Survival Guide for Million-Dollar Cyberattacks

pandasecurity.com

panda

About PandaLabs

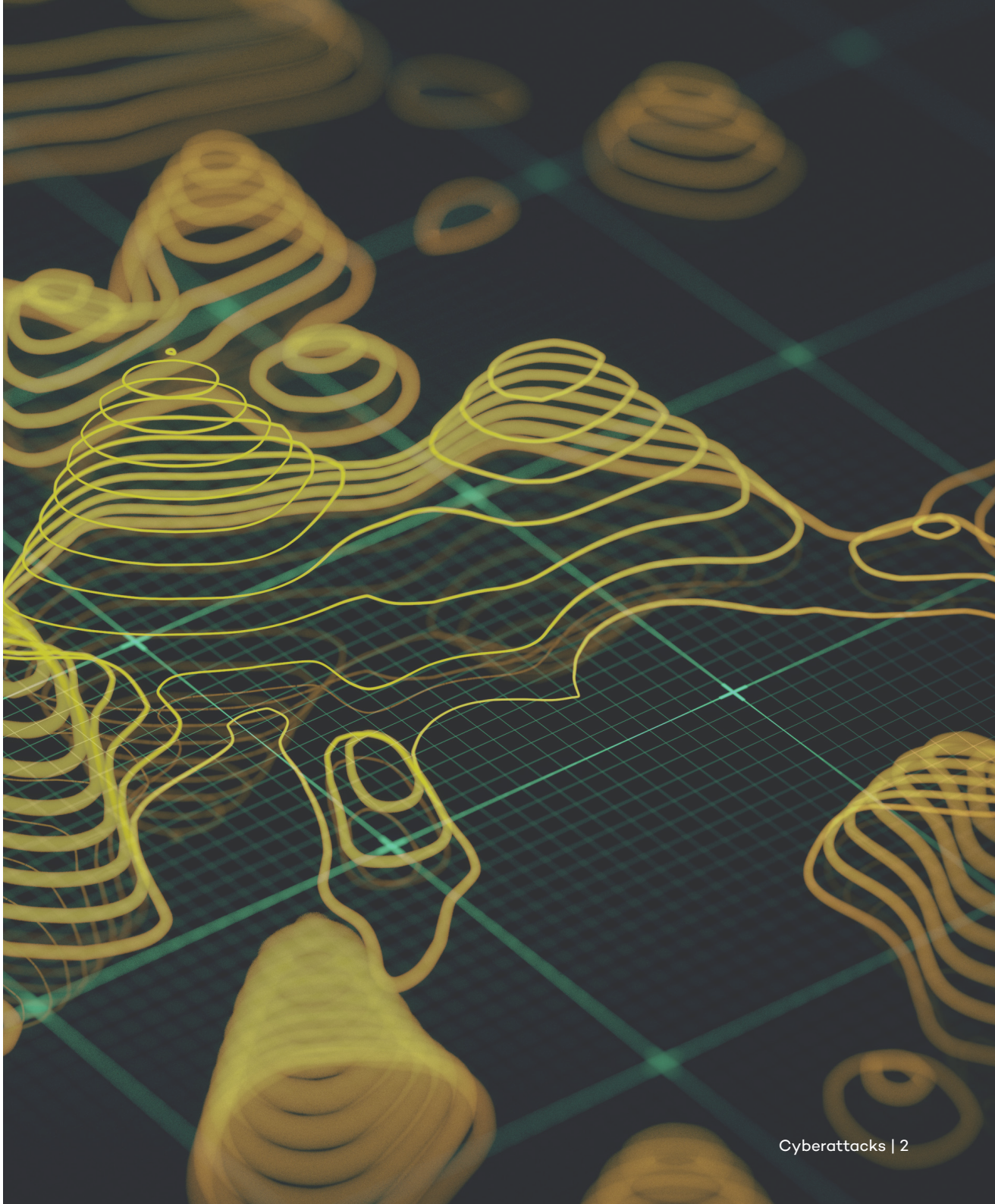
PandaLabs is the antimalware laboratory at Panda Security and represents the nerve center of the company for everything malware-related.

At the laboratory, the countermeasures necessary to protect Panda Security's customers from all types of malicious code on a global scale are produced in real time and uninterruptedly.

PandaLabs is responsible for the detailed analysis of all types of malware in order to improve protection, as well as to keep the general public informed about new threats.

The laboratory's technicians maintain a continuous state of vigilance, closely following the different trends and evolutions that have taken place in the field of malware and security.

