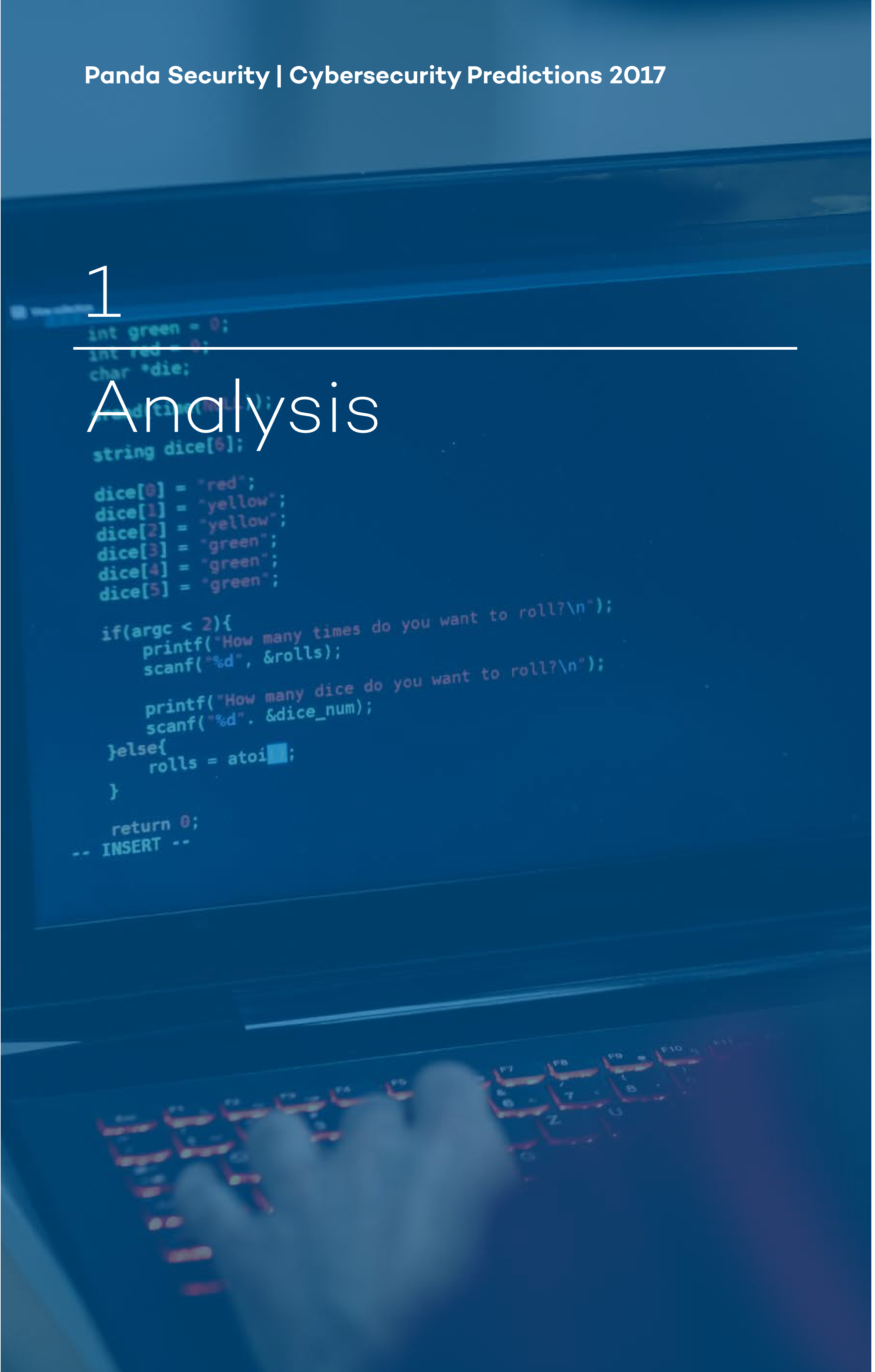
CYBERSECURITY PREDICTIONS 2017

panda

pandalabs

1. ANALYSIS

1 Analysis



```
int green = 0;
int red = 0;
char *die;

string dice[6];

dice[0] = "red";
dice[1] = "yellow";
dice[2] = "yellow";
dice[3] = "green";
dice[4] = "green";
dice[5] = "green";

if(argc < 2){
    printf("How many times do you want to roll?\n");
    scanf("%d", &rolls);

    printf("How many dice do you want to roll?\n");
    scanf("%d", &dice_num);
}else{
    rolls = atoi ;
}

return 0;
-- INSERT --
```

The technological revolution is by now an undisputed reality. It is clearer than ever, now in the last trimester of the year, that digital technologies are transforming the world of business, work, and public administration. It is vital that we promote a climate of digital trust that bolsters user protection. For this reason, cybersecurity has become a crucial element.

