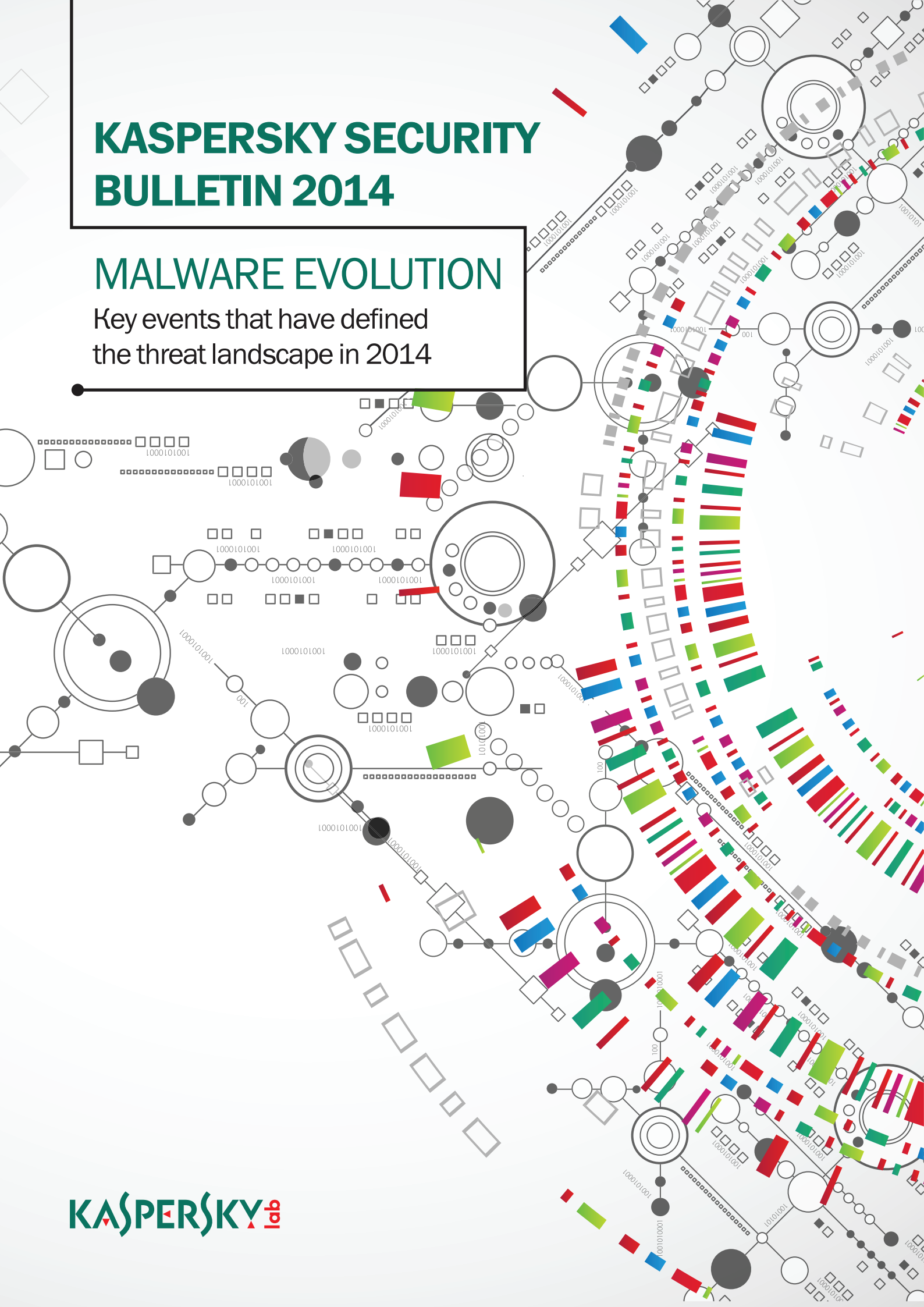
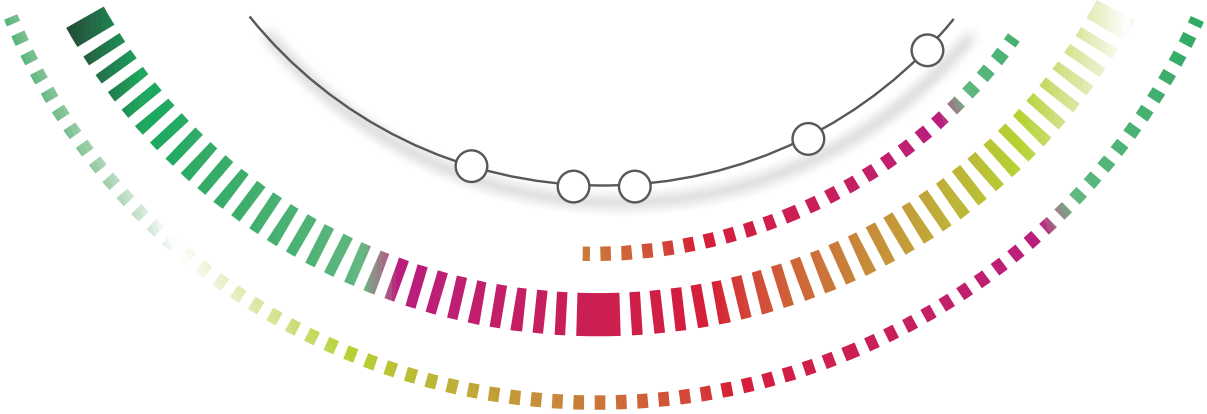
KASPERSKY SECURITY BULLETIN 2014

MALWARE EVOLUTION

Key events that have defined the threat landscape in 2014



KASPERSKY lab



CONTENT

David Emm

The end of the year is traditionally a time for reflection – for taking stock of our lives before considering what lies ahead. We'd like to offer our customary retrospective of the key events that shaped the threat landscape in 2014.