Their aim is to issue alerts on imminent dangers and threats, as well as to formulate forecasts for the future.



Main Conclusions: What Do These Attacks Imply?

Threats have evolved, malware is becoming more sophisticated, and attack techniques are becoming more refined. The victim is no longer randomly selected, but rather attacks have become targeted, coordinated, and use different vectors. The motive has also changed. Gaining recognition is no longer the concern. It's now all about economic profit.

Cybercrime is a very profitable and attractive business. Attackers today are more professional, have more and better technical and economic means that allow them to make their attacks even more sophisticated. This is why they are no longer afraid to go directly to the banks themselves, something unthinkable a few years ago.

To reinforce the financial system as much as possible, for the first time the European Union plans to carry out tests across the whole European framework to check whether banks have the proper systems in place to defend against the most current known cyberattacks. These tests will be similar to so-called "stress tests". The European Banking Authority (EBA) is also looking to launch initiatives to safeguard digital banking.

And let's not forget the more traditional attacks that have hounded the financial sector — those which targeted the end customer of banking institutions, such as phishing attacks or banking Trojans — and which continue to be perpetrated and have adapted to modern times, such as those that use malware for Android.

Introduction

For years, accumulating money has been the main objective of cybercriminals. Logically, this fact puts financial systems in the crosshairs. For more than a decade attacks have been directed at the weakest link in the chain: the end user of online banking services.

Technological innovation has become a means of offering the best quality and convenience of service to customers. With online banking services, however, this user-friendly transparency and accessibility must go hand in hand with financial prudence to achieve success in the sector.

That's because it offers some advantages for cybercriminals as well, such as lax security on the end user's part, the ability to steal small amounts that may go unnoticed for a certain time, etc. However, it also presents certain drawbacks that stem from the need to find money-carrying 'mules', finding and infecting potential victims who are clients of attacked banks, or avoiding anti-malware solutions.

The million-dollar question is: where are the largest sums of money? They are, without a doubt, in the financial institutions themselves.

Recent changes put system vulnerabilities in the spotlight. **This is a new phase of cyber theft that involves stealing money directly from banks, rather than from their customers, using phishing attacks to infect the computers of bank employees.**

The tactic of directly attacking these entities can significantly raise the profits for attackers, but it also requires a lot of effort and planning on their part. Penetrating banks' security systems is a tricky task. It becomes even more complicated to profile the bank's internal systems in order to gain an understanding of how they work, and leave without a trace after carrying out the virtual heist. It requires a great investment to gather all the data needed for this type of attack. But of course, all the effort pays off if the attacker is able to make off with million-dollar bounties.

It is not easy for the financial sector to perform priority functions such as ensuring an efficient allocation of financial resources, contributing to the development and monetary stability of the country, or manage savings and investments. Nor is it easy to protect the data and accounts of customers.

Despite being a sector with cutting edge anti-malware solutions, both perimeter-based and for devices, **advanced attacks can compromise huge amounts of sensitive data at banking organizations.**

Legislation

The New Regulation: GDPR

Current legislation is not adapted to new cybercrimes, nor to the needs imposed by new technologies and IT management systems. The European Commission's General Data Protection Regulation (GDPR) enters into force on May 25, 2018 and will regulate how companies collect and process the personal data of residents throughout the European Union.

The impact on the financial sector will be significant, as any entity belonging to the EU and using its clients' personal data for marketing and sales purposes will be subject to the GPDR in less than one year. **If a financial institution does not comply with the GDPR, it could be penalized with a fine of up to 20 million euros or 4 percent of its annual international turnover, whichever is greater. IT teams lacking knowledge about the new regulation could end up being very costly for banks that leave their GDPR preparations for the last minute.**

In order to operate safely, the security of banking systems requires constant maintenance. Keeping in mind that one of the biggest problems facing the financial sector today is the protection of personal data against security breaches, having a protocol in place in the event of a cyberattack is essential. The GDPR requires transparency, and we recommend aligning business practices with it sooner rather than later.

It will affect businesses that process **the personal data of natural persons in EU Member States.**

It will be applicable **starting May 25, 2018.**

It will apply to the processing of **personal data of natural persons within the EU.**

Migrating to the Cloud

The financial sector is a complex multi-player industry regulated from several different angles. It is necessary to take into account both network security coverage and the information stipulated in different regulations such as NIST (National Institute of Standards and Technology), as well as the obligations imposed by local regulation.