The year kicked off with more than 20 million new samples of malware detected and neutralized by PandaLabs, with an average of 227,000 per day. This figure is slightly higher than the one found last year in the same quarter, in which the average of new samples rounded off at 225,000 per day. Throughout 2016, we've seen how **the quantity of new malware has been slightly lower than last year's — about 200,000 new samples of malware per day on average — although attacks have become more effective.**

Cybercriminals are becoming more and more confident of their abilities, and, even though we're closing the year with more optimistic figures than when we began it, we can't let our guard down. Black Hats are concentrating their efforts into the most profitable attacks, utilizing tactics and professionalizing the sorts of attacks that allow them to make quick and easy money in an efficient manner.

Black Hats have turned their focus essentially to productivity, proliferating attacks on businesses that handle massive quantities of data and sensitive information (hospitals, pharmaceuticals, hotels, etc.). Once they've gained access to these businesses, they infect the greatest number of computers possible with ransomware, putting themselves in a position in which they can demand millions in ransom or put the data up for sale on the black market.

If there is one thing that hasn't changed over the course of this year, it's the most popular class of malware: trojans, with ransomware at the forefront, have continued to top the statistical charts for years.

2. RANKING THE TOP ATTACKS OF 2016

2

Ranking the top attacks of 2016

Ransomware

We know that ransomware is a substantial business for cybercriminals, but it is incredibly tricky to measure it reliably. We have witnessed the evolution of these attacks, with such advances as the increased implementation of a chat function as a direct line of communication with thieves used to "formalize" payments. Techniques have also evolved, and in some cases have become particularly aggressive, as is the case of **Petya**, which instead of encrypting documents goes straight for the computer's Master Boot Record (MBR) and makes it unserviceable until a ransom is paid.

Also on the rise is the abuse of the **PowerShell** system tool (as we prognosticated in our PandaLabs Annual Report of 2015), installed by default in Windows 10 and frequently used in attacks to avoid detection by security solutions installed on victims computers.

In the second quarter, one of the strangest cases of ransomware involved a company in Slovenia. The company's head of security received an email out of Russia informing him that their network had been compromised and that they were poised to launch ransomware on all of their computers. If the company didn't pay around €9000 (in bitcoins) within 3 days, they would launch the ransomware. To demonstrate that they did in fact have access to their network, they sent them a file with a list of every device connected to the company's internal network.

There are indeed victims who choose to pay the ransom, even though the retrieval of their data is not guaranteed.

It was in the third quarter of this year that we became witness to a higher level of specialization in the ransomware trade.

The best example of this featured the creators of the ransomwares Petya and Mischa, specialized in the development aspect of malware and its corresponding payment platforms, leaving distribution in the hands of third parties, a practice that can be called **Ransom as a Service** (RaaS). Essentially, once they've done their part they leave it up to the distributers to be in charge of infecting their victims. Much like in the legal world, the distributers' profit is derived from a percentage of the money acquired. The higher the sales, the higher the percentage that they receive.

Malicious email

Attacks don't only come in the form of malvertising or compromised websites. A large number of them still arrive through email in the form of false invoices or all kinds of notifications.

An attack of this sort was carried out in at least two European countries, Poland and Spain, where cybercriminals posed as their respective local electric companies.

The message contained no attachment, showing only the billing information in text and including a link that when clicked would take you to the invoice details.

The hook was an exorbitantly high payment that would create a sense of outrage so that, in the throes of frustration, the recipient would click through to consult the supposed bill without thinking. Upon clicking the link, the user was directed to a website that resembled the usurped company's real website, where a bill could be downloaded. If the client downloaded and opened the file, they became infected with ransomware.

Business Email Compromise Phishing

This kind of attack is rapidly gaining in popularity.

The attackers pose as the president or financial director of a company and request a transfer from an employee.

Before doing so, they learn about how the company operates from the inside and get information from their victims off of social networks to give credibility to their con.

One of the most resounding cases this year featured **Mattel**, the well-known toy manufacturer of Barbies and Hot Wheels.

A high ranking executive received a message from the recently appointed CEO soliciting a transfer of $3 million to a bank account in China. After making the transfer, he then confirmed with the CEO that it was done, who in turn was baffled, since he had never given such an order. They got in touch with the

American authorities and with the bank, but it was too late and the money had already been transferred.