TARGETED ATTACKS AND MALWARE CAMPAIGNS

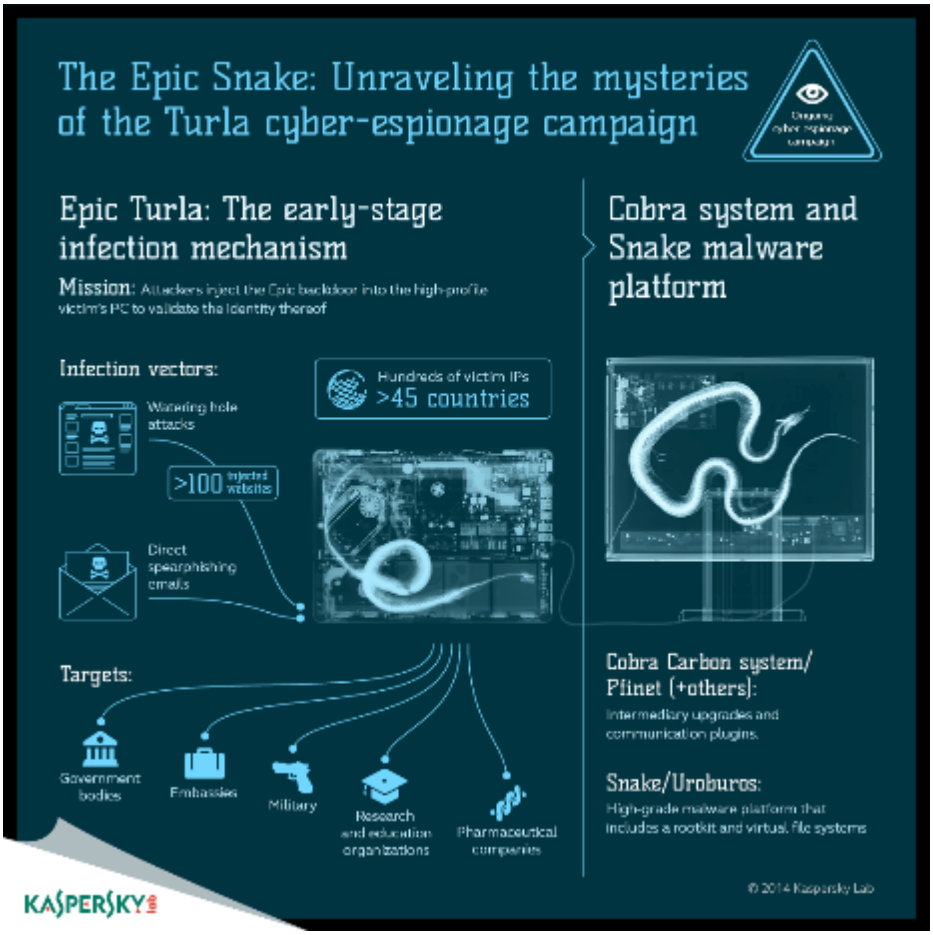
Targeted attacks are now an established part of the threat landscape, so it's no surprise to see them feature in our yearly review.

The complex cyber-espionage campaign called 'Careto' or 'The Mask' (Careto is Spanish slang for 'ugly face' or 'mask') was designed to steal sensitive data from specific organizations. The victims of the attack included government agencies, embassies, energy companies, research institutions, private equity firms and activists from 31 countries around the world. Careto included a sophisticated backdoor Trojan capable of intercepting all communication channels and of harvesting all kinds of data from infected computers – including encryption keys, VPN configurations, SSH keys, RDP files and some unknown file types that could be related to bespoke military/government-level encryption tools. The code was highly modular, allowing the attackers to add new functionality at will. There are versions of the backdoor for Windows and Mac OS X and we also found references in some modules indicating that there might be versions for Linux, iOS and Android. As with any sophisticated campaign of this sort, attribution is difficult. Use of the Spanish language in the code doesn't help, since Spanish is spoken in many parts of the world. Also, it's possible that its use is an intentional piece of misdirection. However, the very high degree of professionalism of the group behind this attack is unusual for cybercriminal groups – one indicator that Careto could be a state-sponsored campaign. Like previous targeted attack campaigns, the roots of Careto stretch back well before the threat first came to light: we believe that the attackers have been active since 2007.

Early in March there was widespread discussion among security researchers about a cyber-espionage campaign called 'Epic Turla'. Researchers at G-DATA believed the malware may have been created by Russian special services; while research carried out by BAE Systems linked it to malware identified as 'Agent.btz' that dates back to 2007 and was used in 2008 to infect the local networks of US military operations in the Middle East. Our initial analysis of Epic Turla focused on the malware's use of USB flash drives to store stolen data that can't be sent directly over the Internet to the attackers' Command-and-Control (C2) server. The worm writes a file called 'thumb.dd' to all USB flash drives connected to an infected computer. If the flash drive is subsequently inserted into another computer, the 'thumb.dd' file is copied to the new computer. Epic Turla isn't the only malware that is aware of 'thumb.dd'. This is one of the files in the 'USB Stealer module' in Red October. Looking back further, Gauss and miniFlame were aware of 'thumb.dd and looked for the file on USB flash drives. You can find a chart showing the

points of comparison here. We think it's likely that there are tens of thousands of USB flash drives around the world containing files called 'thumb.dd' created by this malware.