Cloud computing is gradually being adopted within the European financial sector. However, the process of migrating to the cloud has not yet reached maturity. Although financial institutions and supervisory authorities seem to have a clear vision of the economic and technical benefits of the cloud, they remain cautious about the risk of losing control over data assets, and most still rely on their own infrastructure.

One of the biggest deterrents is based on the arguments of the European Central Bank and its national counterparts, as well as regulations such as the NITS, as these agencies are obliged to rigorously control the location and traceability of data, especially when it comes to confidential data.

Although the most common approach used by financial institutions is a hybrid of private and public cloud services, the regulation states that when dealing with business-critical data a private cloud is required. This mechanism is generally considered more apt for data-processing and is favored by national financial supervisory authorities as it provides greater control over data and operations.

The lack of formal guidelines for cloud-based services is hindering the adoption of cloud computing as a facilitator for innovation, even though it is widely advocated as such by the European Commission in the digital single market.

Cases of Million-Dollar Cyberheists

When cybercriminals first set their sights on the financial industry, they knew that their primary target would have to be the client. This is because clients had fewer security resources at their disposition, and stealing their identity in order to impersonate them would be relatively simple. In other words, the client is the weak link in the chain.

However, in the last two years sophisticated — and ambitious — groups have appeared, and they've taken it a step further. Their objective is to infiltrate the banking entities themselves in order to carry out million-dollar cyberheists.

Bangladesh Bank

One of the most striking examples of this was the heist of the Bangladesh Bank, when a group of hackers were successful in infecting the bank's systems with malware specifically created for the attack, and attempted to make a series of transactions amounting to $951 million. This sum could be found in the Bangladesh Bank's account at the New York Federal Reserve Bank. Fortunately, the majority of transfers were blocked before completion and the attackers made off with "only" $81 million dollars. But this is not the only case.

Tien Phong Bank

Tien Phong Bank, a commercial Vietnamese bank, suffered a similar attack in the final quarter of 2015. On this occasion, cyberattackers once again attempted to make transfers over the SWIFT network, but the bank noticed the transaction in time and was able to block over $1 million in transfers.

Banco del Austro

A few months earlier, in January 2015, an Ecuadorian bank, Banco del Austro, suffered a similar attack, and $9 million was stolen from them.

Bangladesh Bank
Bangladesh — **$81M**

Tien Phong Bank
Vietnam — **$1M**

Banco del Austro
Ecuador — **$9M**

In all of these cases, malware was used to carry out the attack and the money transfers were made over the SWIFT network. A direct attack against this network, which is used to make secure worldwide transfers, would be devastating. Fortunately, it would appear that SWIFT has not fallen victim to any successful attacks, as confirmed in a press release issued by the organization: "First and foremost we would like to reassure you again that the SWIFT network, core messaging services and software have not been compromised."

However, it all depends on your perspective: cybercriminals have, in fact, successfully used the SWIFT network to perpetrate these heists. And once again, they have taken aim at the weak link in the chain. SWIFT provides a secure system for banks to communicate with each other, but in the end every financial institution has its own internal system for communicating with this network. In much the same way that cybercriminals targeted end clients using banking Trojans, instead of targeting SWIFT itself they now target the banking institutions that connect to it.

The same group is responsible for all three of these heists, and as of today the evidence points to North Korea. In December 2016, it became known that SWIFT had sent an alert to its clients, as new cases of attacks were cropping up. According Stephen Gilderdale, head of SWIFT's Customer Security Program, in statements made to Reuters, banks using the SWIFT network — be they central banks or commercial banks — were attacked on a significant number of occasions since the Bangladesh Bank heist. **And 20% of them resulted in attackers successfully stealing funds.**

Another tactic that seems to be on the rise is the targeting of POS (Point of Sale) terminals to steal information from credit and debit cards. In our analysis of the hotel industry we saw how the majority of attacks against this sector came through malware that targeted POS terminals and aimed to steal clients' credit and debit card data. But this practice affects every area of commerce, from small restaurants to major supermarket chains.

At PandaLabs, we've analyzed different attacks carried out with malware specifically designed for this, such as the PunkeyPOS, where attackers had compromised establishments across the United States.

POS terminals affected by PunkeyPOS

You can find more information about other POS-oriented malware, such as Multigrain or PosCardStealer, in Panda Security's Mediacenter.

Trends in Financial Cybercrime

The first attacks against the financial sector came in 2003. At the time, online banking was becoming popular and the number of operations being carried out over the Internet multiplied rapidly. Measures taken by banking institutions to identify clients were very basic: with a simple username and password, you were able to access all of your data and make and kind of transaction.