In this case they were fortunate. It was a bank holiday in China and there was enough time to alert the Chinese authorities. The account was frozen, and Mattel was able to recover their money.

Mobile Devices

SNAP is one the most popular vulnerabilities that we've seen this year.

It affects LG G3 mobile phones. The problem stemmed from an error in LG's notifications app, called Smart Notice, which gives permission for the running of any JavaScript. The researchers at BugSec discovered the vulnerability and notified LG, which rapidly published an update that resolved the problem.

Gugi, an Android trojan, managed to break through Android 6's security barriers to steal bank credentials from apps installed on the phone. To accomplish this, Gugi superimposed a screen on top of the screen of the legitimate app asking for information that would then be sent directly to the criminals without their victims' knowledge.

In August, Apple published an urgent update of version 9.3.5 of iOS, its operating system for mobile phones. This version resolves three 0-day vulnerabilities employed by a **software spy known as Pegasus**, developed by the NGO Group, an Israeli organization with products similar to those offered by Hacking Team.

Internet of things

The automobile sector is one of the most at risk. Investigators at the University of Birmingham showed how they had succeeded in compromising the power door lock system of every vehicle sold by the Volkswagen Group in the last twenty years. Researchers Charlie Miller and Chris Valasek, who last year demonstrated how to hack a Jeep Cherokee, took it one step further this year to show how they could manipulate at will the throttle, the break, and even the steering wheel while the car was in gear.

Smart homes are also vulnerable to cyberattacks. Researcher Andrew Tierny showed a proof of concept that he himself had elaborated to hijack a thermostat. After taking control of the thermostat (inserting an SD card in it), he raised the temperature to 99 degrees Fahrenheit and required a PIN to deactivate it. The thermostat connected to an IRC channel, giving the MAC address of as an identifier of every compromised device. It demanded a bitcoin in exchange for the PIN, which changed every 30 seconds.

Cyberwarfare

In the cyberwarfare sector, 2016 saw the United States go on the offensive and concede that it is launching cyberattacks against Daesh targets.

Robert Work, United States Deputy Secretary of Defense, made this clear in statements to CNN.

In June, **South Korean officials disclosed an attack originating from North Korea**. The attack allegedly began over a year ago, its primary target being 140,000 computers belonging to organizations and government agencies, as well as defense contractors. But up until February of this year the attack was not discovered. According to police statements, more than 42,000 documents were stolen, of which 95% were related to defense, such as, for example, documents containing plans and specs for the F15 fighter jet.

At the height of the United States presidential election, one of the most relevant incidents that took place was the discovery of an **attack on the DNC (Democratic National Commettee) in which a stockpile of data was plundered**, and was then leaked to the public.

On the subject of the elections, the FBI issued an alert after detecting two attacks on electoral websites, and at least one of the attackers — identified as foreigners — was able to make off with voter registration data.

In August, a group calling itself **"The Shadow Brokers" announced that it had hacked the NSA** and published some of the "cyber weapons" that it had stolen, promising to sell the rest to the highest bidder.

Cybercrime

In June, a criminal dubbed "The Dark Overlord" put patient information from three US institutions up for sale on the black market.

He had stolen information from over 650,000 patients and asked for around $700,000 for its return. Shortly thereafter, he put the personal information of 9.3 million clients of a medical insurance agency up for sale for 750 bitcoins (around a half million dollars).

In the last few months, Dropbox has also fallen prey to cybercrime. It was recently revealed that the well-known file sharing service suffered an attack in 2012.

The outcome: the theft of data from 68 million users.

But if there's one theft we should be talking about, it's the one that happened at **Yahoo**. Although it took place in 2014, it only became known recently. A total of **500 million accounts were compromised**, becoming the greatest theft in history.

On August 2, one of the greatest bitcoin thefts in history occurred. **Bitfinex**, a company that deals in the commerce and exchange of cryptocurrency, was jeopardized and had an equivalent of **60 million dollars in bitcoins stolen** from it, money which belonged to clients that had deposited their bitcoins in this "bank".

There is still no evidence pointing to the culprits, and the company has offered no information as to how it happened, as law enforcement agencies are still investigating the case.

DDoS Attacks

In September, Brian Krebs, the famed journalist specializing in security, blew the cover off of vDOS, a "company" that offered DDoS attack services.

Shortly thereafter, the people responsible, who in two years had lead 150,000 attacks and made a profit of $618,000, were arrested.

