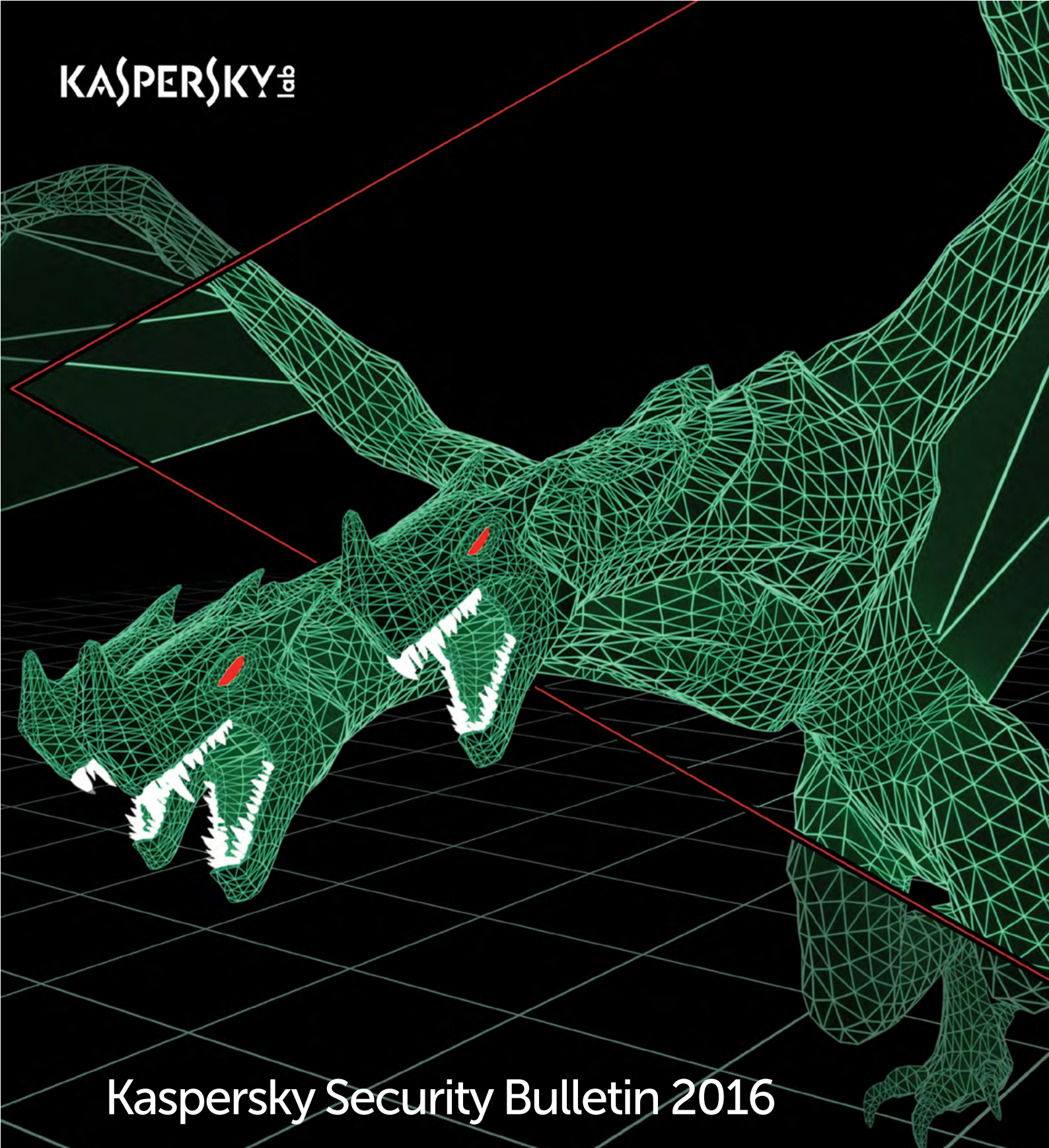
KASPERSKY lab



Kaspersky Security Bulletin 2016

REVIEW OF THE YEAR

David Emm, Roman Unuchek, Kirill Kruglov

GREAT

CONTENTS

TARGETED ATTACKS

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

Here are the major APT campaigns that we reported this year.

BlackEnergy

In one massive attack, BlackEnergy disabled power distribution, wiped software and launched a DDoS

The year started with the developing picture of the BlackEnergy cyber-attack on the Ukrainian energy sector. This attack was unique because of the damage it caused: hackers managed to disable the power distribution system in Western Ukraine, launch a wiper program on targeted systems and conduct a telephone Distributed Denial of Service (DDoS) attack on the technical support services of the affected companies. Kaspersky Lab experts revealed several aspects of the activities of the group responsible for the attack: in particular, an analysis of the tool used to penetrate the target systems. For an overview of the attack, read the report prepared by the SANS Institute and ICS-CERT.

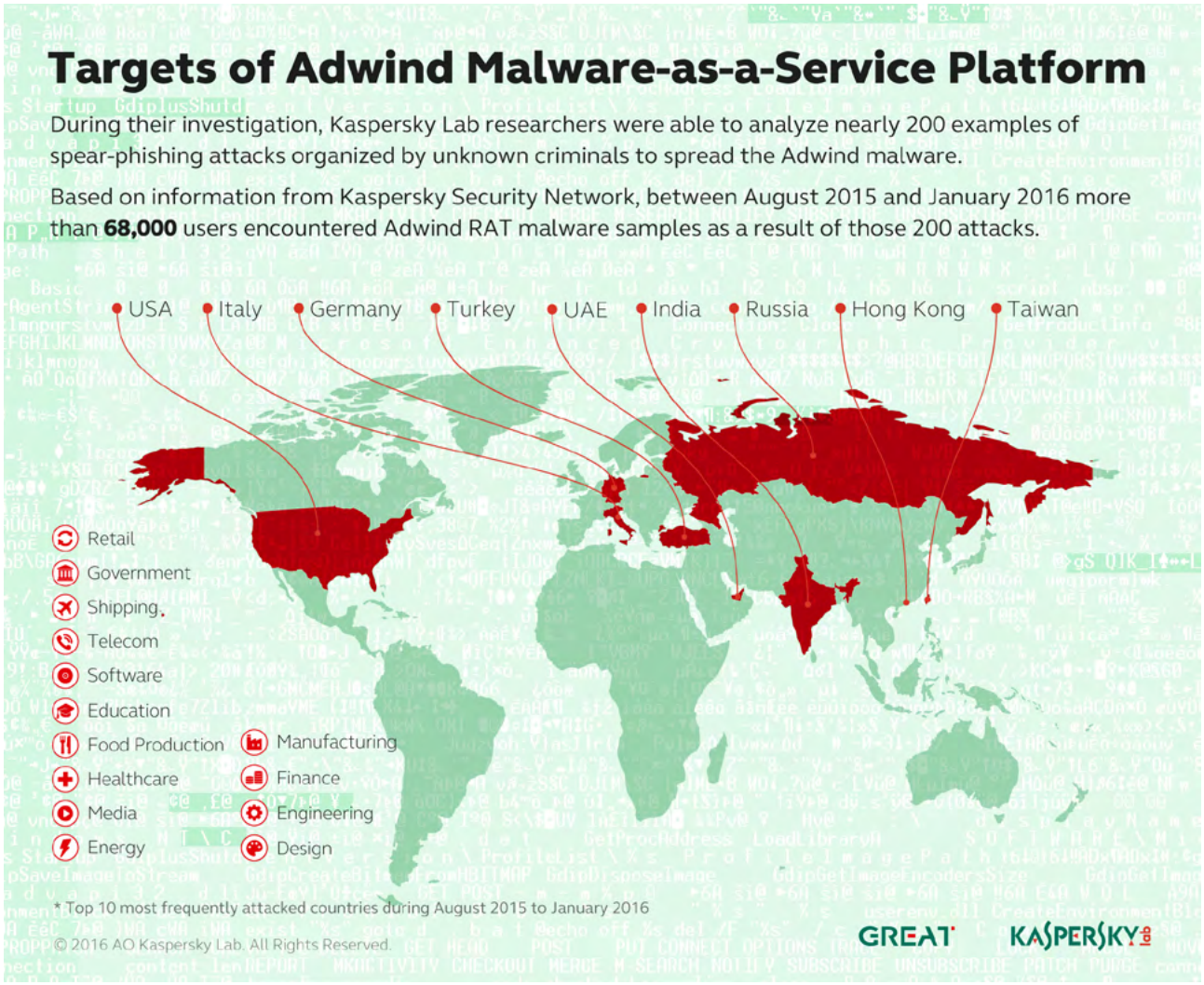
Operation Blockbuster

Kaspersky Lab was among the participants in Operation Blockbuster, a joint investigation conducted by several major IT security companies into the activities of the Lazarus group (you can read our own report here). Lazarus is a cybercrime gang — supposedly of North Korean origin — responsible for the attack on Sony Pictures in 2014. The group has been around since 2009, although its activities ramped up after 2011. Lazarus is responsible for such well-known attacks as Troy, Dark Seoul (Wiper) and WildPositron. The group targeted companies, financial institutions, radio and television.