The first attacks came primarily in the form of phishing, emails that pretended to come from banking institutions warning of a security flaw in the recipient's user credentials, and that the account would be frozen until the client goes to the webpage indicated in the email. Upon clicking the link, the client is taken to a fake website. Believing him or herself to be on a trusted bank website, the client introduces his or her credentials, which then fall right into the hands of the cybercrook.

About a year later, the first **banking Trojans** appeared on the scene. These Trojans had the same goal as phishing attacks —stealing the victim's identity in order to trick the bank into transferring funds into the desired account. But threats also became more sophisticated, and new Trojans appeared that were able to avoid protection techniques.

The techniques being used to steal data have gotten better, while banks, aware of the threats posed by these Trojans, have stepped up security on their websites. For example, banks have introduced virtual keyboards for user logins, which was a big step forward for online banking security. This way, a **keylogger** could not be used to capture the user's login information.

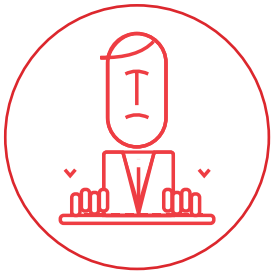
However, the creators of malware developed new functionalities for banking Trojans, giving them the ability to record mouse movements and even take screen captures and recordings, as was the case of Trj/Banbra.DCY.

Phishing

Creates a false URL to obtain your data and steal your identity

Banking Trojans

Installs various applications that allow hackers to take control of your computer and steal your information.



Keylogger

Records, stores, and sends every keystroke that users make on their keyboards.

Some examples, such as those belonging to the BankoLimb family, have a file with a list of URLs of target banks. When the user infected with BankoLimb accesses any website whose address coincides with a website on its list, the Trojan is activated, at which point it injects extra html code into the bank's website. In addition to the usual fields a user needs to fill out to log in, the user would need to provide further information. **The user is on the legitimate webpage, only slightly modified. For this reason, if a user accesses a bank's website and is asked for more information than usual, they should not trust the site or introduce any information, since it is possible that they've been infected with a Trojan and their movements will be captured.**

In other cases, Trojans superimpose a false page on the original so that the user is unaware that they are dealing with an imitation website. Once the user logs into the false website, they may receive an error message or be redirected to the real website, so that they don't get suspicious. Some variants of the Sinowal family of Trojans are truly sophisticated, with the ability to modify data "on the fly". For example, if a user is making a transfer through their bank's website, these variants of Trojan can modify the recipient of the transfer once the request is sent. What's more, the confirmation that is sent to the user will be doctored to reflect the original information of the transfer, so the user will be completely unaware that they've been swindled.

Other variants consult the server to find out if they need to carry out any sort of action in accordance with the websites being visited by the user. This way, the malware does not depend on a configuration file and the cybercriminal can expand or modify the list of websites where they would like to inject malicious code, or whose information they wish to steal, etc.

The more we access online banking systems through our smartphone, **the more hackers are willing to dedicate their resources to developing banking malware for Android that has the same goal as its PC counterpart.** A smartphone has an operating system, applications, etc., and, in short, is just another computer.

The number of families of banking malware is astounding. To simplify, we'll divide it into two main branches:

1. Brazilian

(Banbra, Banker, Bancos, etc.)

Their objectives are clients of Brazilian, South American, and sometimes Spanish and Portuguese banks. From a technology point of view they are not groundbreaking. They are at their most creative when designing social engineering techniques to deceive victims.

2. Russian

(Bankolimb, Zeus, Sinowal, SpyEye, Citadel, Dyreza, etc.)

Its objectives are mainly clients of European and North American banking entities. Historically they have been — and are — the most sophisticated at a technical level.

Many of them share a lot of resemblances, since it was in their heyday that the source code of Zeus was published, from which there arose a multitude of subfamilies: SpyEye, Citadel, Ice IX, Ramnit, Zberp, Kins, Murofet, GameOver (Zeus P2P), etc.

These attacks have been traditionally aimed at customers of financial institutions, as they are the weakest link in the chain and the easiest to compromise.

However, in recent years we've seen how criminal groups have diversified, and seek out money in other areas:

Computer-controlled POS terminals

As mentioned above, malware specifically created for these terminals does exist, and is used to steal information from debit and credit cards from terminals at restaurants, hotels, supermarkets, etc

ATMs

These are also nothing more than computers with a very specific purpose, and cases have been recorded in which hackers have infiltrated them to withdraw money directly. This can be achieved through direct manipulation of the machine (by installing, for example, card skimmers) or by compromising the bank's internal network and from there access its ATMs.

