PANDALABS REPORT
Q2 2016

panda

pandalabs

1. INTRODUCTION

1 Introduction

Cyberspace has become an essential part of our daily lives. Digital transformation has affected both business and personal environments as the number of devices connected to the network continues to grow.

Concepts like “digital home” and “BYOD” (Bring Your Own Device) practices already form part of our hyper connected universe; more and more Internet users are working from home or using their own devices for both personal and business use which means there are more security holes.

This has been proved in the 18 million new samples of malware that PandaLabs detected this quarter.

Trojans maintain their position at the top of the captured malware list, highlighting the rise of ransomware attacks in this category. The average number of new threats detected every day is 200,000. This number is much lower than the previous quarter where there were 227,000 samples. **Alongside ransomware attacks, the majority of other attacks have led to the theft of personal information and log-in credentials.**

Businesses can see **a huge boom in the Internet of Things**. This will become a birthplace for attacks and has the potential to affect our personal lives. For example, in the near future, cyber-attacks could allow delinquents to steal our cars by remotely deactivating the car alarm and authorizing the vehicle to start.

Every day we see more and more vulnerabilities in the land of mobile phones. To recap, most problems that derive from these security holes are in large part due to the lack, or slowness, of updates that come from various hardware manufacturers.

2. THE QUARTER AT A GLANCE

2

The quarter at a glance

Ransomware

We know that ransomware is a huge business for cyber-criminals but to give it an accurate value is complicated. In 2015, the United States Department of Justice publicized that the Internet Crime Complaint Center (IC3) received 2,500 complaints of ransomware attacks.

A total ransom of 24 million dollars was paid by these ransomware victims. Ransomware is a global phenomenon. Taking into account the total ransom payment in this example and the widespread growth of the malware, **we can infer that ransomware costs billions of dollars every year**.

Looking back, there have been various cases of ransomware attacks in the healthcare sector. This quarter began with a new victim, *MedStar Health*. This non-profit healthcare organization suffered a ransomware attack so serious that they had to disconnect their systems for multiple days.

In the case of MedStar Health, it seems that this was a targeted attack that used a vulnerability existing in its systems. Nevertheless, most of these attacks are carried out through malicious email attachments or compromised Internet sites. As it happens, this April, *Maisto International*, a business that is known for manufacturing remote control toys, unknowingly exposed website visitors to ransomware. Their compromised website infected visitors with the well-known exploit kit Angler; Angler's objective is to identify popular software programs (flash, java, etc.), then it uses the diverse vulnerabilities from these installed applications to endanger the computer.

However, attacks via websites are not all consequences of the same kind of hack. Cyber-criminals use another popular tactic known as malvertising (malicious advertising), where they use public spaces on high traffic websites to infect visitors.

The well-known blog perezhilton.com recently fell victim to two malvertising attacks. Hackers used the exploit kit Angler to infect more than 500,000 daily visitors.

Targeted attacks use vulnerabilities in the system. Website hacks and malvertising are the most common threats.

One of the most interesting ransomware cases that we have seen during this quarter came from a business out of Slovenia.

The IT responsible at the company received an email from Russia indicating that they had compromised their network. The Russian cyber-criminals compromised the network and left it ready to execute ransomware on all company computers. **If the Slovenian company refused to pay the €9000 (in bitcoins) ransom within a 3-day period**, the ransomware would be executed. To prove that they had access to the company's network, the culprits sent a file with a list of all devices connected to the company's internal network.

There are many ransomware victims that choose to pay the ransom, but this does not guarantee that their stolen data will be returned. In May, *Kansas Heart Hospital* was attacked by ransomware and the people in charge decided to pay the ransom to retrieve their stolen data. They were shocked to discover that the password they were given could only unlock part of the kidnapped information. To recapture the entirety of the stolen information, the attackers demanded a second payment. The hospital declined to pay the second time.

The CSLFR, a professional NASCAR team, witnessed ransomware attacks to three of their computers. The ransomware encrypted information that was valued at more than 3 million dollars. In this case, CSLFR also paid the ransom ($500), but luckily they retrieved all of their information.

Is it recommended to pay these ransoms?

Let's put it this way: every time victims pay cybercriminals it boosts results.

If an attack is successful and the results are lucrative, the more users or groups will be attacked. In the long run, these attacks will harm us all.

Paying a ransom to retrieve stolen information further promotes criminal activity.