In our subsequent analysis of Epic Turla we explained how the attackers use social engineering to spread the malware and highlighted the overall structure of the campaign. The attackers use spear-phishing emails to trick their victims into installing a backdoor on their computer. Some of these include zero-day exploits – one affecting Adobe Acrobat Reader and the other a privilege escalation vulnerability in Windows XP and Windows Server 2003. They also use watering-hole attacks that deploy a Java exploit, Adobe Flash exploits and Internet Explorer exploits, or trick victims into running fake 'Flash Player' malware installers. Depending on the IP address of the victim, the attackers serve Java or browser exploits, signed fake Adobe Flash Player software or a fake version of Microsoft Security Essentials. Unsurprisingly, the choice of web sites reflects the specific interests of the attackers (as well as the interests of the victims). However, our analysis showed that the Epic Turla backdoor is just the first stage of the infection. It is used to deploy a more sophisticated backdoor known as the 'Cobra/Carbon system' (named 'Pfinet' by some anti-malware products). The unique knowledge to operate these two backdoors indicates a clear and direct connection between them: one is used to gain a foothold and validate the high-profile victim. If the victim proves to be of interest to the attackers, the compromised computer is upgraded to the full Carbon system. You can find an overview of the Epic Turla campaign here:



In June we reported on our research into an attack on the clients of a large European bank that resulted in the theft of half a million euros in just one week. We named this 'Luuuk', after the path in the administration panel used in the C2 server. Although we were unable to obtain the malware used to infect the victims, we believe the criminals used a banking Trojan that performed 'Man-in-the-Browser' operations to steal the victims' credentials through a malicious web injection. Based on the information available in some of the log files, the malware stole usernames, passwords and one-time passcodes (OTP) in real time. The attackers used the stolen credentials to check the victim's account balance and perform malicious transactions automatically, probably operating in the background of a legitimate banking session. The stolen money was then transferred automatically to pre-defined money mule accounts. The classification of pre-defined money mules used by the attackers was very interesting. There were four different money mule groups, each defined by the amount of money the mules in the group could accept – probably a reflection of the level of trust between them. We identified 190 victims in total, most of them located in Italy and Turkey. The sums stolen from each victim ranged from €1,700 to €39,000; and amounted to €500,000.

Although the attackers removed all sensitive components soon after our investigation started, we believe that this represents a change of infrastructure rather than a complete shutdown of the operation. The cybercriminals behind the campaign are highly professional and very active. They have also shown proactive operational security activities, changing tactics and removing traces when discovered. The investigation into this campaign, which we reported to the bank concerned and to the appropriate law enforcement agencies, is ongoing.

The end of June saw the re-activation of a targeted attack campaign from early 2013, called 'MiniDuke'. The original campaign stood out for several reasons. It included a custom backdoor written in the 'old school' Assembler programming language. The attack was managed using an unusual command-and-control (C2) infrastructure: it made use of multiple redundancy paths, including Twitter accounts. The developers transferred their updated executables hidden inside GIF files.

Targets of the new operation, known as 'CosmicDuke', or 'TinyBaron', include government, diplomatic, energy, military and telecom operators. But unusually the list of victims also includes those involved in the trafficking and reselling of illegal substances, including steroids and hormones. It's not clear why: maybe the customizable backdoor was made available as so-called 'legal spyware', or it was available in the underground market and was purchased by various rivals in the pharmaceutical business to spy on each other.

Victim geography (Miniduke and CosmicDuke)

The malware spoofs popular applications designed to run in the background - including file information, icons and even file size. The backdoor itself is compiled using 'BotGenStudio' - a customizable framework that al-

lows the attackers to enable and disable components when the bot is constructed. The malware not only steals files with specific extensions, but also harvests passwords, history, network information, address books, information displayed on the screen (screenshots are made every five minutes) and other sensitive data. Each victim is assigned a unique ID, making it possible to push specific updates to individual victims.

The malware is protected with a custom obfuscated loader which heavily consumes CPU resources for 3-5 minutes before passing execution to the payload. This makes it hard to analyze. But it also drains the resources needed by security software to emulate the malware's execution. On top of its own obfuscator, the malware makes heavy use of encryption and compression based on the RC4 and LZRW algorithms. They are implemented slightly differently to the standard versions - we believe that this is done deliberately to mislead researchers. The internal configuration of the malware is encrypted, compressed and serialized as a complicated registry-like structure, which has various record types including strings, integers and internal references. Stolen data uploaded to the C2 server is split into small chunks (of around 3KB), which are compressed, encrypted and placed in a container to be uploaded to the server. If it's a large file, it may be placed into several hundred different containers that are all uploaded independently. It's likely that these data chunks are parsed, decrypted, unpacked, extracted and reassembled on the attacker's side. While this method might add an overhead, the layers of additional processing ensure that very few researchers will get to the original data. This method also offers increased reliability against network errors.

In July we published an in-depth analysis of a targeted attack campaign that we dubbed 'Crouching Yeti' – also known as 'Energetic Bear', because researchers from CrowdStrike had suggested that the attackers were located in Russia: we don't think there's enough evidence to confirm this one way or the other. This campaign, active since late 2010, has so far targeted the following sectors: industrial/machinery, manufacturing, pharmaceutical, construction, education and information technology. So far there have been more than 2,800 victims worldwide, and we have been able to identify 101 different victim organizations – mostly in the United States, Spain, Japan, Germany, France, Italy, Turkey, Ireland, Poland and China.