Banks

Of all possible victims, who has the most money? Of course, it's the banks themselves. These highly-sophisticated attacks require far greater resources and ingenuity to carry out, but the million-dollar payoffs make it worth the while for attackers.

Recommendations for avoiding Cyberheists

One of the most frustrating things for victims is the lack of information shared with them about the attack. For example, after the attack on the Bangladesh Bank, three samples of malware were recovered — and that is all that was left behind. The attackers surely used many other tools that were deleted after use, and of which the victims will never know a thing.

Knowledge is power, and knowing how an incident happened is key to fixing security flaws and anticipating future incidents. Having unlimited visibility of everything that happens on your IT infrastructure allows you to have complete control, and avoid potential attacks before they occur.

The inexistence of a common cyberspace, of regulations, of certification, of interoperability, and legal protection is one of the greatest obstacles facing banks looking to make the shift to cloud computing, a system which allows financial entities to obtain the benefits of software at a reduced cost, increased system performance, greater data fidelity, and universal access to documents, among other things.

So, how should cybersecurity software treat data stored on the cloud in order to be at its most effective in complying with regulations?

Information classified as "secret": the service should not access confidential personal information or information classified as "High Level" by the LOPD (Ley Orgánica de Protección de Datos, a Spanish organic law on the protection of personal data), or as "secret" by the banking institution. The only nuance could be that, indirectly, data regarding a company's use of IT resources as a result of user activity is gathered. This information could be included as a restriction in internal rules of conduct, and it may end up being the case that protection operators and banking staff have access to this information.

Information classified as "confidential": the service accesses user information classified as "Basic Level" by the LOPD. This information could be the user's login information (but not the password, which is never collected), the name of the device if it uniquely identifies the user, and the IP address of the computer, also if it uniquely identifies a user. This data is necessary for the service to function correctly and therefore it is understood that operators could be authorized to access such data.

These two characteristics underpin the security model of Adaptive Defense 360, the first advanced cybersecurity service to combine Next Generation protection (NG EPP) and technologies of detection and remediation (EDR) with the ability to classify 100% of running processes.

With this model, **banking institutions will be able to protect their main asset, the data and sensitive information of their clients, with a solution capable of detecting data leaks whether they come from malware or from the bank's own employees.** This is one of the most highly-valued abilities within this sector. Adaptive Defense 360 obtains data enriched by the SIEM, which allows for total visibility of each and every endpoint on workstations.

In addition to complying with the demanding current legislation in the sector and detecting and blocking any kind of attack targeting the system, **Adaptive Defense 360** allows for the discovery and resolution of vulnerabilities in the system and its applications, and also prevents the use of undesired programs such as navigation bars, adware, or add-ons.

Panda Security's corporate solution is part of a platform that uses contextual logic that analyzes, categorizes, and correlates cyberthreat data in order to carry out prevention, detection, response, and remediation tasks.

An advanced cybersecurity solution endorsed by AV- Comparatives and with the guarantee of all Panda Security products. **We're reinventing cybersecurity.**

Adaptive Defense 360

More information at:

BENELUX
+32 15 45 12 80
belgium@pandasecurity.com

BRAZIL
+55 11 3054-1722
brazil@pandasecurity.com

FRANCE
+33 (0) 1 46842 000
commercial@fr.pandasecurity.com

GERMANY (& AUSTRIA)
+49 (0) 2065 961-0
sales@de.pandasecurity.com

HUNGARY
+36 1 224 03 16
hungary@pandasecurity.com

ITALY
+39 02 24 20 22 08
italy@pandasecurity.com

MEXICO
+52 55 8000 2381
mexico@pandasecurity.com

NORWAY
+47 93 409 300
norway@pandasecurity.com

PORTUGAL
+351 210 414 400
geral@pt.pandasecurity.com

SOUTH AFRICA
+27 21 683 3899
sales@za.pandasecurity.com

SPAIN
+34 900 90 70 80
comercialpanda@pandasecurity.com

SWEDEN (FINLAND & DENMARK)
+46 0850 553 200
sweden@pandasecurity.com

SWITZERLAND
+41 22 994 89 40
info@ch.pandasecurity.com

UNITED KINGDOM
+44(0) 800 368 9158
sales@uk.pandasecurity.com

USA (& CANADA)
+1 877 263 3881
sales@us.pandasecurity.com

Adaptive Defense 360

Limitless Visibility, Absolute Control

pandasecurity.com

panda

More information at:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

by calling:

+27 21 683 3899

or by email sales@za.pandasecurity.com

panda