Adwind

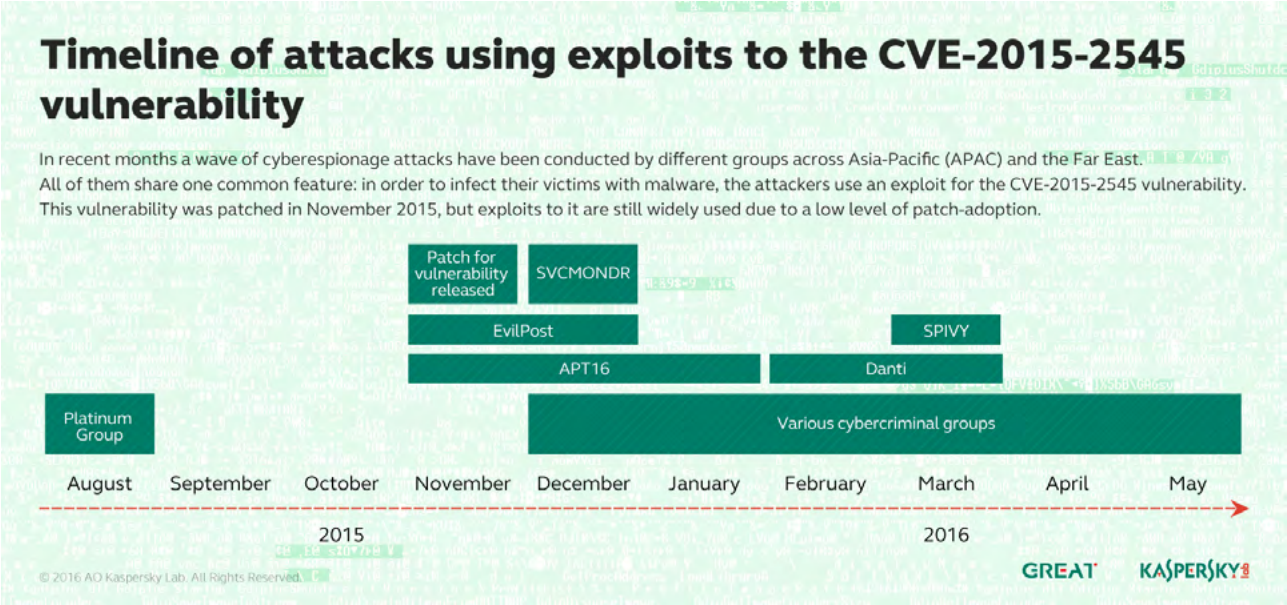
Adwind's malware-for-rent had 1,800 customers

In February, at the Security Analyst Summit, we presented the results of our investigation into Adwind, a cross-platform, multi-functional RAT (Remote Access Tool) distributed through a single Malware-as-a-Platform service. This Trojan has been renamed several times since its first release in 2012 — AlienSpy, Frutas, Unrecom, Sockrat, JSocket and jRat. We believe that between 2013 and 2016 this malware was used in attacks against more than 443,000 individuals, commercial and non-commercial organisations around the world. One of the main features that distinguishes Adwind from other commercial malware is that it is distributed openly as a paid service, where the customer pays a fee in return for use of the malicious software. We estimate that there were around 1,800 customers in the system by the end of 2015. This makes it one of the biggest malware platforms in existence today.



Attacks using exploits to the CVE-2015-2545 vulnerability

In May, we reported a wave of cyber-espionage attacks conducted by different APT groups across the Asia-Pacific and Far East regions. They all shared one common feature: they exploited the CVE-2015-2545 vulnerability. This flaw enables an attacker to execute arbitrary code using a specially-crafted EPS image file. It uses PostScript and can evade the Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) protection methods built into Windows. The Platinum, APT16, EvilPost and SPIVY groups were already known to use this exploit. More recently, it was used by the Danti and SVCMONDR groups. You can find an overview of the APTs that use this vulnerability here.



Over six APT groups used the same vulnerability — patched back in 2015

One of the most striking aspects of these attacks is that they are successfully making use of a vulnerability that had been patched by Microsoft in September 2015. In our 2016 predictions, we suggested that APT campaigns would invest less effort in developing sophisticated tools and make greater use of off-the-shelf malware to achieve their goals. This is a case in point: using a known vulnerability, rather than developing a zero-day exploit.

This underlines the need for companies to pay more attention to patch management to secure their IT infrastructure.

Operation Daybreak

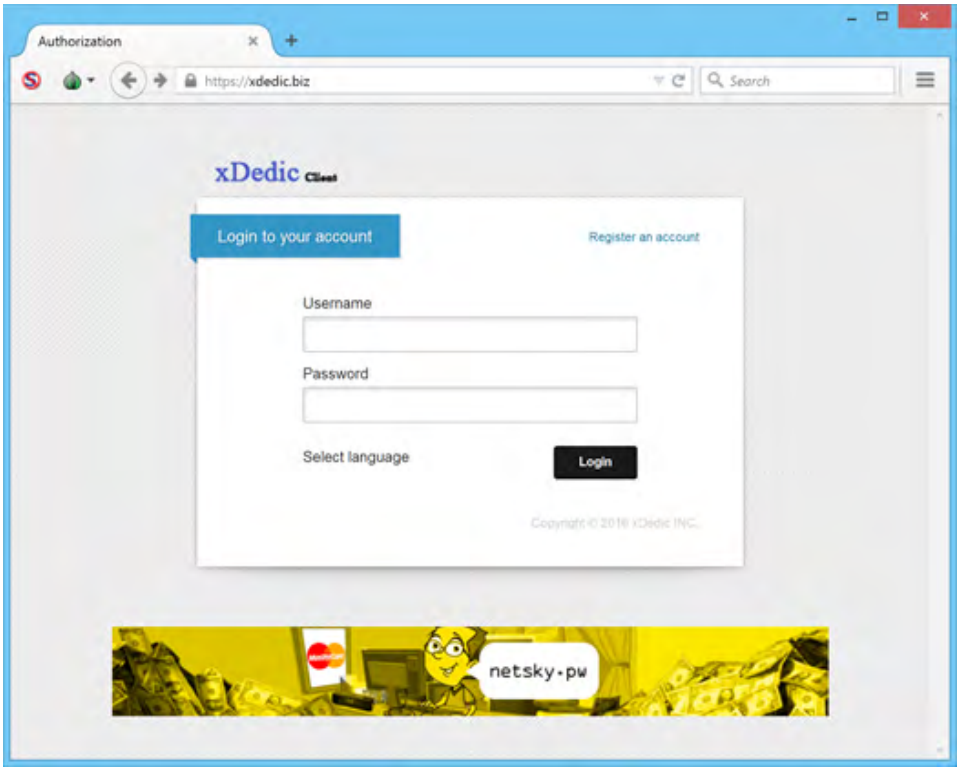
The Operation Daybreak spying campaign by ScarCruft used an unknown zero-day — CVE-2016-1010

Of course, there will always be APT groups that seek to take advantage of zero-day exploits. In June, we reported on a cyber-espionage campaign — code-named Operation Daybreak and launched by a group named ScarCruft — using a previously unknown Adobe Flash Player exploit (CVE-2016-1010). This group is relatively new and has so far managed to stay under the radar. But we think the group might have previously deployed another zero-day exploit (CVE-2016-0147) that was patched in April. The group's targets include an Asian law enforcement agency, one of the world's largest trading companies, a mobile advertising and app monetisation company in the United States, individuals linked to the International Association of Athletics Federations and a restaurant located in one of Dubai's top shopping centres.

While there's no such thing as 100% security, the key is to increase security defences to the point that it becomes so expensive for an attacker to breach them that they give up or choose an alternative target. The best defence against targeted attacks is a multi-layered approach that combines traditional anti-virus technologies with patch management, host intrusion detection and a default-deny whitelisting strategy. According to a study by the Australian Signals Directorate, 85% of targeted attacks analysed could have been stopped by employing four simple mitigation strategies: application whitelisting, updating applications, updating operating systems and restricting administrative privileges.

xDedic

This year, Kaspersky Lab investigated an active cybercriminal trading platform, called xDedic, an online black market for hacked server credentials around the world — all available through the Remote Desktop Protocol (RDP). We initially thought that this market extended to 70,000 servers, but new data suggests that the xDedic market was much wider — including credentials for 176,000 servers. xDedic includes a search engine, enabling potential buyers to find almost anything — from government and corporate networks — for as little as $8 per server. This low price provides 'customers' with access to data on such servers and their use as a bridgehead for further targeted attacks.



xDedic was the marketplace for at least 70,000 hacked servers — most victims had no idea

The existence of off-the-shelf underground markets is not new. But we are seeing a greater level of specialisation. And while the model adopted by the xDedic owners isn't something that can be replicated easily, we think it's likely that other specialised markets will appear in the future.

Dropping Elephant

Dropping Elephant showed the fearsome power of high quality social engineering

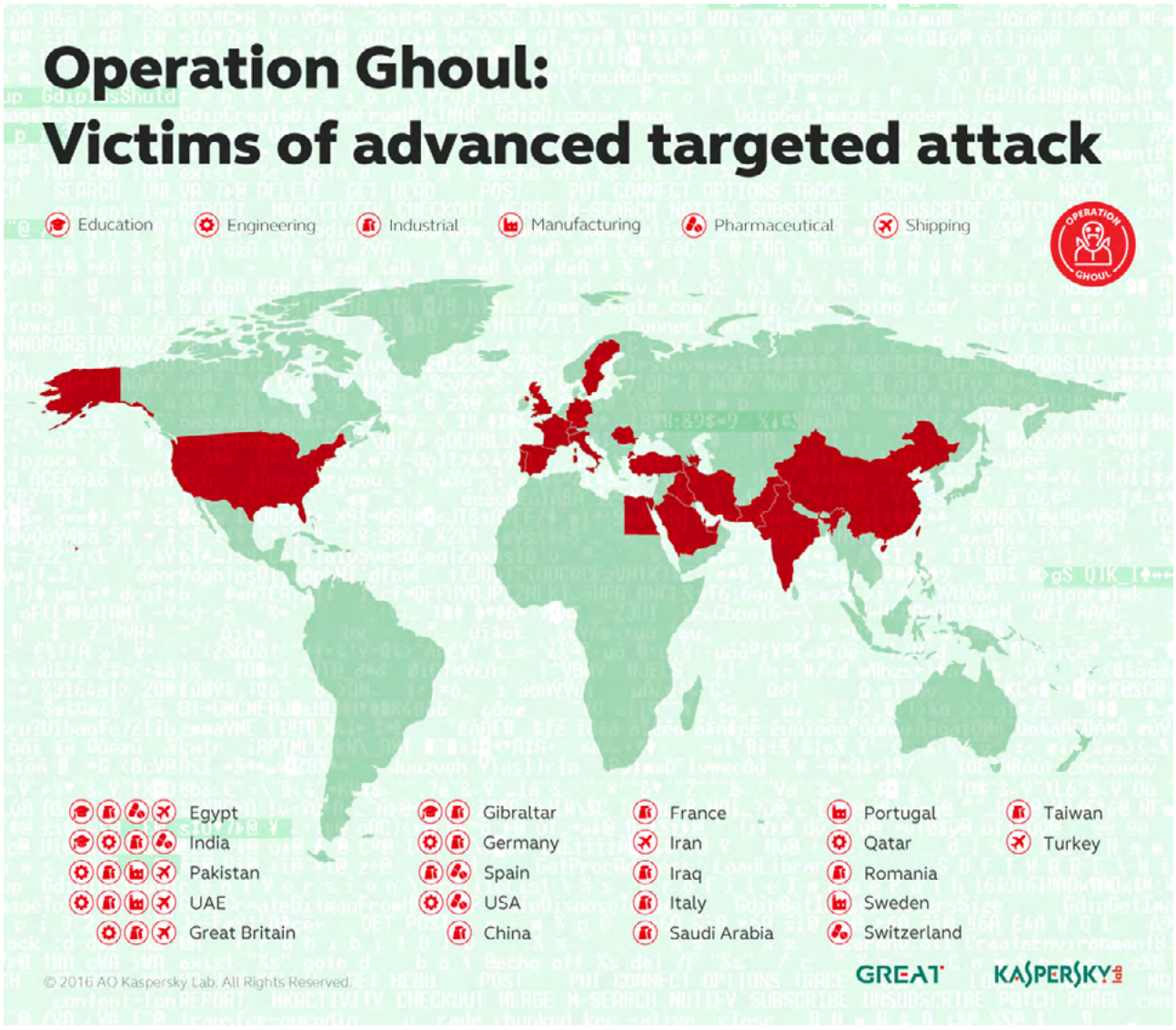
Targeted attack campaigns don't need to be technically advanced in order to be successful. In July, we reported on a group called Dropping Elephant (also known as 'Chinastrats' and 'Patchwork'). Using a combination of social engineering, old exploit code and some PowerShell-based malware this group was able to steal sensitive data from its victims — high-profile diplomatic and economic organisations linked to China's foreign relations. The attackers use a combination of spear-phishing e-mails and watering-hole attacks. The success of the Dropping Elephant group is striking given that no zero-day exploits or advanced techniques were used to target high-profile victims. In fact, Dropping Elephant provides a clear example of how low investment and use of ready-made toolsets can be very effective when combined with high quality social engineering.

