant than ever before. The struggle for the means to collect, manage, store and use information, about everything and everybody, will define the nature of threats for the next decade. Therefore the problem of privacy protection will be one of the key issues of the decade.

NSCI: How would you characterize the cybersecurity threat to mobile devices? What about cloud computing?

GREBENNIKOV: Today we can say that smartphones are almost equal to personal computers. We do same things with their help: social networking, gaming, emails, online banking, etc. And, as a fact, a lot of personal information is stored on a device. All these things led to the fact that 99% of all mobile malware today is created for profit. Cybercriminals found different ways in order earn money illegally: SMS trojans, dialing trojans, malware which is able to steal personal information, backdoors which are able to receive commands from remote servers and execute them. So that's why it is important to pay same attention to security on mobile devices.

Today almost all popular mobile platforms are targeted by cybercriminals and malware. We've seen pieces of malicious software for Symbian, Windows Mobile, Android, iOS, Blackberry and J2ME. Just over one year ago (in early August 2010), the first-ever malicious program for the Android operating system was detected: the SMS Trojan FakePlayer. Since its emergence, the global malware situation — both for mobile threats in general and Android in particular — has changed dramatically. Less than one year ago, the number of malicious programs targeting Android caught up with the number of malicious programs targeting the Symbian platform (the first threat for Symbian appeared in 2004). Today, threats designed for Android represent approximately 24% of the overall number of detected threats targeting mobile platforms.



The distribution of malicious programs targeting mobile platforms, by operating system

A total of 85% of all smartphone threats (i.e. excepting J2ME) detected from August 1, 2010 through August 31, 2011 target the Android system.

The current monetization scheme used by most mobile Trojans involves sending text messages to short numbers. The result is withdrawals of funds from users' accounts or the implementation of subscriptions to fee-based services without the individual user's consent. In the latter case, which is more common in Asia, a user will receive a text message from a service with information about the subscription. To prevent the user from noticing anything suspicious, the Trojan will delete the message about the fee-based service as soon as it arrives. As a result, the Trojan can continue to operate on a device for a long time, making money for the malicious user all the while.

What is worrying is the fact that malicious programs designed for mobile devices are being spread not only through a variety of resources belonging to third parties, but also via official app stores. Clearly, Android Market needs to review its app publication policy. At this point, however, the owners of both official and unofficial stores are in no hurry to change any of their rules — and this failure to take action is playing right into the hands of malicious users. In this situation, the number of those who want to make money at the expense of the average user will grow, which will impact the number of threats, as well as the quality of those threats.

Now we can say that smartphones are almost equal to desktop computers. It means that consumers must use the same rules in order to protect their devices from mobile malware. First of all, it is necessary to update OS third party software regularly. Secondly, install software and applications only from trusted sources like official application stores or marketplaces or developer's websites. Thirdly, ignore all SMS spam messages with suspicious content or URLs. Fourthly, do not leave your device anywhere where you can't see it and try to keep an eye on it always. Fifthly, use encryption and/or password or PIN protection. Sixthly, try to avoid jailbreaking. And finally, don't think that your smartphone is safer than your PC.

When it comes to the security aspect of the 'cloud', it is important to remember that placing data beyond your network perimeter or using third-party services adds more links to the chain – at the very least a network provider and the actual provider of the cloud services. As a result, the overall level of protection of such a setup depends on several parties, and often there is no guarantee of secure, uninterrupted operations between them. Instead of just protecting the corporate perimeter this sort of system entails protecting external channels and external storage spaces. In theory, this reduces the overall level of security, but it also plays a big part in keeping costs down and in a number of cases it is entirely justified. Situations where data stored in the cloud is much safer than it would be if it was stored inside an organization are not uncommon.

The drawbacks of public clouds are obvious and particularly numerous. There's the risk of your data being accessed by foreign government agencies (the services are based in the US and belong to US companies that have to comply with local laws and decisions made by courts and regulators). There's the risk of interrupted services due to technical problems (e.g. hacker attacks or power cuts) or access restrictions on a national level (e.g. China limits access to a range of Google resources). Then, of course, there are direct attacks: if a cybercriminal has access to your computer, he has access to your data in the cloud. Moreover, the cloud itself has become a target for cybercriminals. If there is a vulnerability in the cloud's security, all the data stored in it can be stolen. A good example of this was the HBGary hack in February 2011. The hackers couldn't penetrate the company's local network, but got access to the company's corporate emails located on Google Apps for Business. As a result, the company's whole email archive was stolen and found its way into the public domain.

NSCI: In the future, what technologies will be critical to improving cybersecurity?

GREBENNIKOV: Throughout the history, the nature of the threat landscape has changed many times, depending on several factors. First of all, it changes together with new operating systems and hardware, such as for instance Windows 95 (which killed boot viruses) or the wide adoption of Android smartphones which resulted in the growth of Trojans for this platform. Secondly, it changes with new defense technologies, which limit the spread of certain threats – for instance, the wide adoption of firewalls which resulted in the death of network worms. Finally, threats evolve when the people begin using already existing products, features and technologies in a different way. A good example here is the cloud or social networks. We have seen threats evolve and change a lot during the past 20 years and no doubt, this will continue during the next 20 years. In order to estimate which technologies will be fighting cyberthreats in the future, we need to take a look at how the threats will change as well. So we can assume that malware for mobile hardware (tablets, smartphones) is going to evolve, together with malware which takes advantage of new communication technologies and media (eg. Social networks). Defense against these will not be easy! Luckily, at the moment there are already a couple of promising technologies that are being regarded as the future of ITSec. These include but not limited to sandboxing and virtualization, whitelisting and reputation-based technologies. Many products, including KIS2012 already showcase these technologies in order to fight against new and unknown threats; there is no doubt that these will constitute the foundation for tomorrow's threat-defense products.

NSCI: Thank you very much for taking the time to visit with us.