To pay or not to pay will remain a controversial issue. Adversely, the FBI acknowledged in a statement last year that they advised to pay the ransom in most cases. In April, James Trainor, assistant to the director of the FBI's Cyber-Division, made their position quite clear in a public statement:

> *"Paying a ransom doesn't guarantee an organization that it will get its data back -we've seen cases where organizations never got a decryption key after having paid the ransom-. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might be funding other illicit activity associated with criminals."*

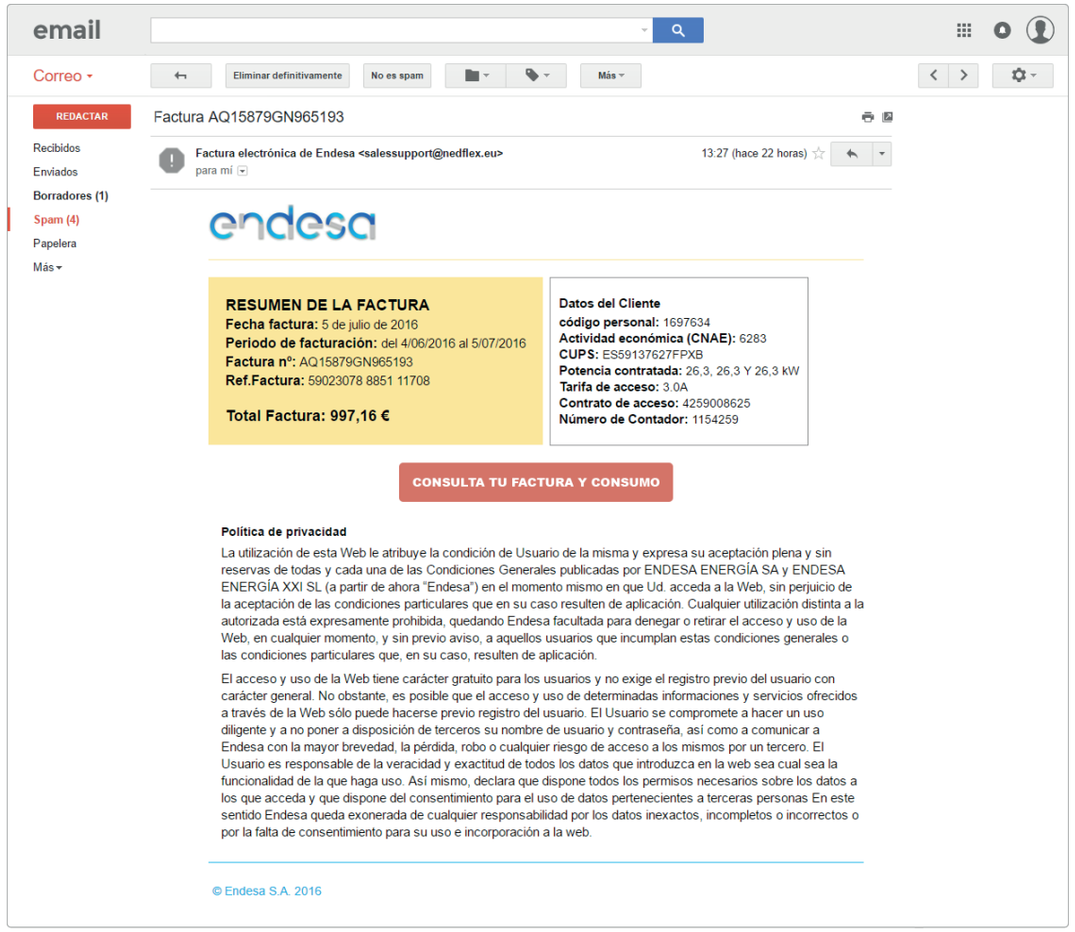
The Evolution of Malicious Emails.

The starting-point for these attacks is not only via malvertising or through compromised websites. A large part of them originate from emails disguised as bills or notices.

One of these email attacks happened in both Poland and Spain, where cybercriminals disguised themselves as electricity companies operating within each country.

The culprits sent out malicious emails to their victims. The emails did not contain attachments, they simply included an invoice and information in text and inserted a link to "consult the invoice in detail".

When this link was clicked, the user was directed to a false website that was an exact replica of the real electricity company's website.



Here, the user could download the "invoice". If the user downloaded and executed the "invoice", that is when they were infected with the ransomware.

If you had the chance, what would you say to a cybercriminal who has their eyes on you?