The success of such attacks cen be prevented by applying security updates and improving the security awareness of staff.

Operation Ghoul

Operation Ghoul confirmed that power — with precision-targeted phishing followed by commercial malware

The success of social engineering as a means for attackers to gain a foothold in a target organisation was also evident in Operation Ghoul — the group behind a series of attacks that we reported in June 2016. The attackers sent spear-phishing e-mails with malicious attachments — mainly to top and middle level managers of numerous companies — that appeared to come from a bank in the UAE. The messages claimed to offer payment advice from the bank and included an attached SWIFT document. But the archive really contained malware. Based on information obtained from the sink-hole of some command and control (C2) servers, the majority of the target organisations work in the industrial and engineering sectors. Others include shipping, pharmaceutical, manufacturing, trading and educational organisations.



The malware used by the Operation Ghoul group is based on the commercial spyware kit Hawkeye, sold openly on the Dark Web. Once installed, the malware collects interesting data from the victim's computer, including keystrokes, clipboard data, FTP server credentials, account data from browsers, messaging clients, e-mail clients and information about installed applications.

The continued success of social engineering as a way of gaining a foothold in target organisations highlights the need for businesses to make staff awareness and education a central component of their security strategy.

ProjectSauron

In September, we uncovered ProjectSauron, a group that has been stealing confidential data from organisations in Russia, Iran and Rwanda — and probably other countries — since June 2011.

ProjectSauron changed the landscape forever – an advanced modular spying platform with unique tools for each victim

The cost, complexity, persistence and the ultimate goal of the operation (i.e. stealing secret data from state-related organisations) suggest that ProjectSauron is a nation-state sponsored campaign. Technical details indicate that the attackers learned from other highly advanced actors, including Duqu, Flame, Equation and Regin — adopting some of their most innovative techniques and improving on their tactics in order to remain undiscovered. All malicious artefacts are customized for each given target, reducing their value as indicators of compromise for any other victim.

ProjectSauron key features:

1. ProjectSauron is a modular platform designed to enable long-term cyber-espionage campaigns.
2. All modules and network protocols use strong encryption algorithms such as RC6, RC5, RC4, AES, Salsa20, etc.
3. It uses a modified Lua scripting engine to implement the core platform and its plugins.
4. There are upwards of 50 different plugin types.
5. The actor behind ProjectSauron has a high interest in communication encryption software widely used by targeted governmental organizations. It steals encryption keys, configuration files, and IP addresses of the key infrastructure servers related to the encryption software.
6. It is able to exfiltrate data from air-gapped networks by using specially-prepared USB storage drives where data is stored in an area invisible to the operation system.
7. The platform makes extensive use of the DNS protocol for data exfiltration and real-time status reporting.
8. The APT was operational as early as June 2011 and remained active until April 2016.
9. The initial infection vector used to penetrate victim networks remains unknown.
10. The attackers utilize legitimate software distribution channels for lateral movement within infected networks.

The single use of unique methods, such as control server, encryption keys and more, in addition to the adoption of cutting-edge techniques from other major threats groups, is new.

The only effective way to withstand such threats is to deploy multiple layers of security, with sensors to monitor for even the slightest anomaly in organisational workflow, combined with threat intelligence and forensic analysis. You can find further discussion of the methods available to deal with such threats here.

FINANCIAL THREATS

One of the most direct ways for cybercriminals to make money is by targeting bank customers. Typically, attackers use social engineering to trick their victims into disclosing personal information or installing malware that harvests the personal information (e.g. passwords) used by the victim to access their bank account. In 2016, Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **2,871,965** devices.

However, it's not only bank customers that are targeted by cybercriminals. In recent years we've seen a growing number of attacks on banks and other financial institutions. Probably the best known is Carbanak, which used the infiltration techniques typical of a targeted attack to steal money. This year we have seen further attacks on financial institutions.

Metel launched targeted attacks on banks — then sent teams to ATMs at night to withdraw the cash

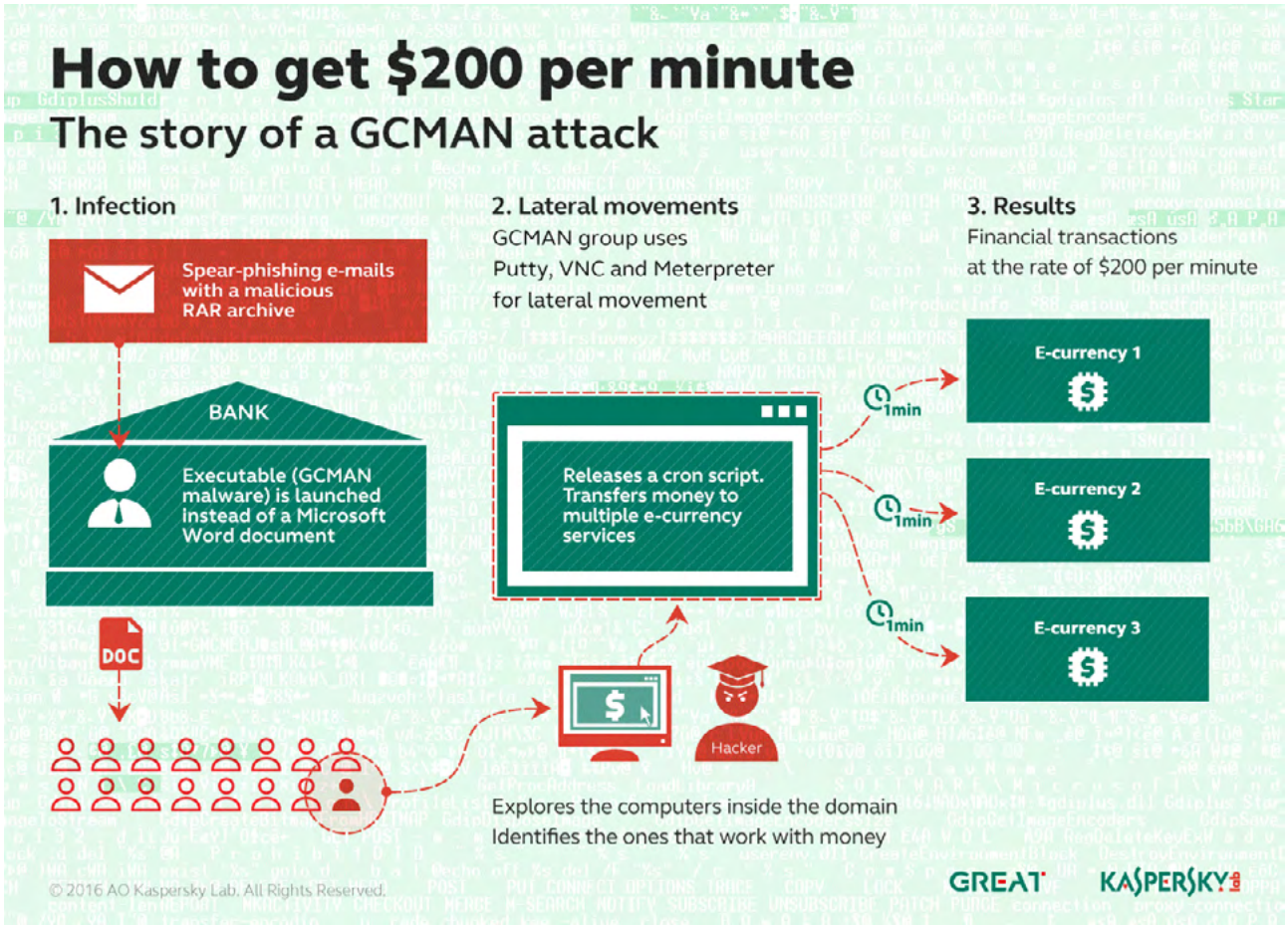
In February 2016, Kaspersky Lab uncovered the activities of other APT groups targeting financial institutions. The group behind Metel used spear-phishing and browser exploits to infiltrate the corporate network of banks and extend their control to key computers within the bank's IT systems. This level of access gave the attackers the ability to automate the roll-back of ATM transactions: gang members were able to use debit cards to steal money from ATMs without affecting the balance on the card — allowing multiple transactions at different ATMs. Our investigations revealed that the attackers drove around in cars in several Russian cities, stealing money from ATMs belonging to different banks. They worked exclusively at night, stealing money at several locations. We discovered Metel in more than 30 financial institutions, although our incident response team was able to clean the infected networks before major damage could be done. However, the cybercriminals behind Metal are still active and we think that the malware is probably much more widespread.

METEL: KEEP CALM AND ROLL BACK THE TRANSACTIONS

*ALL NAMES APPEARING IN THIS CHART ARE FICTITIOUS. ANY RESEMBLANCE IS PURELY COINCIDENTAL.