The attackers behind Crouching Yeti use various types of malware (all designed to infect systems running Windows) to infiltrate their victims, extend their reach within the target organizations and steal confidential data, including intellectual property and other strategic information. The malware used includes special modules to collect data from specific industrial IT environments. Infected computers connect to a large network of hacked web sites that host malware modules, hold information about victims and send commands to infected systems. The attackers use three methods to infect their victims. These include a legitimate software installer re-packaged to include a malicious DLL file; spear-phishing e-mails; and watering-hole attacks.

Technology is now an integral part of our lives, so it's hardly surprising to see a cyber-dimension to conflicts around the world. This is especially true of the Middle East, where geo-political conflicts have intensified in recent years. In August we reported on the increase in malware activity in Syria from early 2013. The victims of these attacks are not only located in Syria: the malware has also been seen in Turkey, Saudi Arabia, Lebanon, Palestine, the United Arab Emirates, Israel, Morocco, France and the United States. We were able to track the C2 servers of the attackers to IP addresses in Syria, Russia, Lebanon, the United States and Brazil. In total, we found 110 files, 20 domains and 47 IP addresses associated with the attacks.

It's clear that the groups involved in the attacks are well organized. So far the attackers have made use of established malware tools rather than developing their own (although they use a variety of obfuscation methods to bypass simple signature-based detection). However, we think it's likely that the number and sophistication of malware used in the region is likely to increase.

In November we published our analysis of the 'Darkhotel' APT, a campaign that has been operating for almost a decade, targeting thousands of victims across the globe. 90 per cent of the infections we have seen are in Japan, Taiwan, China, Russia and Hong Kong, but we have also seen infections in Germany, the USA, Indonesia, India, and Ireland.

The campaign employs varying degrees of targeting. First, they use spear-phishing e-mails and zero-day exploits to infiltrate organizations from different sectors, including Defense Industrial Base (DIB), government and Non-Governmental Organizations (NGOs). Second, they spread malware indiscriminately via Japanese P2P (peer-to-peer) file-sharing sites. Third, they specifically target business executives who are traveling overseas and staying at hotels in a number of countries: using a two-step infection process, the attackers first identify their victims and then download further malware to the computers of more significant targets, designed to steal confidential data from the infected computer.

OUR HOMES AND OTHER VULNERABILITIES

Exploiting unpatched vulnerabilities remains one of the key mechanisms used by cybercriminals to install malicious code on victims' computers. This relies on the existence of vulnerabilities in widely-used software and the failure of individuals or businesses to patch applications.

This year vulnerabilities were discovered in two widely-used open source protocols, known as 'Heartbleed' and 'Shellshock' respectively. Heartbleed, a flaw in the OpenSSL encryption protocol, lets an attacker read the contents of the memory, and intercept personal data, on systems using vulnerable versions of the protocol. OpenSSL is widely-used to secure Internet-based communications, including web, e-mail, instant messaging and Virtual Private Networks (VPN), so the potential impact of this vulnerability was huge. As often happens when there's a risk that personal data might have been exposed, there was a rush to change passwords. Of course, this could only be effective once an online provider had taken steps to patch OpenSSL and thereby secure their systems – otherwise any new password would be just at risk from attackers trying to exploit the vulnerability. We offered some perspectives on the impact of the flaw two months after its disclosure.

In September, the information security world faced a red alert following the discovery of the Shellshock vulnerability (also known as 'Bash'). The flaw allows an attacker to remotely attach a malicious file to a variable that is executed when the Bash command interpreter is invoked (Bash is the default shell on Linux and Mac OS X systems). The high impact of this vulnerability, coupled with the ease with which it could be exploited, caused considerable concern. Many people compared it to Heartbleed. However, unlike Heartbleed, Shellshock provided full system control – not just the ability to steal data from the memory. It didn't take long for attackers to try and take advantage of the vulnerability – we discussed some early examples soon after it was discovered. In most cases attackers remotely attacked web servers hosting CGI (Common Gateway Interface) scripts that have been written in Bash or pass values to shell scripts. However, it remains possible that the vulnerability could have an impact on a Windows-based infrastructure. Unfortunately, the problem wasn't confined only to web servers. Bash is widely used in the firmware of devices that now take for granted in our everyday lives. This includes routers, home appliances and wireless access points. Some of these devices can be difficult or impossible to patch.

The Internet is becoming woven into the fabric of our lives – literally, in some cases, as connectivity is embedded into everyday objects. This trend, known as the 'Internet of Things', has attracted more and more attention. It can

seem very futuristic, but the Internet of Things is actually closer than you may think. The modern home today is likely to have a handful of devices connected to the local network that aren't traditional computers – devices such as a smart TV, a printer, a games console, a network storage device or some kind of media player/satellite receiver.

One of our security researchers investigated his own home, to determine whether it was really cyber-secure. He looked at several pieces of household kit, including network-attached storage (NAS) devices, smart TV, router and satellite receiver, to see if they were vulnerable to attack. The results were striking. He found 14 vulnerabilities in the network-attached storage devices, one in the smart TV and several potentially hidden remote control functions in the router. You can read the full details here. It's important that we all understand the potential risks associated with using network devices – this applies to individuals and businesses alike. We also need to understand that our information is not secure just because we use strong passwords or run software to protect against malicious code. There are many things over which we have no control, and to some degree we are in the hands of software and hardware vendors. For example, not all devices include automated update checks – sometimes consumers are required to download and install new firmware. This is not always an easy task. Worse still, it's not always possible to update a device (most devices investigated during this research had been discontinued more than a year before).