We have witnessed the evolution of ransomware. Generally, detailed instructions of how to carry out the payments are provided to the victims. With some types of ransomware, like the new variant of the Jigsaw family, **the attackers go as far as to include a chat service where users can speak with the extortionists in real-time to negotiate the terms of their payment**.

Now it's possible to chat with cyber-delinquents in order to negotiate payments for your kidnapped information.

One of the most original ransomware attacks in the last few months -and the most dangerous- took place in Russia.

It's unique in the way it propagates because the malware is sent via email but does not actually execute. Instead, it is programmed in its own language copied from a software manufacturer in Russia (with more than 1 million companies in Russia and the former Soviet Union), and it only functions if you have said software on your computer.

It makes you update your system, and if it is executed, it connects to a software database and searches for and sends itself the users' emails. It simultaneously infects the computer with ransomware, encrypts files, and requests the standard bail out.

Cybercrime

We have seen how this can be done in a variety of ways: through Ransomware, by stealing information from businesses and users, and sometimes by specifically targeting banks. These incidents have become extremely serious in the past few months and as we review them, we can see that they have affected all entities, from charity or finance organizations to pornographic websites and voter data... even the police was affected by these attacks. Everybody is at risk.

Information Theft.

Team Skeet, a website that distributes pornographic videos and belongs to the *Paper Street Media network*, recently suffered an attack where data belonging to 237,000 users was stolen. More than just user log-in information and email addresses was stolen, in this case criminals also made off with physical addresses of the users. **This data is being sold online for $400 per credential**, or for all of the credentials the value would add up to almost $95 million dollars. With this excessive price tag, the criminals will almost certainly offer a quantity discount.

Ransomware and stealing data from users and businesses are cybercrime tactics.

A London-based charity organization called the *National Childbirth Trust* (NCT) suffered a security breach on April 7th. During this attack, data belonging to 15,085 users was stolen including usernames, encrypted passwords and email addresses.

Acer, the well-known hardware manufacturer, also fell victim to an attack on their ecommerce site where data was stolen from 34,500 of their users. **The most serious point about this case is that their site was compromised for almost a year (from May 2015 to April 2016) without their knowledge**.

In June, a hacker nicknamed "*TheDarkOverlord*" put patient data, from three different US entities, up for sale. In total, data from more than 650,000 users was stolen and TheDarkOverlord requested a payment of $700,000. Shortly after, this same person attempted to sell data belonging to 9,300,000 clients from a medical insurance agency. This information was put up for sale for 750 Bitcoins, or approximately half a million dollars.

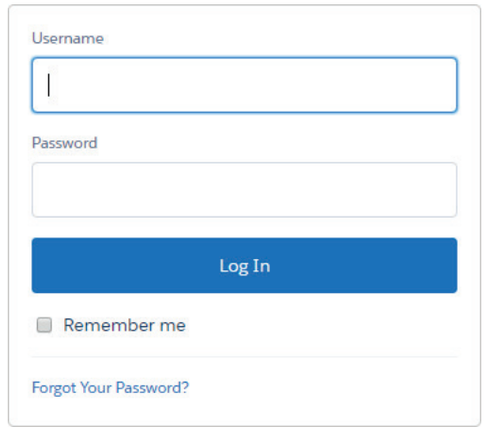
In Spain, **the group Anonymous publicized a list with personal data belonging to 5,000 members of the national police**. The data was not taken from the police servers, it was obtained by attacking the Police Social Welfare Mutuality website, mupol.

When talking about investigations in the fight against cybercrime, the name *Chris Vickery* should ring a bell. This security investigator found a server in the Amazon cloud where someone left **a database containing 93.4 million Mexican voter records**. The information included postal addresses, official identifications, etc. Vickery reported this information to the Mexican authorities, and the database was eliminated. It can be assumed that someone robbed the data and used the Amazon cloud for temporary storage.

Chris Vickery also discovered another incident of information theft. In this case, contact information for 1,100,000 users was stolen from the website beautifulpeople.com. Despite Vickery reporting the incident to heads of website, the delinquent was selling the database on the black market.

In addition to the criminals and organizations whose main objective is to inflict harm all over the internet, there are also legitimate tools that can be made to work against us.

In the case of the popular remote access tool *TeamViewer*, a large number of users were robbed as their computers we open to remote access. Due to the large number of victims, it was first thought that someone entered TeamViewer and took their databases for later, unauthorized access. It was later discovered that the information leaked for this robbery came from the users themselves, who used the same credentials to log-in to multiple services.