GCMAN spent 18 months gathering insight from infected victims before attacking – using legitimate tools for lateral movement

GCMAN (so-called because the malware is based on code compiled with the GCC compiler) is another example. The group infiltrates financial institutions using spear-phishing e-mails containing a malicious RAR file. When the archive is opened, an executable file is run that leads to the initial infection. Once the group gains a foothold in the organisation, they use legitimate penetration testing tools, such as Putty, VNC and Meterpreter, to gain lateral movement across the organisation until they find strategic computers that they can use to transfer money to e-currency services. The attackers do this by planting a Cron script in one of the bank's servers (Cron is a time-based scheduler used in Unix-based operating systems) allowing them to complete financial transactions at a rate of $200 per minute. This script is invoked every minute to post new transactions directly to an upstream payment processing system. Fortunately, the financial institutions detected the suspicious activity, and cancelled the transactions: if they hadn't, the attackers would have successfully transferred money to multiple e-currency services without reporting the transactions to any system within the bank. Kaspersky Lab researchers worked with three financial institutions in Russia that were infected with the GCMAN malware. However, we think that this threat is probably much more widespread.



Interestingly, we learned that the real attack had happened around 18 months before the malware was discovered. The group used an SQL injection attack on commercial software running on one of the bank's public web servers, and returned a year and a half later to take advantage of the information they had harvested to infiltrate the bank. Two months before this incident, someone had tried different passwords for an admin account on a bank's server: they were very persistent, but confined their attempts only to Saturdays and allowed themselves only three tries per week — all in an effort to stay under the radar of security teams within the target institutions. The activities of the GCMAN group throw light on an emerging trend within the threat landscape — the use of legitimate tools in preference to bespoke malware modules.

Legitimate tools can be just as effective, trigger fewer false alarms and offer a quicker return on investment for the cybercriminals. It's important that IT security teams take account of this when reviewing their corporate security strategy.

You can read further information about the Metel and GCMAN campaigns here.

Of course, banks don't operate in isolation. International money transfers require an inter-bank network, called SWIFT (Society for Worldwide Interbank Financial Telecommunication).

Following the theft of $100 million many banks were forced to improve their authentication and SWIFT software update procedures

In February 2016, hackers used the SWIFT credentials of Bangladesh Central Bank employees to send fraudulent transaction requests to the Federal Reserve Bank of New York, to transfer millions of dollars to various bank accounts in Asia. The hackers were able to get $81 million transferred to the Rizal Commercial Banking Corporation in the Philippines and an additional $20 million to Pan Asia Banking. The loss would have been much greater if there hadn't been a typo in one of the transfer requests — the hackers misspelled the word 'foundation' as 'fandation'. The Federal Reserve Bank noticed the typo and the Bangladesh Bank was able to stop other transactions worth $850 million. You can read the story here. Further bank attacks using SWIFT credentials have come to light since the theft from the Bangladesh Bank.

The group behind Metel was not the only one targeting ATMs. Malware for ATMs is not new, but the number of such malicious programs has been growing in recent years. The most notable, prior to 2016, was Tyupkin, where the attackers gained physical access to the ATM and inserted a bootable CD to take control of the machine.

In May 2016 we reported a new version of the Skimer ATM malware — this report was the result of an incident response investigation we carried out the previous year. This malware first surfaced in 2009, but has been re-designed — and so too have the tactics of the cybercriminals using it. The new version targets ATMs around the world — we discovered attacks in the UAE, France, the United States, Russia, Macau, China, the Philippines, Spain, Germany, Georgia, Poland, Brazil and the Czech Republic.

Insecure ATMs became a prime target for cyberattack

Rather than the well-established method of fitting a fake card-reader to the ATM, the attackers take control of the whole ATM. They start by installing the Skimer malware on the ATM — either through physical access or by compromising the bank's internal network. The malware infects the ATM's core — the part of the device responsible for interaction with the wider bank infrastructure, card processing and the dispensing of cash. In contrast to a traditional card skimmer, there are no physical signs that the ATM is infected, leaving the attackers free to capture data from cards used at the ATM (including a customer's bank account number and PIN) or to steal cash directly.

The cybercriminal 'wakes up' the infected ATM by inserting a card that contains specific records on the magnetic stripe. After reading the card, Skimer is able to execute a hard-coded command, or receive commands through a special menu activated by the card. The Skimer user interface appears on the display only after the card is ejected and only if the cybercriminal enters the correct session key within 60 seconds. The menu offers 21 different options, including dispensing money, collecting details of cards that have been inserted in the ATM, self-deletion and performing updates. The cybercriminal can save card details on the chip of their card, or print the details it has collected.

The attackers are careful to avoid attracting attention. Rather than take money directly from the ATM — which would be noticed immediately — they wait (sometimes for several months) before taking action. In most cases, they collect data from skimmed cards in order to create cloned cards later. They use the cloned cards in other, non-infected ATMs, casually withdrawing money from the accounts of the victims in a way that can't be linked back to the compromised ATM.

The upswing in ATM attacks in recent years represents 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.

Kaspersky Lab has several recommendations to help banks protect themselves. They should carry out regular anti-virus scans; employ whitelisting technologies; apply a good device management policy; make use of full disk encryption; password protect the BIOS of ATMs; enforce hard disk booting and isolate the ATM network from the rest of the bank infrastructure. One of our experts provided an in-depth examination of ATM jackpotting and offered some insights into what should be done to secure these devices.

New biometric skimmers target next-gen authentication — fingerprint, palm vein, and iris recognition systems

As you would expect, we don't just investigate attacks that have happened: we also look ahead at emerging technologies and how cybercriminals might try to misuse them. We recently published the results of our investigation into potential methods of authentication — including contactless authentication through NFC, one-time passwords and biometrics. You might be surprised to learn that we discovered 12 manufacturers that are already offering fake fingerprint scanners (i.e. biometric skimmers) and at least three other vendors researching devices to allow criminals to obtain data from palm vein and iris recognition systems. You can find the report here.

THE INTERNET OF THINGS

The risk of connecting everything, regardless — in 2016, need we say more?

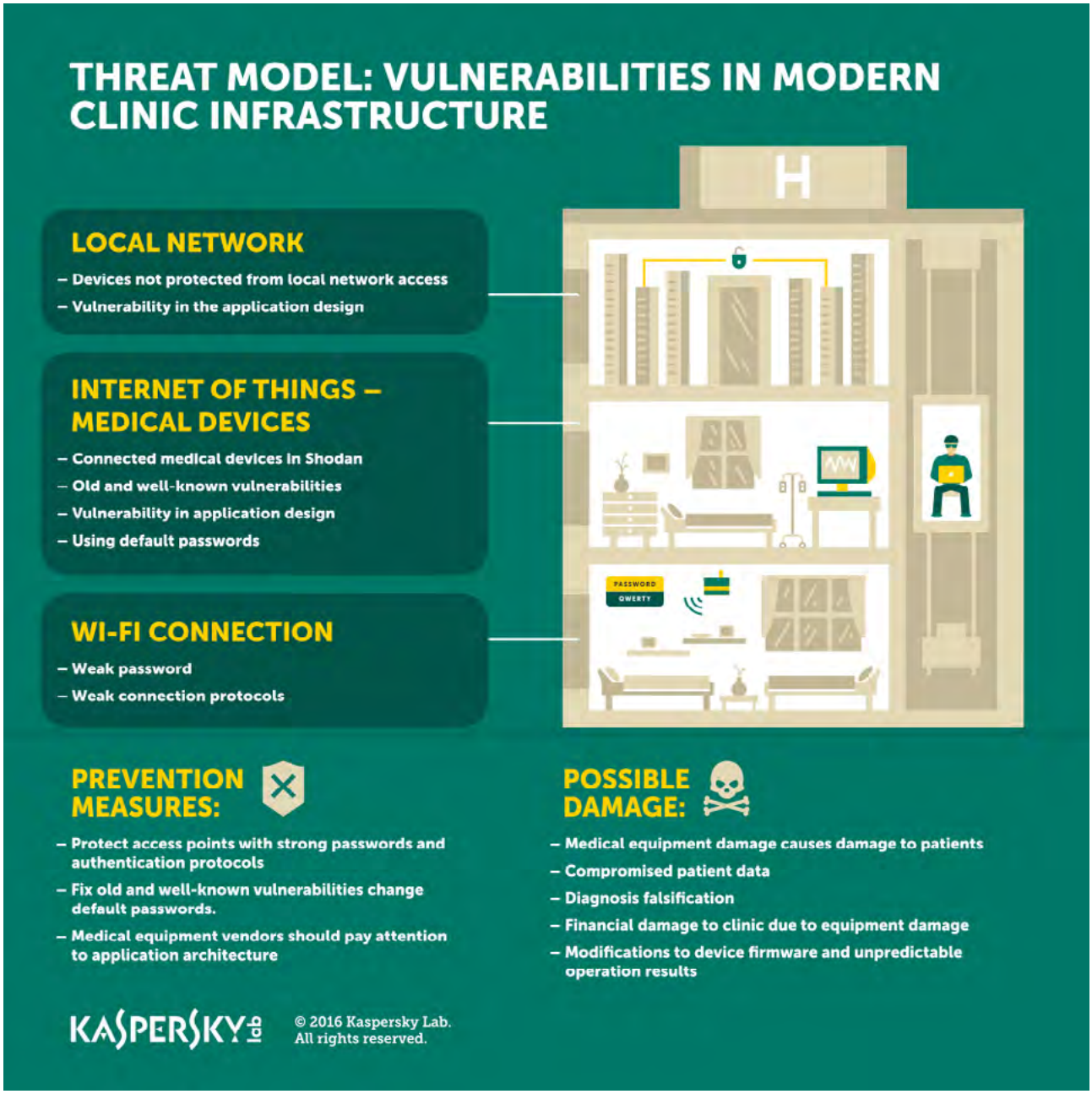
These days we're surrounded by smart devices. A growing number of everyday household objects are now smart — telephones, televisions, thermostats, refrigerators, baby monitors, fitness bracelets and even children's toys. Some homes are even designed with the 'smartness' built-in. But it's not just confined to devices around the home: the list of smart devices also includes cars, medical devices, CCTV cameras and parking meters. Ubiquitous Wi-Fi (if not always as ubiquitous as we would like) brings all these devices online, as part of the Internet of things (IoT).

These things are designed to make our lives easier. Since connected everyday objects are able to collect and transfer data automatically, without human interaction, they can operate more effectively and efficiently. However, a world of connected everyday objects means a bigger attack surface for cybercriminals. Unless IoT devices are secured, the personal data they exchange can be compromised, they can be subject to an attack, or they can be used in an attack.