THE CONTINUING EXPONENTIAL GROWTH OF MOBILE MALWARE

We have seen dramatic growth in the numbers of mobile malware in recent years. In the period from 2004-13 we analyzed almost 200,000 mobile malware code samples. In 2014 alone we analyzed a further 295,539 samples. However, this doesn't give the whole picture. These code samples are re-used and re-packaged: in 2014 we saw 4,643,582 mobile malware installation packs (on top of the 10,000,000 installation packs we had seen in the period 2004-13). The number of mobile malware attacks per month increased tenfold – from 69,000 per month in August 2013 to 644,000 in March 2014 (see Mobile Cyber Threats, Kaspersky Lab and INTERPOL Joint Report, October 2014).

53 per cent of all mobile malware detections are now related to malware capable of stealing money. One of the more notable examples is Spveng, designed to steal money from customers of three of Russia's biggest banks. The Trojan waits until a customer opens an online banking app and replaces it with its own, to try and obtain the customer's login details. It also tries to steal credit card data by displaying its own window over the Google Play app and asking for card details. Another is Waller which, in addition to behaving like a typical SMS Trojan, steals money from QIWI wallets on infected devices.

Cybercriminals have also diversified their efforts to make money from their victims, using methods that have been well-established on desktops and laptops. This includes ransomware Trojans. Fake anti-virus apps are another example of an established approach now being applied to mobile devices. Finally, this year saw the appearance of the first Trojan that is managed through a C2 server hosted in the Tor network. The Torec backdoor is a modification of the commonly-used Tor client, Orbot. The benefit, of course, is that the C2 server can't be shut down.

Until recently, nearly all malware targeting iOS was designed to exploit 'jailbroken' devices.

However, the recent appearance of the 'WireLurker' malware has shown that iOS is not immune from attack.

Mobile devices are now integrated into the fabric of our lives, so it's hardly surprising that the development of mobile malware is underpinned by a cybercrime business that includes malware writers, testers, app designers, web developers and botnet managers.

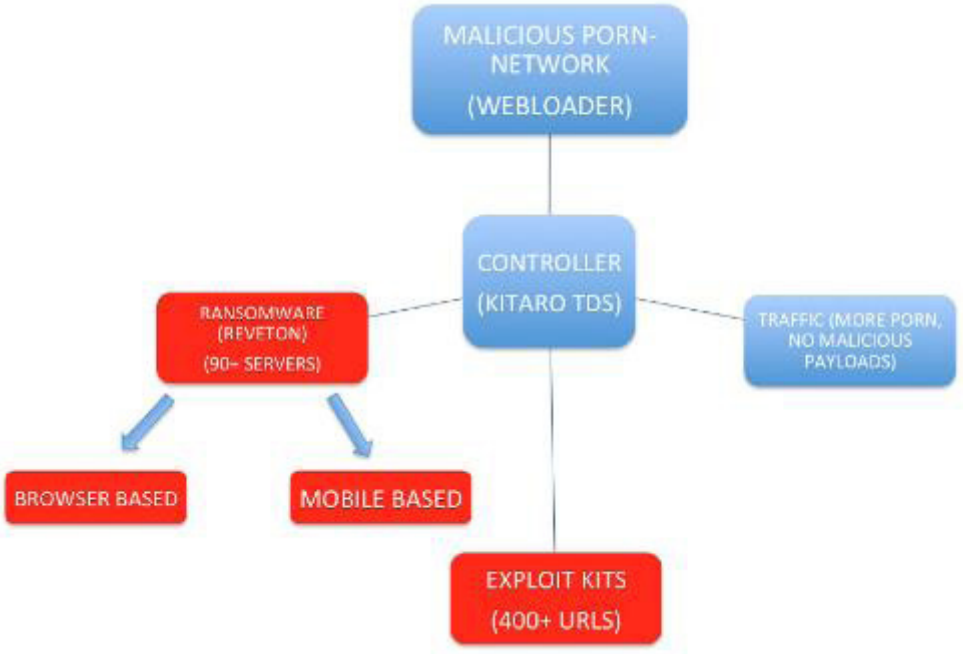
YOUR MONEY OR YOUR FILE(S)

The number of ransomware programs has been growing in recent years. Some simply block access to the victim's computer and demand a ransom payment in order to restore normal access. But many go further than this, encrypting data on the computer. One recent example is 'ZeroLocker'. ZeroLocker encrypts nearly all the files on the victim's computer and adds the extension '.encrypt' to encrypted files (although it doesn't encrypt files located in directories containing the words 'Windows', 'WINDOWS', 'Program Files', 'ZeroLocker' or 'Destroy' and doesn't encrypt files larger than 20MB in size). The Trojan uses a 160-bit AES key to encrypt files. Once the files are encrypted, it runs the 'cipher.exe' utility to remove all unused data from the drive. Both these things make file recovery very difficult. The cybercriminals behind ZeroLocker demand an initial $300 worth of Bitcoins to decrypt the file. If the victim does not pay promptly the fee increases to $500 and $1,000 as time goes on.

Another ransomware program that we analyzed this year is Onion. Not only does this Trojan use the Tor network to hide its C2 servers, but it also supports full interaction with Tor without any input from the victim. Other programs like this communicate with the Tor network by launching (sometimes by injecting code into other processes) the legitimate 'tor.exe' file. By contrast Onion implements this communication as part of the malware code itself. Onion also uses an unorthodox cryptographic algorithm that makes file decryption impossible, even if traffic between the Trojan and the C2 server is intercepted. This Trojan not only uses asymmetric encryption, it also uses a cryptographic protocol known as ECDH (Elliptic Curve Diffie-Hellman). This makes decryption impossible without the master private key – which never leaves the cybercriminals' controlled server.