This is a tactic that is widely used by hackers; **once they are able to steal credentials from one site, they try to access different services using the same username-password combination**. They know that a lot of people use the same credentials on different websites. In this case, once the attackers obtained access to the victim's computer, they accessed their PayPal accounts and robbed all the money they could find.

The Rise of PoS.

Another widespread and popular theft tactic is through Point of Sale (PoS) terminals. PoS terminals are susceptible to custom malware infections that are designed specifically to steal credit card information from these terminals.

Hotels are the usual victims, like we have seen in the attack against the *Hard Rock Hotel & Casino* in Las Vegas. It is known that the PoS terminals were infected from October 2015 until March 2016 and that data was stolen from credit cards used in this establishment.

These cases happen all over the world. Recently, a Spanish chain of luxury hotels was attacked. Fortunately, the attack was stopped in time and was not able to reach the PoS terminals, which thwarted the heist. This "foolproof" attack was specifically designed for this hotel chain. To allow for outside communication and to pass by undetected, the attackers registered the domain under the name of one of the victims from an African country.

PoS terminals in hotels, restaurants and businesses are becoming more attractive to hackers.

But it is not only PoS terminals and hotel establishments are in the line of fire. Cyber-criminals are focusing on restaurants to steal credit card data. Over 1,000 establishments belonging to the popular *Wendy's* fast-food chain were victims of PoS malware. The delinquents were able to extract credit card data from Wendy's customers.

At Pandalabs, we discovered an attack that launched a known malware (PunkeyPOS) and infected more than 200 restaurants in the United States.

Image: Illustrative image of the Wendy's restaurants, it does not mean that this specific establishment was affected.

Financial Entities: The Most Sought After.

What is the most succulent theft that we have spoken of thus far? The only thing that gives a more lucrative result is to directly rob the banks, something very complex that we happened upon.

It was discovered that the *Central Bank of Bangladesh* suffered an attack where hackers were able to transfer more than 1 billion dollars. Fortunately, when the bank realized, they were able to block a large number of the transfers, but the thieves were still able to escape with 81 million dollars.

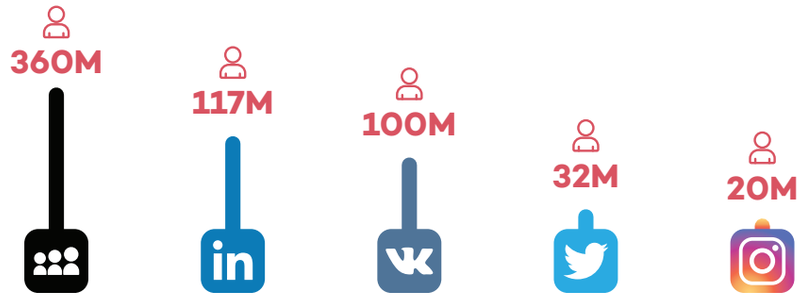
Subsequently, two similar cases occurred: one against a bank in Vietnam and another against a bank in Ecuador.

Even though going after cybercriminals can be extremely complex and time consuming, it yields results. In April, *Dmitry Fedotov*, aka "Paunch" and author of the Blackhold exploit kit, was sentenced to 7 years in a Russian prison.

Aleksandr Panin, a 27-year-old Russian was sentenced in the United States, to 9 and a half years in prison. Panin was also behind SpyEye, a well-known banking Trojan.

Social Media

If there is something that has stood out in social media during this quarter, it is the enormous amount of stolen credentials that, almost always, ends up in the wrong hands. Let's review the most popular ones:



Linkedin.

117 million LinkedIn users' security was vulnerable after a list of email addresses and passwords was publicized. Although the security breach happened in 2012, the complete list wasn't published until recently.

The best way to protect yourself against these type of attacks is by activating two-step verification. In this way, if your credentials fall into the wrong hands, they still won't be able to access your account.

Twitter.

32 million Twitter usernames and passwords were put up for sale for 10 Bitcoins, or some $6,000 dollars. The social media site denied that the data was taken from their server. In fact, the passwords were in plain text and the majority of them belonged to Russian users, which indicates that they could have been stolen with phishing attacks or Trojans.

VKontakte.

The “Russian Facebook” witnessed the sale of data belonging to **100 million of their users**, including email addresses, names, physical addresses, telephone numbers, and passwords. The same thing that happened in the LinkedIn case, except that in this incident, the data that was stolen years ago is currently up for sale.

Instagram.