Unfortunately, security features are hard to sell. Connected devices are created by different vendors — in an open market that makes return on investment critical. In a competitive marketplace, things that make customers' lives easier tend to take precedence. In addition, connectivity is often added to a pre-existing communication network that wasn't created with security in mind. So security is often not considered at the design stage — if at all. Historically, security has often been addressed only after something bad has happened to demonstrate the impact of a security weakness.

In the last few years, researchers have highlighted security issues in various connected devices. You may remember that one of our security researchers investigated his own home, to determine whether it was really cyber-secure. Last year, Charlie Miller and Chris Valasek demonstrated how it was possible to gain wireless access to the critical systems of a Jeep Cherokee — successfully taking control and driving it off the road! Vasilios Hioureas from Kaspersky Lab and Thomas Kinsey from Exigent Systems conducted research into the potential security weaknesses in CCTV systems. More recently a manufacturer withdrew an insulin pump after discovering that there was a risk of an attacker disabling the device or altering the dosage. There have also been concerns about everyday household objects such as children's toys, baby monitors and door-bells.

In February, we showed how easy it was to find a hospital, gain access to its internal network and take control of an MRI device — locating personal data about patients and their treatment procedures and obtaining access to the MRI device file system. Our researcher, Sergey Lozhkin, presented his findings at the Security Analyst Summit this year, highlighting the key factors affecting the security of hospital systems. First, medical devices connected to the Internet were accessible using default passwords. Some were running Windows XP and were susceptible to dozens of old, unpatched vulnerabilities that could be used to compromise hospital systems. Second these medical devices were not segregated from the hospital's local area network. So after obtaining access to one of the hospital's Wi-Fi networks (protected using a weak password), it was possible to get full access to these devices. Third, software architecture vulnerabilities meant that — after connecting to the device and passing through the default login screen — it was possible to access the control interface and personal and diagnostic data about hospital patients. On top of this, there was a command shell implemented in the user interface that provided access to the device's file system. You can read the report here.



Hospitals should take steps to secure their systems:

- Use strong passwords to protect external connection points.
- Update IT security policies, develop vulnerability assessments and patch systems.
- Protect medical equipment applications in the local network with passwords, in case of unauthorized access to a trusted area.
- Protect infrastructure from malware and hacking attacks with a comprehensive security solution.
- Backup critical information regularly and keep an offline copy.

Traffic sensor study showed that 'security-through-obscurity' won't work in a connected world

In April, we published the results of our research into the traffic sensors that have sprung up in Russian cities and elsewhere over the last few years. These sensors can help to enforce speed limits: drivers' speed camera detectors react to the signals emanating from the new sensors in the same way they do to the radar guns used by traffic police. But that's not why the sensors were installed. They collect raw data about traffic on the roads (the number of cars in each lane, average speed, etc.) and pass it on for analysis by the city authorities.

Smart cities are complex open ecoystems that need 'security-by-design'

Our researcher, Denis Legezo, discovered that the data traffic not protected and can be manipulated. There was no authorization, except that required for Bluetooth, and that was not configured properly. The manufacturer of the road sensors we examined is very generous in its support for service engineers, with a lot of information about the devices publicly available on the manufacturer's official web site and elsewhere.

This is a positive thing. 'Security through obscurity' doesn't make a lot of sense: any determined attacker would be able to find out the command system and gain access to the engineering software anyway. So it makes more sense to combine openness, big bounty programs and a fast response to any identified vulnerabilities — if only because the number of researchers will always be bigger than the number of employees in any information security department. You can read the report here.

Most smart city devices hide their OS behind a public interface — but these carry weaknesses that let attackers in

Modern cities are complex eco-systems made up of hundreds of different components — including digital ones. The aim of the smart city is to make life more convenient and safe for citizens. But if something can be used, it can also be abused. In September, we presented the findings of our research into various aspects of the smart city. Our researchers, Denis Makrushin and Vladimir Dashchenko, prepared a report, based on their findings, as part of Kaspersky Lab's support for 'Securing Smart Cities' — an international non-profit initiative created to bring together experts in smart city IT security technologies. Ticket terminals in movie theatres, bike rental terminals, service kiosks in government organizations, booking and information terminals at airports and passenger infotainment terminals in city taxis might all have a different appearance, but inside most of them are the same. Each such terminal is either a Windows-based or an Android-based device. The main difference in comparison to ordinary devices is the special kiosk-mode software that runs on public terminals and serves as the user interface. This software provides easy access to specific features of the terminal whilst at the same time restricting access to other features of the device's operating system, including launching a web browser and then virtual keyboard. Accessing these functions provides an attacker with numerous opportunities to compromise the system, as if he was in front of a PC. The research showed that almost any digital public kiosk contains one or multiple security weaknesses which allow an attacker to access hidden features of the OS. You can read the report here.

More and more aspects of everyday life are being made digital. If security isn't considered at the design stage, the potential dangers could be far-reaching — and retro-fitting security might not be straightforward. For a smart city to be safe for the people who live in it, they need to be treated as information systems whose protection requires a custom approach and expertise.

The Internet was ambushed by kitchen equipment

In October, cybercriminals used a botnet of Internet-connected home devices (such as IP-enabled cameras, DVRs, CCTV cameras and printers) to launch a DDoS attack against Dyn — a company that provides DNS services to Twitter, Amazon, PayPal, Netflix and others. The result was that the web sites of these companies went down or worked only intermittently. The attackers infected vulnerable devices with the Mirai malware. This malware had previously been used in a DDoS attack against the blog site of security researcher Brian Krebs — reputedly the most powerful DDoS attack ever (since the source code for Mirai was recently published online, this doesn't mean that the attack on Dyn was carried out by the same attackers). It's estimated that the Mirai botnet comprises around 550,000 bots. The attackers used default passwords to gain access to online devices. Once the malicious code was written to a device, it became part of the Mirai botnet. As in any DDoS attack, the attackers use the compromised devices to flood their chosen victim's site with traffic, to prevent it operating normally.

This attack, like others that involve compromised IoT devices, exploited the fact that many people don't change the manufacturer's default credentials when they buy a smart device. This makes it easy for attackers to access the device — they simply have to try the known default password. In addition, there are no firmware updates for many devices. IoT devices are also an attractive target for cybercriminals because they often have 24/7 connectivity.

The best advice for anyone using connected/IoT devices at home, is to ensure the default passwords on all devices are changed (using unique, complex passwords) to prevent them being remotely accessed — this includes home routers, which are the gateway to your home network. The temptation may be for people to want to disconnect all devices in the light of such news, but in today's increasingly connected world, that's not realistic; although it's always good to review the functionality of a smart device and disable any functions that you don't actually need. However, good password 'housekeeping' goes a long way to keeping cybercriminals away from your devices. This kind of large scale attack also highlights the need for manufacturers to consider security by design, rather than an afterthought.

MOBILE THREATS

The main mobile threats in 2016 were advertising Trojans able to use root rights on the infected device. Although obtaining superuser rights isn't new for such malware, in 2016 more and more Android Trojans starting using them, because with such rights they can do everything on the device. In order to gain root rights on a device, Trojans have to exploit vulnerabilities in the system. Since many devices aren't regularly updated, they won't receive the fixes for these vulnerabilities. Because of this, we predict a growth in the number and sophistication of Trojans that use root rights.

Recent updates for the Android system contained not just vulnerability fixes but also new security features — which Trojans quickly found a way to bypass. We expect to see more successful bypassing of new security features in the future. Some of these features may disrupt attacks by the mobile Trojan-Ransom, so their behavior may change in line with this.

Rooting malware

The most popular and dangerous mobile Trojans in 2016 were advertising Trojans that can use superuser rights on the device. Most of these came from the Trojan.AndroidOS.Ztorg and Trojan.AndroidOS.Iop families

During 2016 they continue their growth, doubling their presence in the TOP 30 most popular Trojans, when compared with last year (occupying 22 places in 2016, vs. 11 in 2015).

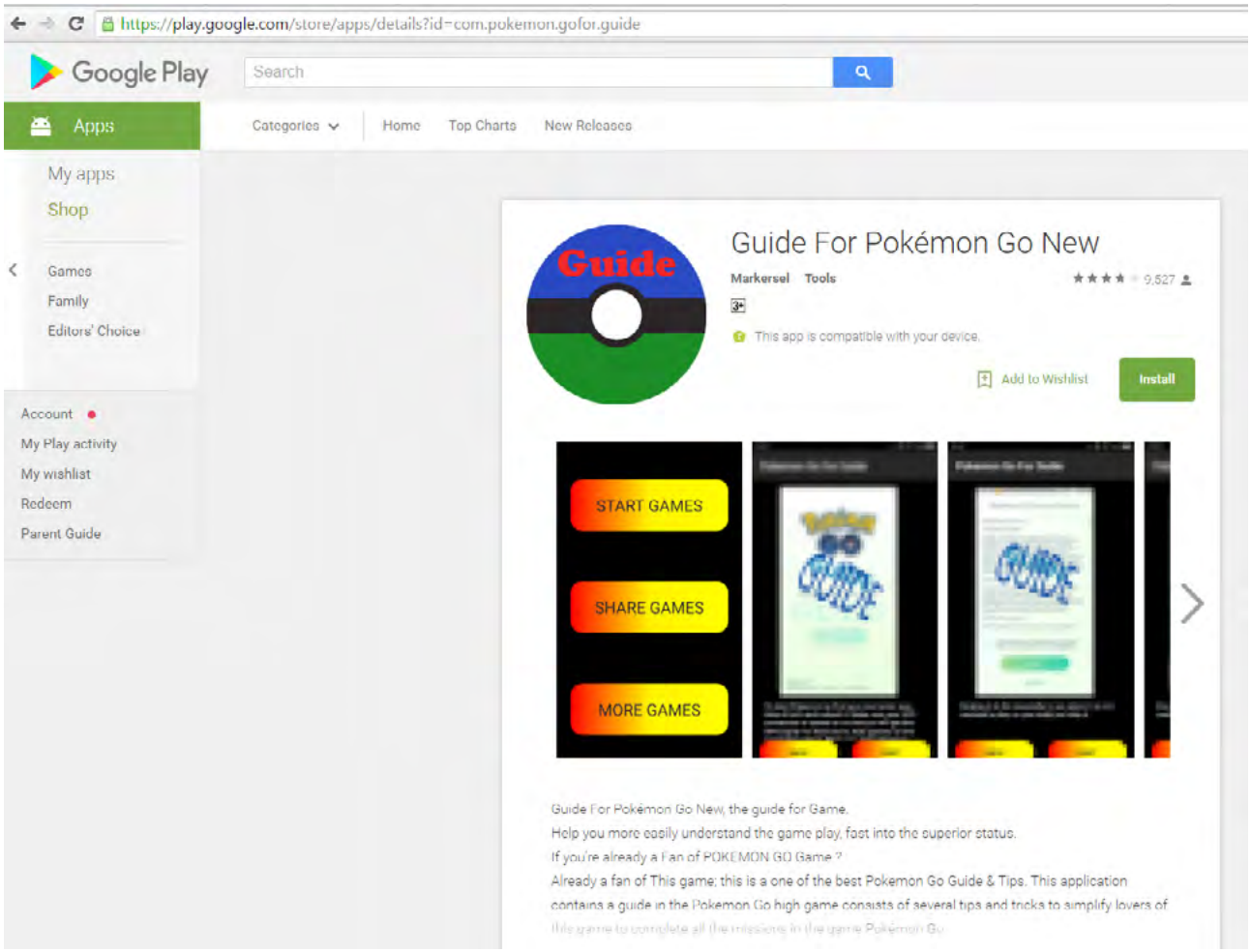
To obtain superuser rights they may use different exploits or existing superuser rights if the device was previously rooted.