Not long after, Krebs's website began to receive a crippling DDoS attack that brought it down for a week. In the end, Google, through its Project Shield, was able to protect it and the page came back online.

In the last quarter of the year, a wave of large-scale cyberattacks against the American internet provider DynDNS jeopardized the service of some major global corporations' websites. The brutal attack affected major organizations and international communications tools, such as Netflix, Twitter, Amazon, and The New York Times. Service was interrupted for almost 11 hours, affecting more than a billion clients worldwide.

POS's and Credit Cards

The popular fast food chain Wendy's saw the Points of Sale at more than 1,000 of its establishments infected with malware that stole credit card information from its clients.

In PandaLabs we discovered an attack carried out with malware known as PunkeyPOS, which was used to infect more than 200 US restaurants.

Another such attack was discovered in 2016 by our laboratory. Once again, the victims were US restaurants, a total of **300 establishments** whose POS's had been infected with the malware **PosCardStealer**.

Financial Institutions

This year, the Central Bank of Bangladesh suffered an attack in which 1 billion dollars in bank transfers were made.

Fortunately, a large portion of those transfers were blocked, although the thieves had already succeeded in making off with 81 million dollars.

Shortly after that we witnessed two similar cases: one against a bank in Vietnam, another against a bank in Ecuador.

Social Networks

The security of **117 million LinkedIn users** was at risk after a list of email address and their respective password hashes were published.

On Twitter, 32 million usernames and passwords were put up for sale for around $6000.

The social network denied that the account information had been attained from their servers. In fact, the passwords were in plaintext and the majority of them belonged to Russian users, hinting at the possibility that they were attained by means of phishing or Trojans.

It turns out that, even though practically nobody uses it, **MySpace** was attacked. The intrusion happened in 2013, although up until May of this year it remained unknown. Usernames, passwords, and email addresses were taken, reaching up to **360 million affected accounts**.

A user may not have used MySpace in years, but if they are in the habit of reusing passwords, now is the time to change this habit and activate a two-factor authentication.

Activating two-factor authentication, creating complex passwords and not reusing them for different websites — these are some cybersecurity tips to be taken into consideration.

3. WHAT CYBERNETIC NIGHTMARES DOES 2017 HAVE IN STORE FOR US?

3

What cybernetic nightmares does 2017 have in store for us?

Ransomware

It took center stage in 2016, and will presumably do so again through 2017. In some ways, **this kind of attack is cannibalizing other more traditional ones** that are based on information theft. Ransomware is a simpler and more direct way to make a profit, eliminating intermediaries and unnecessary risks.

Companies

Attacks on companies will be more numerous and more sophisticated.

Companies are already the prime target of cybercriminals. Their information is more valuable than that of private users.

Cybercriminals are always on the lookout for weaknesses in corporate networks as a way to find an entry point. Once inside, they use lateral movements to access resources that contain the information they are looking for. They can also launch large-scale ransomware attacks (infecting with ransomware all available devices), in order to demand astronomical sums of money to recover the data of affected companies.

Internet Of Things

Internet of Things (IoT) is the next cybersecurity nightmare. Any kind of device connected to a network can be used as an **entryway into corporate networks**. The majority of these devices have not been designed with security strength in mind.