Security consultant Arne Swinnen found a security fault in Instagram which enabled **20 million of their accounts to be compromised**. After reporting this information, Facebook (the owner of Instagram) compensated the investigator with $5,000 through their reward program. This is not the largest reward that has been given this quarter; Facebook gave a $10,000 reward to a 10-year-old child from Finland. This Finnish prodigy found a security flaw that allowed comments to be erased on any Instagram account.

MySpace.

Nowadays, it’s not commonly used, but it was still vulnerable to an attack that affected millions. The event happened in 2013 but it was not discovered until May of this year. In this attack they stole usernames, passwords, email addresses, and it has been said that more than **360 million accounts were compromised**. Maybe you haven’t logged-in to MySpace in years, but if you are in the habit of reusing usernames and passwords, than now is the time to change them and take advantage of two-step verification.

If you don’t believe us, just ask **Mark Zuckerberg**, the founder of Facebook. Zuckerberg witnessed that accounts on Twitter, Pinterest and Instagram were hacked by some jokers that call themselves OurMine. Apparently, the password used on LinkedIn was the same for all of the accounts, which made it easy for *OurMine* to gain access to all of them.

Activating two-step verification and refraining from using the same passwords on different websites are two important pieces of advice to follow.

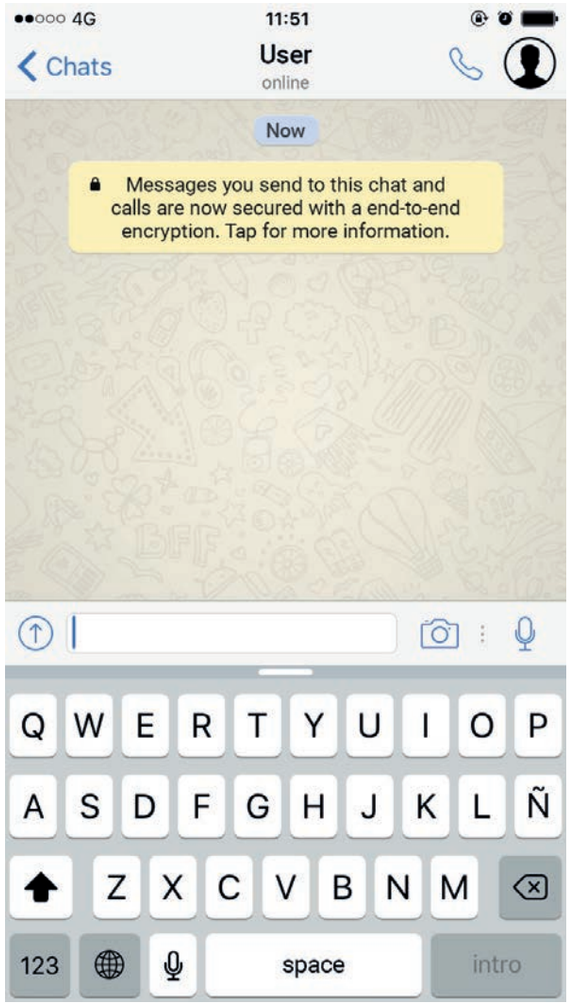
Additionally, it is just as important to use somewhat complex passwords. A study by Kore Logic reviewed 117 million passwords and demonstrated that the majority of users opt for excessively simple passwords. The 10 most used passwords can be seen in the following table:

# USERS	PASSWORD
1.135.936	123456
207.488	linkedin
188.380	password
149.916	123456789
95.854	12345678
85.515	111111
75.780	1234567
51.969	654321
51.870	qwerty
51.535	sunshine

In this respect, we must applaud *Microsoft*'s initiative to prohibit commonly used passwords that are found in these type of lists. We hope that many others follow their lead.

WhatsApp stars in another example of good cybersecurity practice. The most popular messaging app on the planet and its owner, Facebook, decided to increase user privacy by encrypting all messages sent through this app.

These plans will also include Facebook Messenger in the next few months.



Mobile Malware

It seems like Google has gone full throttle when it comes to patching all security holes in its operating systems. With monthly updates to fix all newly discovered vulnerabilities, they were able to correct 25 vulnerabilities (some of them were very serious that enabled the remote execution of the code) in May alone. Although it seems that none of these vulnerabilities were used by attackers, this is one of Google's largest updates... to date.

In spite of improvements, the Android ecosystem still trembles with security issues.