More mobile Trojans seized root rights — to prevent deletion and install adware and malware

They use superuser rights mostly for two things. First of all they may hide themselves in the system folder, which makes their deletion almost impossible. Some of them can even infect the recovery image, which makes it impossible to delete them through a factory reset. Second, they use superuser rights to silently install and launch different apps that aggressively display advertising. Most of these new installed apps are non-malicious apps with ads, but there were several cases where they installed new malware, including the module-based Backdoor.AndroidOS.Triada, which injects the Zygote process. By doing so, it achieves persistence and can modify SMS sent by other apps to steal the user's money. Using root rights, this Trojan can literally do anything, including replacing urls in browsers.

A device that has been infected with an advertising app is almost unusable, due to the sheer number of annoying ads and installed apps. These Trojans are very hard to delete, and they can silently install and even buy new apps from Google Play.

Mostly, they are spread through third party app stores, but sometimes they are preinstalled on low-cost devices. During this year we saw them distributed through the Google Play Store: on a number of occasions infected apps were installed more than 100,000 times, according to the Google Play statistic. In one instance cybercriminals achieved more than 500,000 installations from Google Play — they used an infected Pokemon GO Guide app, detected as Trojan.AndroidOS.Ztorg.am.

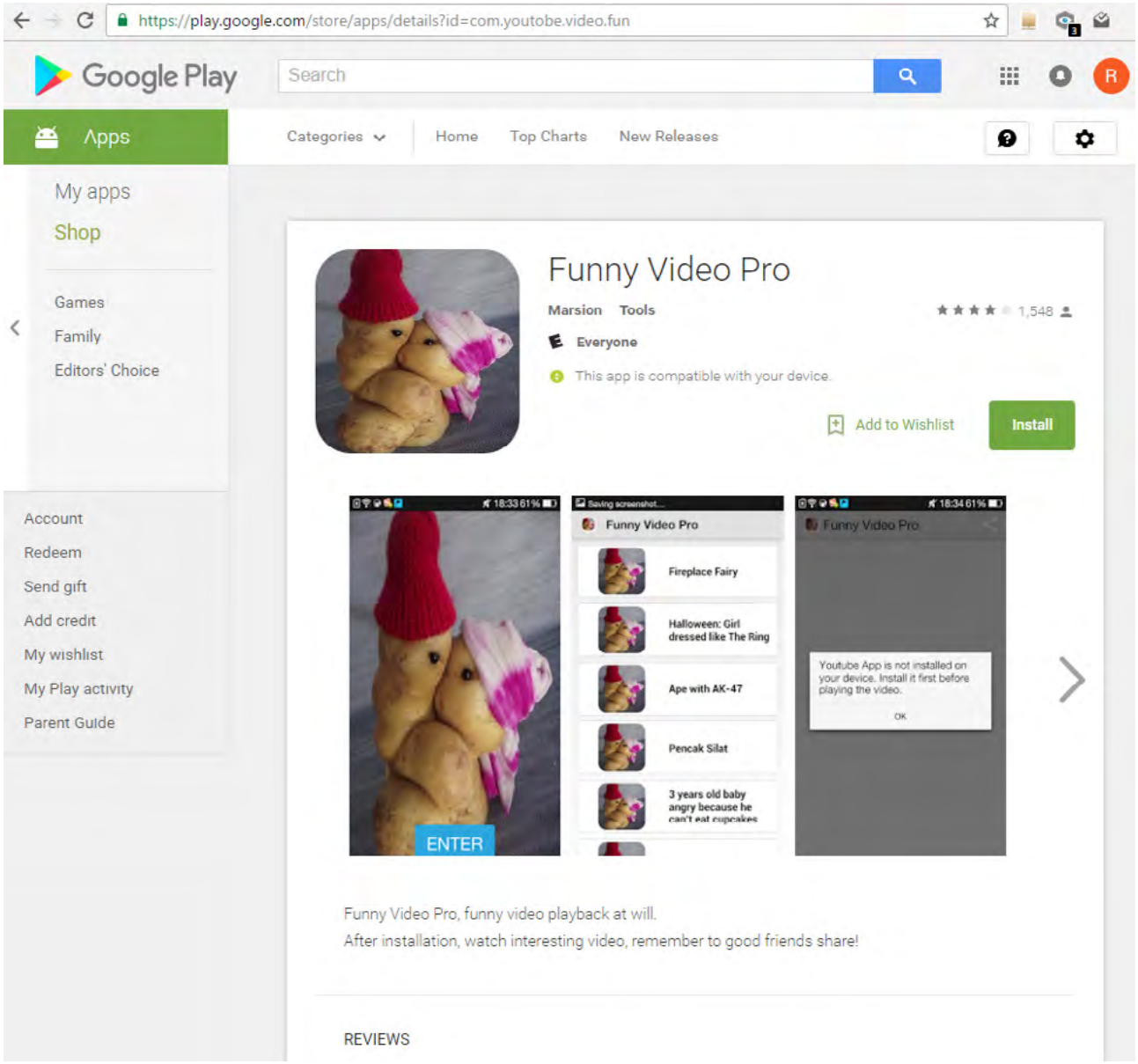


Trojan.AndroidOS.Ztorg.ad in Google Play Store

Cybercriminals still using Google Play Store

Malware distributed through Google Play was downloaded hundreds of thousands of times

Cybercriminals continued to use Google Play Store to spread their malware. During just one week in October, we detected more than ten new apps in the Google Play Store infected by Trojan.AndroidOS.Ztorg.am, a new modification of Trojan.AndroidOS.Ztorg.ad. Many of these new apps had more than 100,000 installations.



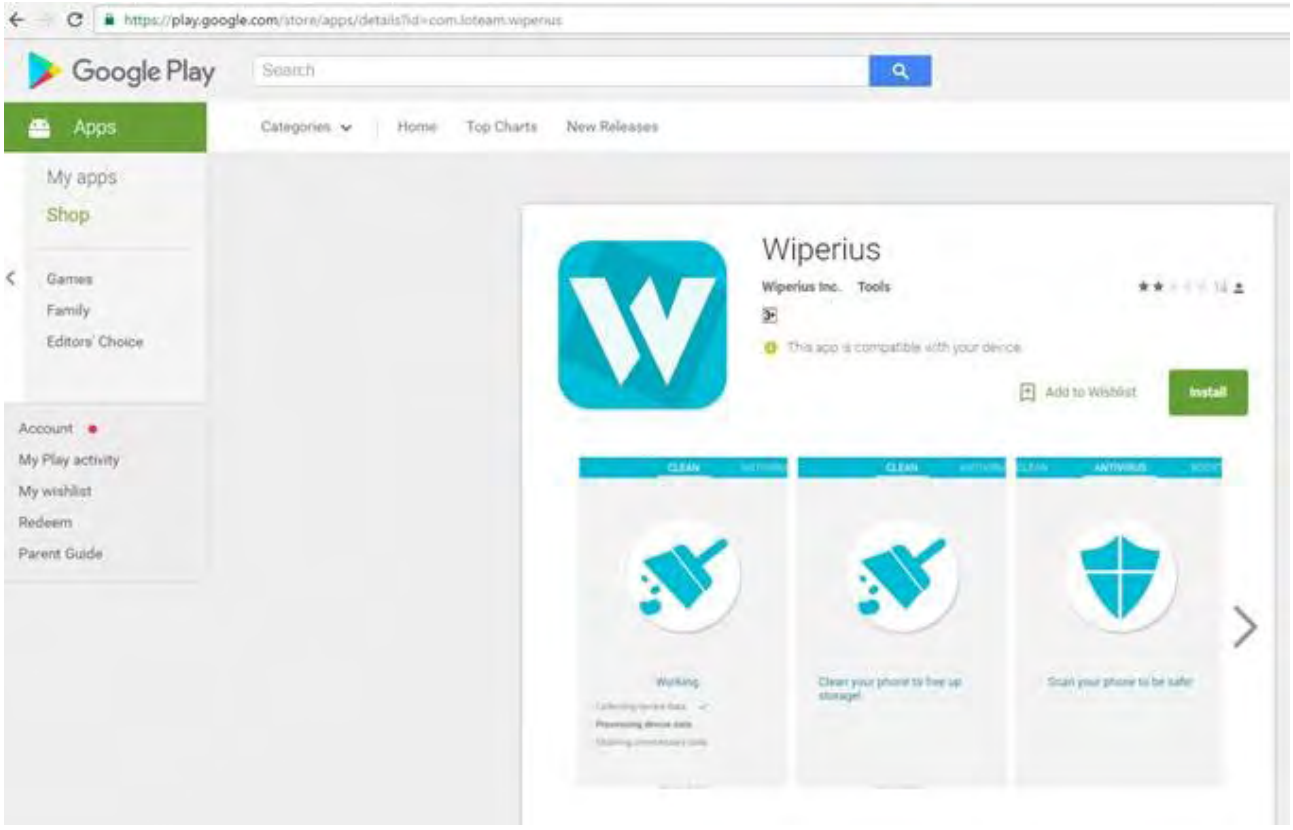
Trojan.AndroidOS.Ztorg.am in Google Play Store

One Android Trojan installed and updated as a clean app before hitting targets with an infected update

However, not only rooting malware is being distributed through Google Play — Trojans-PSW are too. In October 2015 we detected Trojan-PSW.AndroidOS.MyVk.a in the Google Play Store. This infected app had more than 100,000 installations and looked like an app for playing music from the VKontakte social network. Nevertheless, it stole users' credentials from this social network. During the year cybercriminals uploaded new modifications of this Trojan to the Google Play Store several times. To bypass security screening, they started to upload a clean app, without any harmful functionality. Then they uploaded a few clean updates and finally, at some stage they uploaded an infected version. They used this algorithm at least twice.