This year the use of ransomware programs has been extended to devices running Android. The first version of Svpeng, for example, discovered early in 2014, blocks the phone, claiming that the victim was viewing child pornography and demanding a 'fine' of $500 to unlock the phone. A subsequent modification of this malware, discovered in June 2014, completely blocks the device, so that it can only be turned off by pressing down the 'Off' button for a long time – and the Trojan loads again as soon as the device has been switched on again. This version was aimed mainly at victims in the US, but we also saw victims in the UK, Switzerland, Germany, India and Russia. This version demands a payment of $200 to unblock the phone, payment to be made using MoneyPak vouchers. The ransom demand screen displays a photograph of the victim, taken using the frontal camera. Another Trojan, called 'Koler', discovered in May 2014, uses the same approach – blocking

access to the device and demanding a ransom payment of between $100 and $300 to unblock the phone. Like Svpeng, this Trojan displays a message claiming to be from the police – it targets victims in more than 30 countries around the world, using local 'police' messages.



Koler's distribution infrastructure

The first Android Trojan to encrypt data, called 'Pletor', appeared in May 2014. This Trojan uses the AES encryption algorithm to encrypt the contents of the phone's memory card and then displays a ransom demand on the screen, payable using the victim's QIWI Visa wallet, MoneXy or standard transfer of money to a telephone number. This Trojan mainly targets victims in Russia and Ukraine (although we have seen victims in other former Soviet republics) and demands the equivalent of around $300 in rubles or hryvnia.

Ransomware operations rely on their victims paying up. Don't do it! Instead, make regular backups of your data. That way, if you ever fall victim to a ransomware program (or a hardware problem that stops you accessing your files) you will not lose any of your data.

5

CHA-CHING! USING MALWARE TO GET MONEY FROM ATMS

Malware for ATMs is not new. The first malware of this kind, called 'Skimer', was found in 2009 – this targeted ATMs in Eastern Europe running a Windows-based operating system. This used undocumented functions to print details of cards inserted in the infected machine and to open cassettes using a master card command. We saw further ATM malware in Brazil, in 2010 ('SPSniffer'): this collected PIN numbers in outdated ATMs using PIN pads that weren't using strong cryptographic protection. Then last year we saw a further family of ATM malware ('Atmer'), designed to steal money from ATMs in Mexico.

This year, at the request of a financial institution, we carried out a forensic investigation into a new attack on ATMs in Asia, Europe and Latin America. The operation was in two stages. The cybercriminals gain physical access to the ATMs and use a bootable CD to install the malware, called 'Tyupkin'; then they reboot the machine to load the malware, putting them in control of the ATM. The malware then runs in an infinite loop, waiting for a command.

To make the scam less obvious, the malware only accepts commands at specific times on Sunday and Monday nights. The attackers can then enter a combination of digits on the ATM keyboard, make a call to the malware operators, enter a further set of numbers and then collect the cash dispensed by the ATM.

Video Footage obtained from security cameras at the infected ATMs showed the methodology used to access cash from the machines. A unique digit combination key based on random numbers is freshly generated for every session: this ensures that no one outside the gang can accidentally profit from the fraud. Then the malicious operator receives instructions by phone from another member of the gang who knows the algorithm and is able to generate a session key based on the number shown: this ensures that the mules collecting the cash do not try to go it alone. When the correct key is entered, the ATM shows how much money is available in each cash cassette, inviting the operator to choose which cassette to rob. Then it dispenses 40 bank notes at a time from the chosen cassette.

The upswing in ATM attacks in recent years is a natural evolution from the more well-established method of using physical skimmers to capture data from cards used in ATMs that have been tampered with. Unfortunately, many ATMs run operating systems with known security weaknesses. This makes physical security even more important; and we would urge all banks to review the physical security of their ATMs.

WINDOWS XP: FORGOTTEN BUT NOT GONE?

Support for Windows XP ended on 8 April: this means no new security updates, no security hotfixes, free or paid assisted support options or online technical content updates. Sadly, there are still a lot of people running Windows XP – our data suggests that Windows XP accounts for around 18 per cent of infections. This is a lot of people wide open to attack now that security patches have dried up. Effectively, every vulnerability discovered since April is a zero-day vulnerability – that is, one for which there is no chance of a patch. This problem will be compounded as application vendors stop developing updates for Windows XP. Every unpatched application will become yet another potential point of compromise, further increasing the potential attack surface. In fact, this process has already started: the latest version of Java no longer supports Windows XP.

It might seem that the simple and obvious solution is to upgrade to a newer operating system. But even though Microsoft gave plenty of notice about the end of support, it's not difficult to see why migration to a new operating system might be difficult for some businesses. On top of the cost of switching, it may also mean investing in new hardware and even trying to replace a bespoke application developed specifically for the company – one that will not run on a later operating system. So it's no surprise see some organizations paying for continued XP support.

Of course, an anti-virus product will provide protection. But this only holds good if by 'anti-virus' we mean a comprehensive Internet security product that makes use of proactive technology to defend against new, unknown threats – in particular, functionality to prevent the use of exploits. A basic anti-virus product, based largely on signature-based scanning for known malware, is insufficient. Remember too that, as times goes by, security vendors will implement new protection technologies that may well not be Windows XP-compatible.

Anyone still running Windows XP should see this as a stop-gap, while they finalize a migration strategy. Malware writers will undoubtedly target Windows XP while significant numbers of people continue to run it, since an unpatched operating system will offer them a much bigger window of opportunity. Any Windows XP-based computer on a network offers a weak point that can be exploited in a targeted attack on the company – if compromised this will become a stepping-stone into the wider network.