Without a doubt, one of Android's biggest problems is their slow updates, which in large part depend on each hardware manufacturer of the various Android devices. While products that are controlled directly by Google receive these updates almost immediately (for example, Nexus mobile phones and tablets), other Android users have to wait months to receive patches. In some cases, the patches never arrive.

The lack-of-updates makes devices more and more vulnerable to known security problems, and as attacks increase, **it will make the Android ecosystem really dangerous**.

Internet of Things

Lately in this section, there is almost always a news piece about hacked cars, now it's the Mitsubishi Outlander's turn. This hybrid car has its own Wi-Fi network that connects to an app where you can modify the temperature and other settings.

The security investigator *Ken Munro* discovered the Wi-Fi network password through brute force attack; once he was in the network, Munro could sabotage the car (for example, by completely draining the electric motors' battery). But the most serious is that he could remotely deactivate the alarm, something that many delinquents could take advantage of.

The consultant Gartner publicized an interesting report about security in the Internet of Things. In this document, they predicted that **25% of the attacks suffered by businesses will involve IoT devices by 2020**. It is expected that in 2016, 6.4 billion of these devices will be connected to the net (30% more than 2015), in 2018 they calculate that the number of these devices will be over 11.4 billion.

The spending on IoT security will gradually increase, although taking into account the predictions in the table below, it probably won't be enough:

Worldwide IoT Security Spending Forecast
(Millions of Dollars)

2014	2015	2016	2017	2018
231.86	281.54	348.32	433.95	547.20

Source: Gartner (April 2016)

Cyberwar

Last year we wrote about how the company *Hacking Team*, was completely compromised. This business is well-known because they sell tracking software (malware) to governments and security forces worldwide. They headlined news when the Italian newspaper "Il Fatto Quotidiano" published that "Hacking Team" had lost their exportation license, making it nearly impossible to sell their programs outside of the European Union, at least without having to go through lengthy bureaucratic procedures.

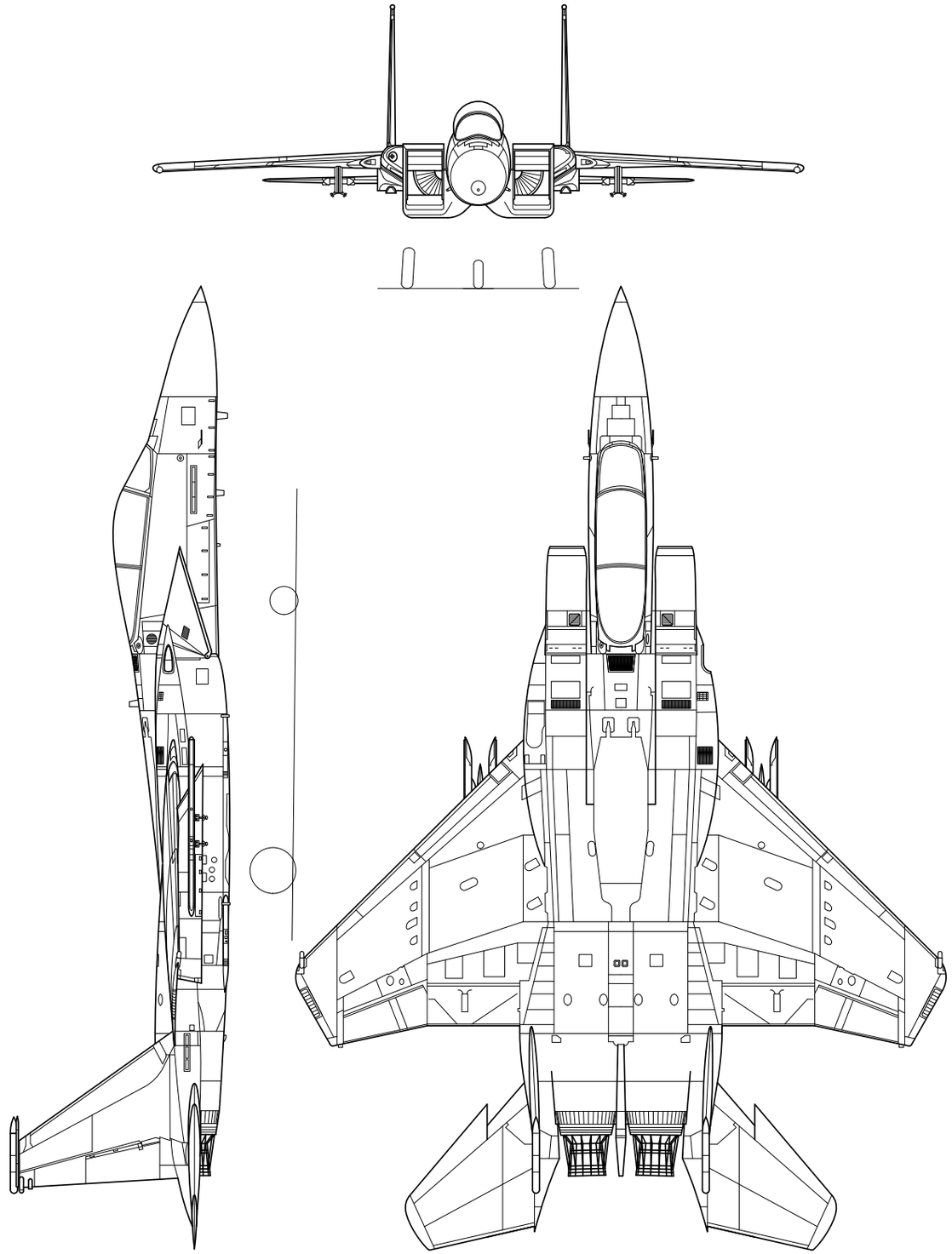
When we are discussing cyberwar in the majority of these occasions, we are talking about attacks that are probably sponsored by different countries, even though it is rare to find evidence that confirms who is responsible for the attack.