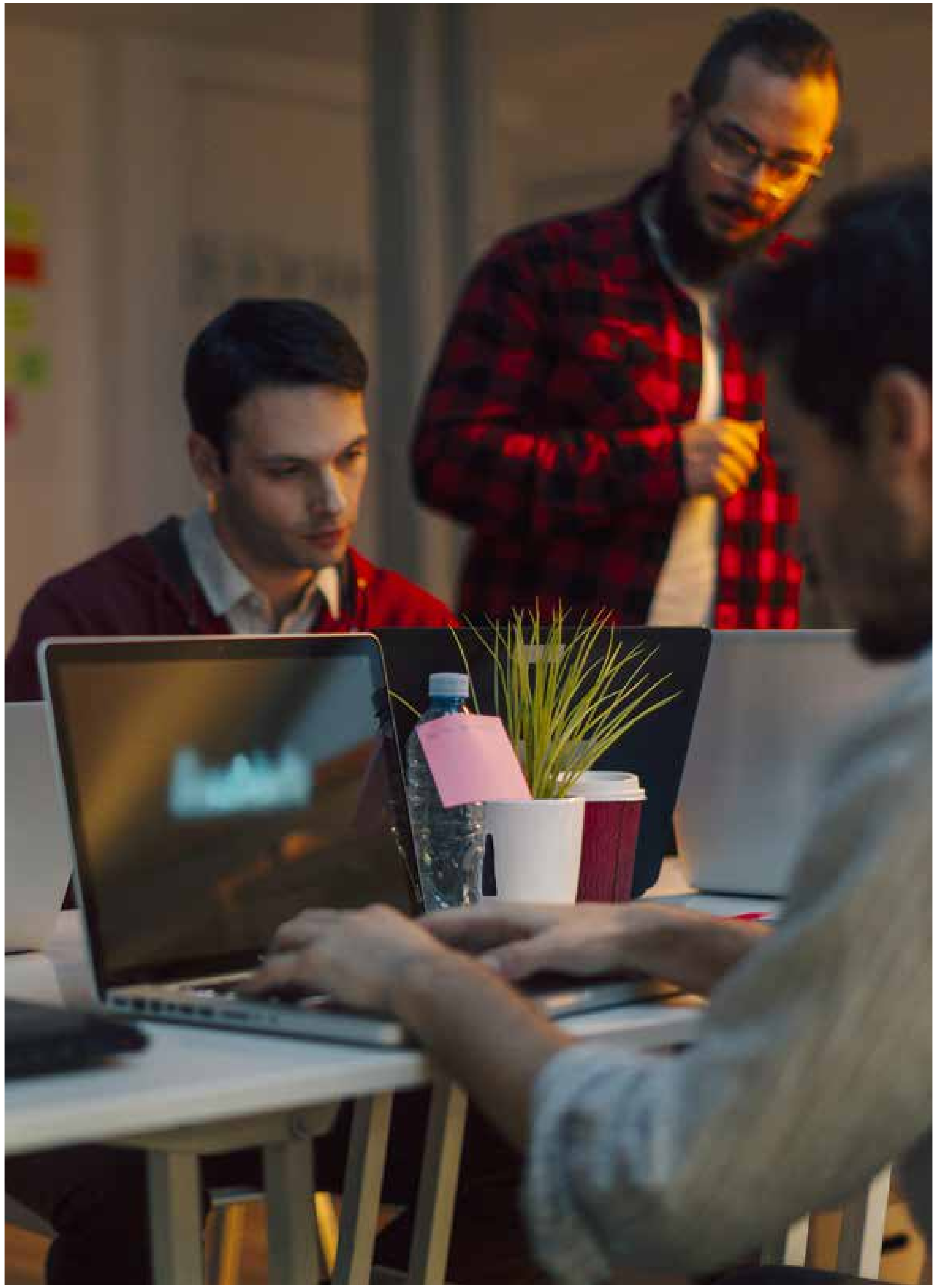
Typically they do not receive automatic security updates, use weak passwords, reuse the same credentials in thousands of devices, etc. All of this together makes them extremely vulnerable to outside attacks.

DDoS

The final months of 2016 witnessed the most powerful DDoS attacks in history. It began in September with an attack on **Brian Krebs** after his having reported on the activities of an Israeli company that offered this kind of service.

On the heels of that attack came another on the French company OVH (reaching 1Tbps of traffic) and another on the American company Dyn that left several major tech giants without Internet service.

These attacks were carried out by bot networks that relied on thousands of affected IoT devices (IP cameras, routers, etc.). We can be certain that 2017 will see an increase in this kind of attack, which is **typically used to blackmail companies or to harm their business** (by blocking web access, online shopping, etc.).



Mobile Phones

The target is clear here as well — **Android devices got the worst of it.** Which makes sense, given that Android has the greatest market share, and is the OS of the greatest number of devices. Apple retains a modest percentage with iOS, and the rest of the alternatives are negligible. Focusing on one single OS makes it easier for cybercriminals to fix a target with maximal dissemination and profitability.

To complicate matters (or, if you're a cybercriminal, simplify them), updates do not only depend on the rollout of what Andoid can do, but also depends on each hardware manufacturer's decision of when and how to incorporate them (if at all). Given the amount of security issues that crop up every month, this situation only puts users at greater risk.

Cyberwarfare

We are living through one of the most precarious moments in international relations of the last several years — threats of commercial warfare, espionage, tariffs with the potential to polarize the positions of the great powers. This can no doubt have huge — and serious — consequences in the field of cybersecurity.

Governments will want access to still more information (at a time when encryption is becoming more popular), and intelligence agencies will become still more interested in obtaining information that could benefit industry in their countries.

A global situation of this kind could hamper data sharing initiatives — data that large companies are already sharing in order to better protect themselves against cybercrime, setting standards and international engagement protocols.

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