There's no question that switching to a newer operating system is inconvenient and costly - for individuals and businesses. But the potential risk of using an increasingly insecure operating system is likely to outweigh the inconvenience and cost.

BENEATH THE LAYERS OF THE ONION

Tor (short for The Onion Router) is software designed to allow someone to remain anonymous when accessing the Internet. It has been around for some time, but for many years was used mainly by experts and enthusiasts. However, use of the Tor network has spiked this year, in large part because of growing concerns about privacy. Tor has become a helpful solution for those who, for any reason, fear surveillance and the leakage of confidential information. However, our investigations highlighted the fact that Tor is also attractive for cybercriminals, who value the anonymity it offers.

We started seeing cybercriminals actively using Tor to host their malicious infrastructure in 2013. In addition to malware, we found many related resources, including C2 servers, administration panels and more. By hosting their servers in the Tor network, cybercriminals make them harder to identify, blacklist and eliminate. There's also a Tor-based underground marketplace, including the buying and selling of malware and stolen personal data – typically paid for using the crypto-currency Bitcoin, enabling cybercriminals to remain untraceable. Tor allows cybercriminals to conceal the operation of the malware they use, to trade in cybercrime services and launder their illegal profits.

In July we published our analysis of a ransomware Trojan, called 'Onion' that broke new ground in its use of Tor.

Developers of Android-based malware have also started to use Tor. The Torec Trojan, a malware variation of the popular Orbot Tor client, uses a domain in the .onion pseudo zone as a C2 server. Some modifications of the Pletor ransomware Trojan also use the Tor network to communicate with the cybercriminals managing the scam.

Cybercriminals can't always operate with impunity, despite using Tor, as demonstrated by the recent global law enforcement operation against a number of Tor-based cybercrime services ('Operation Onymous').

This begs the question of how the police agencies involved were able to compromise a supposedly 'impenetrable' network – because, in theory at least, there's no way of knowing the physical location of a web server behind a hidden service that someone visits. However, there are ways to compromise a hidden service that don't involve attacking the Tor architecture itself, as we discussed here. A Tor-based service can only remain secure if it's properly configured, if it's free from vulnerabilities or configuration errors and the web application doesn't have any flaws.

THE GOOD, THE BAD AND THE UGLY

Unfortunately, software isn't neatly divided between good and bad programs. There's always the risk that software developed for legitimate purposes might be misused by cybercriminals. At the Kaspersky Security Analyst Summit 2014 in February we outlined how improper implementation of anti-theft technologies residing in the firmware of commonly used laptops and some desktop computers could become a powerful weapon in the hands of cybercriminals. Our research started when a Kaspersky Lab employee experienced repeated system process crashes on one of his personal laptops, related to instability in modules belonging to the Computrace software developed by Absolute Software. Our colleague hadn't installed the software and didn't even know it was present on the laptop. This caused us concern because, according to an Absolute Software white paper, the installation should be done by the owner of the computer or their IT service. On top of this, while most pre-installed software can be permanently removed or disabled by the owner of the computer, Computrace is designed to survive a professional system cleanup and even a hard disk replacement. Moreover, we couldn't simply dismiss this as a one-off occurrence because we found similar indications of Computrace software running on personal computers belonging to some of our researchers and some enterprise computers. As a result, we decided to carry out an in-depth analysis.

When we first looked at Computrace, we mistakenly thought it was malicious software, because it uses so many tricks that are popular in current malware. Indeed, in the past this software has been detected as malware although at present most anti-malware companies whitelist Computrace executables.

We believe that Computrace was designed with good intentions. However, our research shows that vulnerabilities in the software could allow cybercriminals to misuse it. In our view, strong authentication and encryption must be built into such a powerful tool. We found no evidence that Computrace modules had been secretly activated on the computers we analyzed. But it's clear that there are a lot of computers with activated Computrace agents. We believe that it's the responsibility of manufacturers, and Absolute Software, to notify these people and explain how they can deactivate the software if they don't wish to use it. Otherwise, these orphaned agents will continue to run unnoticed and will provide opportunities for remote exploitation.

In June, we published the results of our research into a piece of 'legal' software called Remote Control System (RCS) developed by the Italian company HackingTeam. We discovered a feature that can be used to fingerprint its C2 servers. This allowed us to scan the entire IPv4 space and find all the IP addresses of RCS C2 servers across the globe. We found 326 in total, the greatest number of them located in the US, Kazakhstan and Ecuador. Several IPs were identified as 'government'-related, based on their WHOIS information. Of course, we can't be sure that the servers located in a specific country are being used by law enforcement agencies in that country, but this would make sense: after all, it would avoid cross-border legal problems and avoid the risk of servers being seized by others. We also found a number of mobile malware modules coming from HackingTeam, for Android, iOS, Windows Mobile and BlackBerry. They are all controlled using the same configuration type – a good indication that they are related and belong to the same product family. Unsurprisingly, we were particularly interested in those relating to Android and iOS, because of the popularity of those platforms.

The modules are installed using infectors – special executables for either Windows or Mac OS that run on already-infected computers. The iOS module supports only 'jailbroken' devices. This does limit its ability to spread, but the method of infection used by RCS means that an attacker can run a jailbreaking tool (such as Evasi0n) from the infected computer to which the phone is connected – as long as the device isn't locked. The iOS module allows an attacker to access data on the device (including e-mail, contacts, call history, cached web pages), to secretly activate the microphone and to take regular camera shots. This gives complete control over the whole environment in and around a victim's computer.