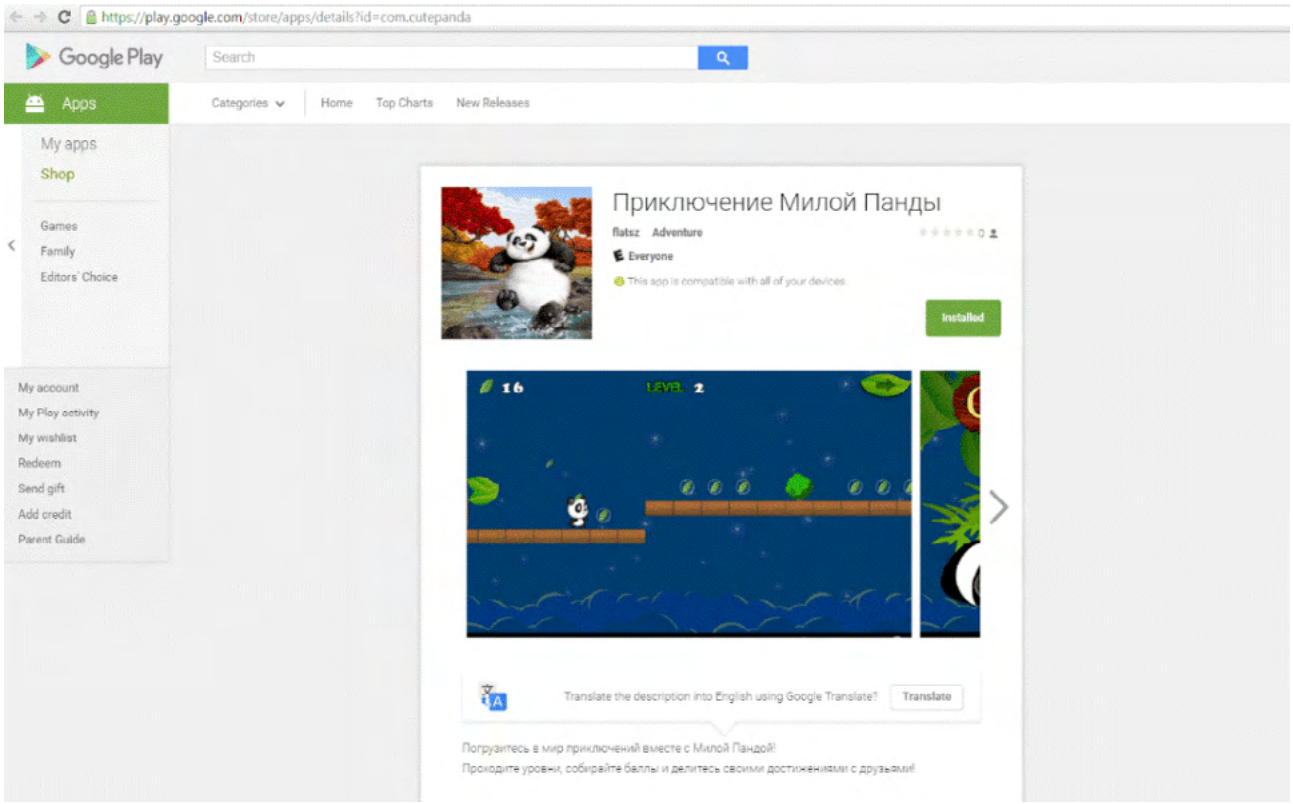
Another example of credential-stealing malware available in the Google Play Store is HEUR:Trojan-Spy.AndroidOS.Instealy.a. These malicious apps were pretending to let users know who has viewed their profile; but in reality it abused the authentication process to connect to Instagram.

Not only were rooting malware and Trojan-PSW distributed through the Google Play Store. We spotted cybercriminals also using this channel to distribute Trojan-Ransom.AndroidOS.Pletor.d.



Trojan-Ransom.AndroidOS.Pletor.d in Google Play Store

Originally, the Trojan-Ransom.AndroidOS.Pletor family encrypted user files on the infected device, but this modification only blocks the infected device and asks the user for money. It is interesting that Pletor was created by the same cybercriminal group that created the mobile banking Trojan Acecard. In December 2015, this group used the Google Play Store to distribute Trojan-Downloader.AndroidOS.Acecard.b — a Trojan that downloads and installs Trojan-Banker.AndroidOS.Acecard.a.



A Trojan-Downloader.AndroidOS.Acecard.b page in Google Play Store

Not only Google Play Store

While advertising Trojans used exploits after infection to obtain superuser rights, there were a few cases where malware used exploits for distribution.

Our colleagues from Bluecoat detected Trojan-Ransom.AndroidOS.Fusob distributed by exploits. The exploit kit was able to download and install malicious apps. Some time later we detected cybercriminals trying to use well-known vulnerabilities to distribute malware.

Trojans were also distributed through advertising networks

Another interesting way to infect users was used to distribute Trojan-Banker.AndroidOS.Svpeng. In this case, the cybercriminals used the Google AdSense advertising network to distribute Trojan-Banker.AndroidOS.Svpeng.q. Svpeng can steal information about the user's bank cards via phishing windows, and intercept, delete and send text messages. Distributing through one of the most popular online advertising networks allowed Svpeng to become the most popular Android banking Trojan in 2016. In addition, it became the second most popular Trojan overall after rooting Trojans.

Bypassing security features

As mentioned above, in 2016, some Trojans found new ways to bypass some Android security features.

Recent versions of the Android OS ask for the user's approval when an SMS is sent to a premium number. The Tiny SMS Trojan overlays this dialog with its own screen without covering the buttons in the original window.

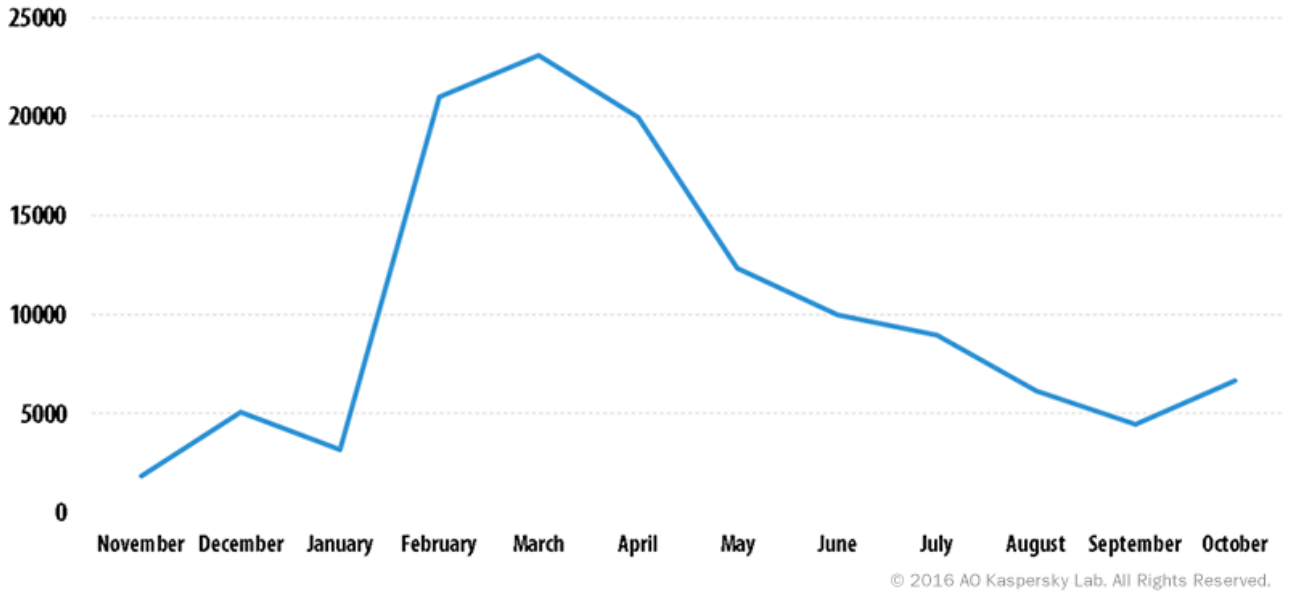
The same technique was used by Trojan-Banker.AndroidOS.Asacub. In this case the Trojan overlays the regular system window with its own window, containing buttons, and requests device administrator privileges. The Trojan thereby conceals the fact that it is gaining elevated privileges in the system from the user, and tricks the user into approving these privileges. Furthermore, the Asacub Trojan acquired SMS messenger functionality and started to offer its services in place of the device's standard SMS app. This allows the Trojan to bypass system constraints first introduced in Android 4.4 as well as delete or hide from the user any incoming SMSs.

The Gugi and Asacub Trojans found ways round new Android security features

In June 2016, we detected a new modification of Trojan-Banker.AndroidOS.Gugi with the capability to bypass two new security features added in Android 6: permission-based app overlays and a dynamic permission requirement for dangerous in-app activities such as SMS or calls. The modification does not use any vulnerabilities, just social engineering.

Mobile ransomware

The most popular Trojan-Ransom in 2016 was Trojan-Ransom.AndroidOS.Fusob. It was most actively distributed in Germany, the United States and the United Kingdom and will not work in CIS and some neighbouring countries. The criminals usually demand between $100 and $200 to unblock the device. The ransom has to be paid in the form of codes from pre-paid iTunes cards. This Trojan saw a huge rise in popularity between November 2015 and March 2016: with the number of users attacked increasing 12-fold over that time, but then its popularity fell to almost the same number of attacked users as in the previous year.



Number of unique users attacked by Trojan-Ransom.AndroidOS.Fusob

While there are more users attacked by mobile bankers than there are those attacked by mobile ransoms, the opposite is seen in the number of collected installation packets: starting from Q2 2016 we see a higher number of Trojan-Ransoms than Trojan-Bankers.

Mobile ransomware overlays rather than encrypts data as it's often backed-up

While the first mobile Trojan-Ransom encrypted user files and demanded money for their decryption, most modern Trojan-Ransoms for Android do not encrypt user files. They just show their window over all other apps, overlapping even system dialogs. Mobile encryptions are so unpopular mainly because user data on the mobile device is usually backed-up on cloud services. Regular Trojan-Ransoms that overlap all other windows with their own window also works well and it is very hard to get rid of such a Trojan.

One of the most popular mobile ransom families in China — Trojan-Ransom.AndroidOS.Congur — blocks the infected device in another way: it asks for Device Administrators rights after the start and then changes the pin code or sets one up (if there was no pin code before). It asks the user to contact cybercriminals via QQ messenger to find out the new device pin code. This method is very simple but still effective.

Trojan-Ransom is one of the technologically simplest and most effective Trojans. That is why we expect them to continue their growth and to see more new Trojan-Ransom families next year.

DATA BREACHES

Personal information is a valuable commodity, so it's no surprise that cybercriminals target online providers, looking for ways to bulk-steal data in a single attack. We've become accustomed to the steady stream of security breaches reported in the media. This year has been no different, with data leaks at beautifulpeople.com, Tumblr, the nulled.io hacker forum (underlining the fact that it's not just legitimate systems that are targeted), Kiddicare, VK.com, Sage, the official forum of DotA 2, Yahoo, Brazzers, Weebly and Tesco Bank.

Some of these attacks resulted in the theft of huge amounts of data, highlighting the fact that many companies are failing to take adequate steps to defend themselves. It's not simply a matter of defending the corporate perimeter.

There's no such thing as 100% security, so it's not possible to guarantee that systems can't be breached, especially when a breach occurs with help from an insider or where someone on the inside is tricked into doing something that jeopardises corporate security.

But any organisation that holds personal data has a duty of care to secure it effectively. This includes hashing and salting customer passwords and encrypting other sensitive data.

Consumers have no direct control over the security of the personal data they disclose to online providers. But they can limit the damage of a security breach at an online provider by ensuring that they choose passwords that are unique and complex: an ideal password is at least 15 characters long and consists of a mixture of letters, numbers and symbols from the entire keyboard. If this seems like a daunting task, you can find useful tips on how to create secure — but easy to remember — passwords. As an alternative, you could use a password manager application to handle all this for you automatically.

The theft of LinkedIn data revealed a million accounts with the password '123456'

Unfortunately, all too often people use easy-to-guess passwords and re-use the same password for multiple online accounts — so that if the password for one is compromised, all the victim's online IDs are vulnerable. This issue was highlighted publicly in May 2016 when a hacker known as 'Peace' attempted to sell 117 million LinkedIn e-mails and passwords that had been stolen some years earlier. More than one million of the stolen passwords were '123456'.

In July, we took a look back at the impact of the Ashley Madison breach, one year after the attack that led to the leak of customer data, offering some good tips to anyone who might be considering looking online for love (and good advice for managing any online account).

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 identity theft. The problem is compounded if we recycle the same password across multiple online accounts. 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.

Given the potential impact of a security breach, it's hardly surprising to see regulatory authorities paying closer attention to the issue. The UK Information Commissioner's Office (ICO) recently issued a record fine of £400,000 to Talk Talk for the company's 'failure to implement the most basic cyber security measures', related to the attack on the company in October 2015. In the view of the ICO, the record fine 'acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue'.

The EU General Data Protection Regulation (GDPR), which comes into force in May 2018, will require companies to notify the regulator of data breaches, with significant fines for failure to secure personal data. You can find an overview of the regulation here. It's to be hoped that this will ensure that companies report breaches in a timely fashion. This issue was thrown into sharp relief this year after Dropbox sent a notification to many of its customers requiring them to change their passwords. The security breach at Dropbox in 2012 resulted in the leaking not only of e-mail addresses, but passwords too. Dropbox notified customers about e-mail addresses — but not passwords — at the time. Fortunately, the passwords were hashed and salted and Dropbox offers two-step verification.

Several companies are hoping to replace passwords altogether. Apple allows fingerprint authorization for iTunes purchases and payments using Apple Pay. Samsung has said it will introduce fingerprint, voice and iris recognition for Samsung Pay. Amazon has announced 'selfie-pay'. MasterCard and HSBC have announced the introduction of facial and voice recognition to authorise transactions. The chief benefit, of course, is that it replaces something that customers **have to remember** (a password) with something they **have** — with no opportunity to short-circuit the process (as they do when they choose a weak password).

Authentication beyond passwords is a major issue for security

Biometrics are seen by many as the way forward. However, they are not a security panacea. Biometrics can be spoofed, as we've discussed before (here, here and here); and biometric data can be stolen. It would be more helpful to see biometrics as a replacement for usernames, rather than passwords. In the end, multi-factor authentication is essential — combining something you know, something you have and something you are.

INDUSTRIAL CYBER SECURITY: THREATS AND INCIDENTS

We can't call 2016 a remarkable year in terms of the number or criticality of cyber-security incidents in industrial environment. Nevertheless there were several interesting cases we'd like to highlight in the report.

Incidents

This year we've heard twice about cyber security issues in nuclear power plants. The first time it happened was at the end of April when the operator company of the Gundremmingen nuclear power plant reported about the Kido (aka Conficker) worm infection discovered in the computers of the unit B control system. This control system is a part of the nuclear fuel rods loading machine. Fortunately, the worm did not affect the technological process and didn't damage the power plant.

The relevant supervisory authority and the German Federal office for information security (BSI) have been informed. All critical systems and devices were checked, and no other signs of malicious infection were found. As the result of the incident, security measures have been extended. The incident was classified according to the German reporting criteria in category N (Normal). According to the international scale for assessment of events (INES), it is classified to level zero (below scale, no or very low safety significance).

The source of infection has not been disclosed, but the press officer of the Nuclear Power Plant has said that about 18 USB removable devices used in the office network were found infected with same Kido worm. He said that no damage could be inflicted because all critical control systems of the power plant are decoupled and the whole system architecture is redundant to denial-of-service and safe from manipulation.

Although, in this case the Kido infection did not cause any serious damage (fortunately), it is silly to think that only targeted and specifically designed malware could. At the very end of 2015, the Ukrainian power distribution substations were hit by a highly coordinated cyber attack. The adversaries sent phishing emails containing exploit to individuals in the administrative or IT network of the electricity companies. As soon as the first computers were infected, adversaries found their way into the OT network and managed to disrupt the power supply. And, what is important in this case, they cut off all remote access to the grid network. By wiping specific engineering software and corrupting the system's boot sectors, the adversaries made it impossible for the system to be managed and repaired remotely.

The idea here is that even if malware does not affect a technological process, but causes denial-of-service of critical supporting systems such as SCADA, OPS gateway, remote access, etc. – the ICS will probably continue to work according to its latest settings, but there would be no way to control and correct the process in case of accident or emergency.

ICS attacks that are not communicated to the security industry can't be analysed and nothing is learned

Months ago, Yukiya Amano, the head of the International Atomic Energy Agency (IAEA), revealed that a nuclear power plant was attacked by hackers about 2-3 years ago. Amano said that 'This actually happened and it caused some problems. While the plant did not have to shut down, it needed to take some precautionary measures'. But, it's not just a problem of a cyber-security issue causing some disruption on a power plant. Obviously, it's also the bigger problem of absence of communication and transparency between ICS and cyber security communities. At the end of the day, cyber security specialists have no chance to analyze the issue and ICS owners and vendors could not proactively implement mitigation measures.

Proof-of-Concept PLC based malware

This August, a proof-of-concept PLC worm was presented at the Black Hat 2016 conference by researchers from OpenSource Security team. The worm written solely as a PLC program is capable of autonomously identifying programmable logic controllers (PLC) in the network and spread from one PLC to another. It is also able to manipulate PLC input and output, cause denial-of-service of a PLC, connect to command and control servers and serve as a proxy for attack propagation.

The most interesting part of the proof-of-concept (PoC) is the techniques used to infect a PLC. The PoC was written for Siemens S7-1200 controllers which have the access protection feature. This feature, if turned on, allows for the password required to access the PLC using the S7CommPlus protocol to be set. Thus, it prevents any unauthorized actor from reading and modifying the code on the PLC. But, by default, the access protection is turned off. If the feature is turned on than the only way for a worm to infect the PLC is to either brute force the password or to steak/hijack it somehow.

On the other hand, if the access protection feature is turned off, there are still two other protection mechanisms, designed to limit access to the PLC:

- Know-how protection which forbids extraction and modifications of the PLC program from a device
- Copy protection that prohibits the duplication of the PLC program to another PLC device.

The access verification for both protection mechanisms – 'Know-how Protection' and 'Copy protection' – was implemented client side (within the TIA portal), which means that a simple self-written tool can read and write blocks on the PLC bypassing the authentication checks. Siemens published the advisory and provided the patch for S7-1200 firmware.

The important lesson here is that any rough device or threat actor with access to an ICS network could easily compromise whole control systems. Moreover, the PLC devices are more vulnerable to attack (especially DoS) because it doesn't expect anyone except SCADA or engineering software to communicate with it, so there is little to no protection against unauthorized access, bad input or malicious manipulations.

Zero-days in ICS software and hardware

According to US ICS CERT data in the fiscal year 2015 fiscal (from October 2015 to September 2016) they received 427 vulnerability reports, compared to 245 vulnerability reports received during the previous year. About 25% of those vulnerabilities are due to improper input validation and 27% – due to poor access controls. Other significant category of vulnerabilities – configuration and operational ones – are often disclaimed by vendors. The vulnerabilities such as default credentials, default security settings (which are often switched off), hidden API or undocumented functionality are very dangerous because they do not require high technical skills while providing extensive access into a control system.

The gap between reporting an ICS vulnerability and the issue of a patch is often too long

The sad news is that it takes an enormously long time between a vulnerability report being sent to a vendor and a patch being provided. Sometimes it never happens, because a vendor claims the vulnerable product is discontinued. From the standpoint of an ICS owner it results in undertaking a huge cost for modernization or a huge risk of being compromised.

In conclusion, we want to highlight the importance of contributing to ICS cyber security by communities of security researchers. For the last few years we have seen a remarkable growth in interest in ICS security topics. A significant number of research reports as well as tools and frameworks are published each year. For example, earlier this year we published our own review of Industrial cybersecurity threat landscape. It allows cyber security specialists from other (not ICS) fields to quickly jump in and contribute their experience and knowledge.

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