However, the United States went on the offensive, and they acknowledged that they are launching cyberattacks against Daesh (also known as ISIS). Robert Work, the United States Deputy Secretary of Defense, said:

> *"We are dropping cyber bombs. We have never done that before. Just like we have an air campaign, I want to have a cyber campaign. I want to use all the space capabilities I have."*

In June, South Korea's police department publicized an attack from North Korea. It seems that the attack began over a year ago, focused on 140,000 computers belonging to organizations and government agencies, as well as defense contractors. This attack was not discovered until this February. According to police, **more than 42,000 documents were stolen in which 95% of them were defense-related**, for example the plans and specifications of the American F15 fighter plane's wings.

The US Democratic National Committee acknowledged that their systems were compromised for a year (maybe more). They believe that the attackers belonged to Russian intelligence. The attackers had access to emails, chats and all kinds of research papers. **All computers belonging to the investigation department were accessed and some files were stolen**.



3. CONCLUSION

3 Conclusion

The number of attacks used to steal information and money continues to rise. Users witness the theft of their identities or accounts, and many times they are not even attacked directly. Instead, their information is discovered in stolen databases from compromised companies.

Additionally, some users reuse their passwords, which has facilitated the thefts and is something that could be easily solved by activating the two-step verification offered by most sites. Another possibility is that service providers require their users to activate these security measures, which does not seem probable now that usability is prioritized over security.

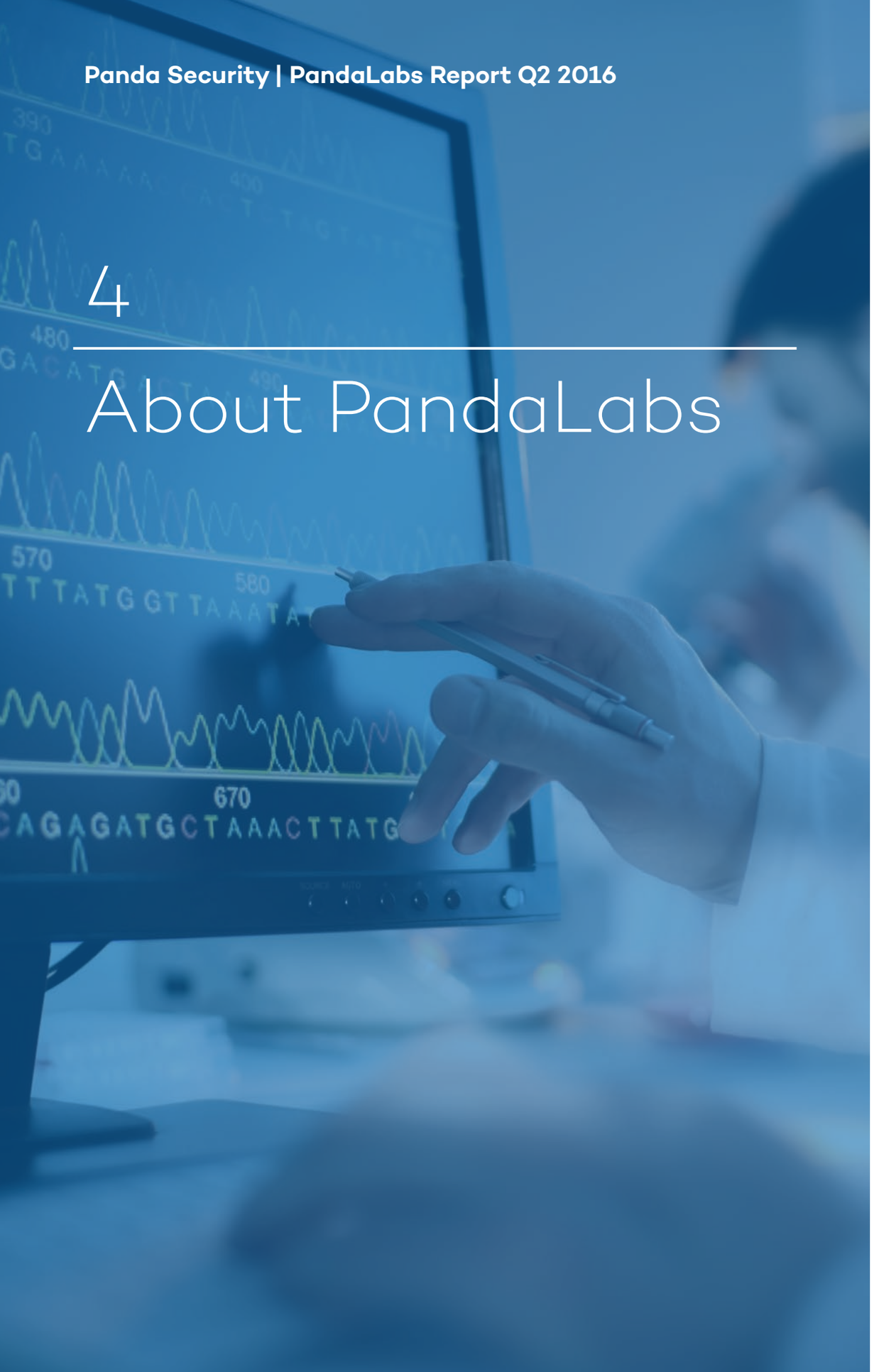
Ransomware attacks can be highly sophisticated. Hackers are making huge profits. In the coming months, we will see how these attacks continue to rise.

Another worrying trend is credit card theft via PoS systems, where the majority of the affected establishments are small businesses (restaurants, bars, etc.) that, evidently, do not have a dedicated IT security team to depend on. Taking into account how easy it is to sell this stolen information on the "black market" and make a profit, it makes sense that this will continue to be an objective for cyber-criminals.

We will see you in three months to analyze and discuss the 3rd quarter of 2016. Meanwhile, PandaLabs will keep you informed of all cybersecurity news through our Media Center:

http://www.pandasecurity.com/mediacenter/

4. ABOUT PANDALABS



4 About PandaLabs

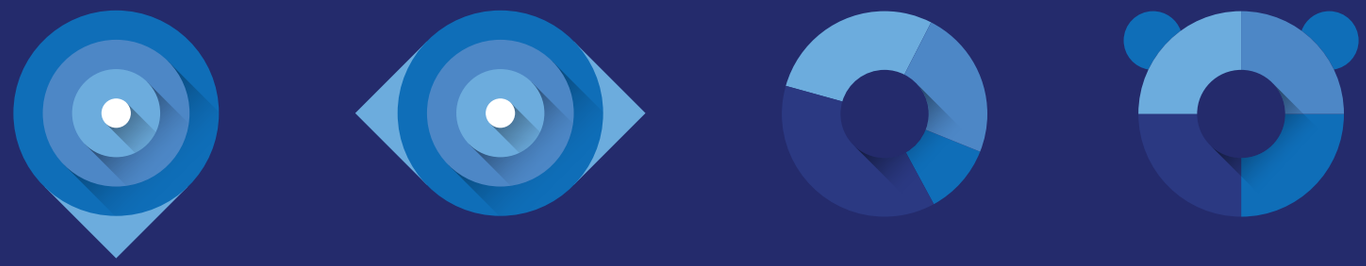
PandaLabs is Panda Security's anti-malware laboratory and R&D center where:

PandaLabs creates automated and real-time systems necessary to protect Panda Security clients from all types of malicious code countermeasures worldwide.

PandaLabs is responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.

Likewise, PandaLabs maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security.

Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.



panda

pandalabs