The Android module is protected by the DexGuard optimizer/obfuscator, so it was difficult to analyze. But we were able to determine that it matches the functionality of the iOS module, plus offering support for hijacking information from the following applications: 'com.tencent.mm', 'com,google,android,gm', 'android,calendar', 'com,facebook', 'jp,naver,line,android' and 'com,google.android,talk'.

This new data highlighted the sophistication of such surveillance tools. Our policy in relation to such tools is very clear. We seek to detect and remediate any malware attack, regardless of its origin or purpose. For us, there's no such thing as 'right' or 'wrong' malware; and we've issued public warnings about the risks of so-called 'legal' spyware in the past. It's imperative that these surveillance tools don't fall into the wrong hands – that's why the IT security industry can't make exceptions when it comes to detecting malware.

PRIVACY AND SECURITY

The ongoing tension between privacy and security has continued to make headlines.

Among the usual steady stream of security breaches this year, it's not really surprising that the incident that attracted most attention was the theft and subsequent publication of explicit photographs of various Hollywood celebrities. This story highlights the dual responsibility of providers and individuals in securing data stored online. It seems that the theft was made possible by a loophole in iCloud security: the 'Find My iPhone' interface lacked any limitation on the number of password attempts, allowing attackers to brute-force the passwords of the victims. Apple closed up this loophole soon afterwards. However, the attack would not have been possible had the victims not used weak passwords. We increasingly live our lives online. But many of us fail to consider the implications of storing personal data online. The security of a cloud service depends on the provider. The moment we entrust our data to a third-party service, we automatically lose some control over it. It's important to cherry-pick the data we store in the cloud and decide what data is automatically moved from our devices to the cloud.

The issue of passwords is one that keeps surfacing. If we choose a password that is too easy to guess, we leave ourselves wide open to identify theft. The problem is compounded if we recycle the same password across multiple online accounts – if one account is compromised, they're all at risk! This is why many providers, including Apple, Google and Microsoft, now offer two-factor authentication – i.e. requiring customers to enter a code generated by a hardware token, or one sent to a mobile device, in order to access a site, or at least in order to make changes to account settings. Two-factor authentication certainly enhances security – but only if it's required, rather than just being an option.

There's always a trade-off between security and ease of use. In an effort to strike this balance, Twitter recently launched its Digits service. Customers no longer need to create a username and password combination in order to sign in to an app. Instead, they simply enter their phone number. They receive a one-time passcode to confirm each transaction – this code is read automatically by the app. Twitter is effectively making itself a go-between, verifying the identity of the customer for the app provider. There are several benefits. Consumers no longer have to worry about creating a login and password combination to set up an account with an app provider; and they don't need to have an e-mail address. App developers don't need to create their own framework for verifying logins; and they won't lose potential customers

who don't use e-mail. Twitter gets more visibility into what its customers are interested in. In addition, the fact that no passwords are stored on the app provider's server is also a plus: a breach of an app provider's server will not result in the loss of personal data belonging to customers. However, if someone loses their device, or if it's stolen, the number verification will still work – and anyone with access to the device will be able to access an app in the same way as the legitimate owner. That said, it doesn't represent a step backwards in security compared to the traditional username and password method. Currently, mobile apps don't force a login each time an app is run anyway, so if someone steals a phone, and the owner isn't using a PIN, passcode or fingerprint, the thief has access to everything – e-mail, social networks and apps. In other words, security is dependent on a single-point-of-failure – the PIN, passcode or fingerprint used to access the device itself.

In response to increasing concerns about privacy, the developers of the 'pwnedlist.com' web site created an easy to use interface where people can check to see if their e-mail addresses and passwords have been stolen and published online. This year they have made this a chargeable service.

The response of both Apple and Google to growing fears about loss of privacy was to enable default encryption of data on iOS and Android devices, something that some law enforcement agencies believe plays into the hands of cybercriminals – making it easier for them to evade detection.

INTERNATIONAL LAW ENFORCEMENT: CO-OPERATION BRINGS RESULTS

Cybercrime has become an established part of life, on the back of the ever-increasing online activities we engage in. It's tempting to imaging that cybercriminals are able to operate with impunity, but the actions of law enforcement agencies can have a significant impact on their activities. International co-operation is particularly important, given the global nature of cybercrime. This year there have been some notable police successes.

In June 2014 an operation involving law enforcement agencies of several countries, including the UK's NCA (National Crime Agency) and the FBI, was able to take down the global network of computers responsible for managing the 'GameoverZeus' botnet. The police operation ('Operation Tovar') disrupted the communications underlying the botnet, thereby preventing the cybercriminals from controlling it. GameoverZeus was one of the largest operating botnets based on the code of the Zeus banking Trojan. In addition to infecting computers with the Zeus Trojan and stealing login credentials for online e-mail accounts, social networks, online banking and other online financial services, the botnet also distributed the 'Cryptolocker' ransomware program. The police campaign offered victims a breathing-space in which to clean their computers.

Earlier this year Kaspersky Lab contributed to an alliance of law enforcement and industry organizations, co-ordinated by the NCA, to disrupt the infrastructure behind the 'Shylock' Trojan. The Shylock banking Trojan, so-called because its code contains excerpts from Shakespeare's The Merchant of Venice, was first discovered in 2011. Like other well-known banking Trojans Shylock is a man-in-the-browser attack designed to steal banking login credentials from the computers of bank customers. The Trojan uses a pre-configured list of target banks, located in different countries around the world.

In November, Operation Onymous resulted in the take-down of dark markets running within the Tor network.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy