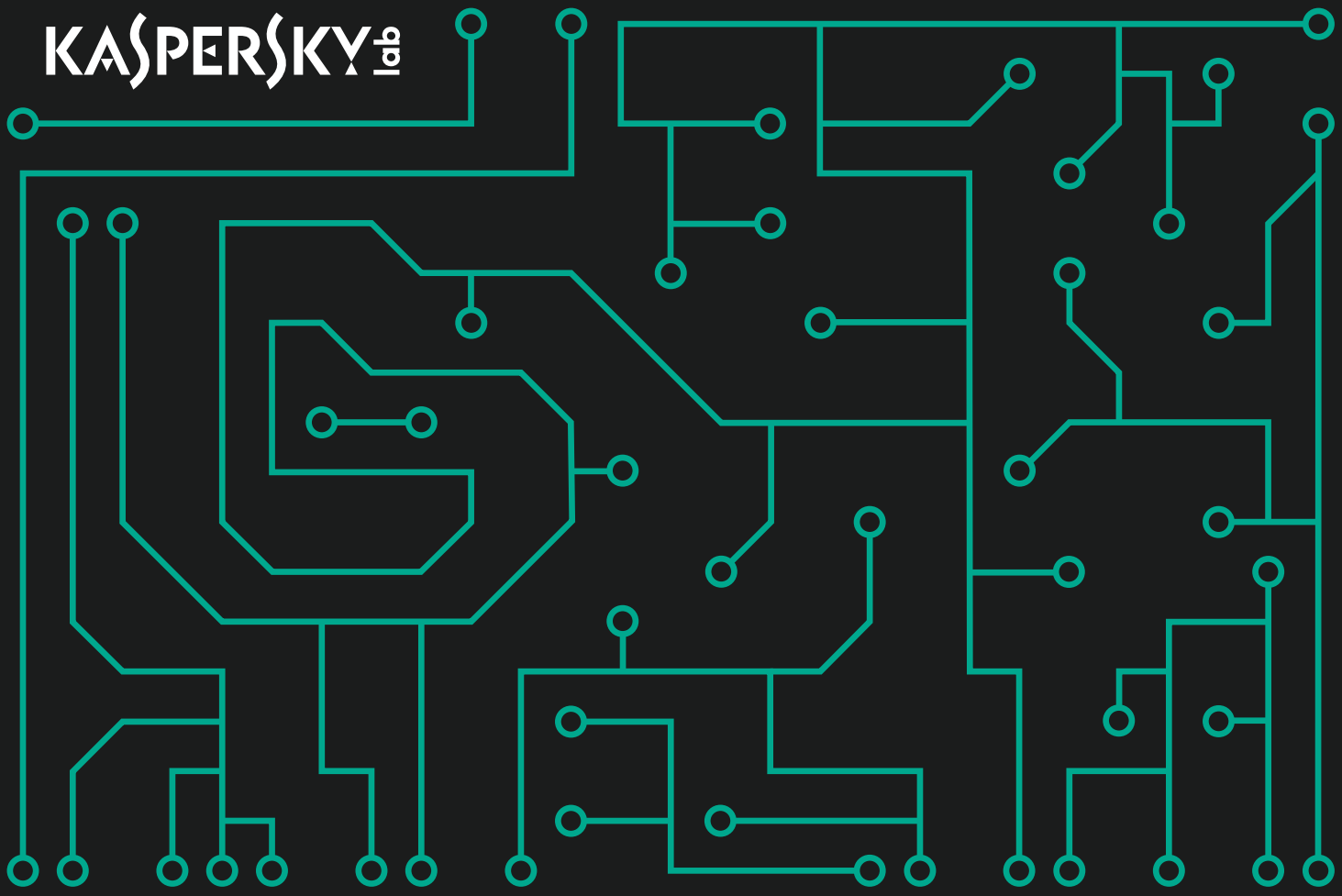
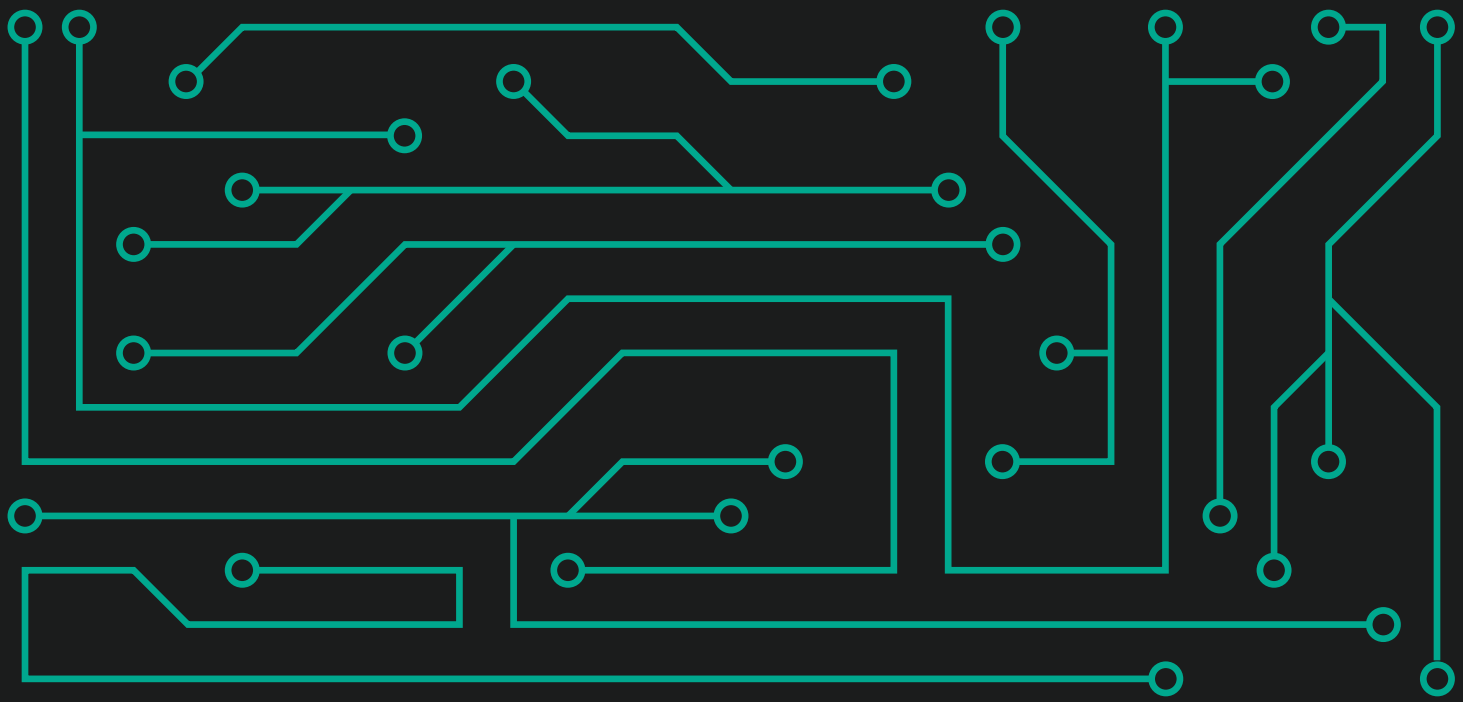
KASPERSKY lab



Cyberthreats to financial institutions 2019:

OVERVIEW AND PREDICTIONS



CONTENTS

INTRODUCTION – KEY EVENTS IN 2018

The past year has been extremely eventful in terms of the digital threats faced by financial institutions: cybercrime groups have used new infiltration techniques, and the geography of attacks has become more extensive.

Despite this, let's start the review with a positive trend: in 2018 police arrested a number of well-known cybercrime group members responsible for Carbanak/Cobalt and Fin7, among others. These groups have been involved in attacks on dozens, if not hundreds of companies and financial institutions around the world. Unfortunately, the arrest of group members including the leader of Carbanak, did not lead to a complete halt in activities – in fact, it seemingly started the process of splitting the groups into smaller cells.

The most active actor of 2018 was Lazarus. This group is gradually expanding its arsenal of tools and looking for new targets. The area of interest today includes banks, fin-tech companies, crypto-exchanges, PoS terminals, ATMs, and in terms of geography, we have recorded infection attempts in dozens of countries, most of which are located in Asia, Africa and Latin America.

At the end of last year, we noted that young fin-tech companies and crypto-exchanges are at a higher risk, due to the immaturity of their security systems. This certain type of companies was targeted most often. The most creative attack seen in 2018, from our point of view, was AppleJeus, which targeted cryptocurrency traders. In this case, criminals created special software that looked legitimate and carried out legitimate functions. However, the program also uploaded a malicious update that turned out to be a backdoor. This is a new type of attack, which infects its targets via the supply chain.

Continuing the topic of supply chain attacks, it is worth mentioning the MageCart group, which, by infecting website payment pages (including those of large companies such as British Airways) was able to access a huge amount of payment card data this year. This attack was even more effective because the criminals chose an interesting target – Magento, which is one of the most popular platforms for online stores. Using vulnerabilities in Magento, criminals were able to infect dozens of sites in a technique that is likely to be used by several other groups.

We should also note the development of ATM malware families. In 2018, Kaspersky Lab specialists discovered six new families, meaning that there are now more than 20 of this kind. Some ATM malware families have also evolved: for example, the Plotus malware from Latin America has been updated to a new version, Peralda, and has gained new functionality as a result. The greatest damage associated with attacks on ATMs was caused by infections from internal banking networks, such as FASTCash and ATMJackPot, which allowed attackers to reach thousands of ATMs.

2018 also saw attacks on organizations that use banking systems. Firstly, our machine learning-based behavioral analysis system detected several waves of malicious activity related to the spread of the Buhtrap banking Trojan this year, as attackers embedded their code in popular news sites and forums. Secondly, we detected attacks on the financial departments of industrial companies, where payments of hundreds of thousands of dollars would not cause much suspicion. Often in the final stages of attacks like this, attackers install remote administration tools on infected computers such as RMS, TeamViewer, and VNC.

Before giving our forecasts for 2019, let's see how accurate our forecasts for 2018 turned out to be...

- **Attacks made through the underlying blockchain technologies of financial systems implemented by the financial institutions themselves** – this did not happen in the financial field, but was seen in the online casino sector.
- **More supply chain attacks in the financial world** – yes
- **Attacks on mass media (in general, including Twitter accounts, Facebook pages, telegram channels and more) including hacks and manipulation for getting financial profit through stock/crypto exchange trade** – yes
- **ATM malware automation** – yes. For example, there are malicious programs that immediately give money to attackers.
- **More attacks on crypto exchange platforms** – yes
- **A spike in traditional card fraud due to the huge data breaches that happened in the previous year** – no
- **More nation-state sponsored attacks against financial organizations** – yes
- **The inclusion of fin-techs and mobile-only users in attacks: a fall in the number of traditional PC-oriented internet banking Trojans, with novice mobile banking users becoming the new prime target for criminals** – yes. In particular, some banking Trojans stopped attacking users of online banking on PCs, while the number of Trojans attacking users of mobile devices has more than doubled over the past year.

PREDICTIONS FOR 2019

- **The emergence of new groups due to the fragmentation of Cobalt/Carbnal and Fin7: new groups and new geography**

The arrest of leaders and separate members of major cybercrime groups has not stopped these groups from attacking financial institutions. Next year, we will most likely see the fragmentation of these groups and the creation of new ones by former members, which will lead to the intensification of attacks and the expansion of the geography of potential victims.

At the same time, local groups will expand their activities, increasing quality and scale. It is reasonable to assume that some members of the regional groups may contact former members of the Win7 or Cobalt group to facilitate access to regional targets and gain new tools with which they can carry out attacks.

- **The first attacks through the theft and use of biometric data**

Biometric systems for user identification and authentication are being gradually implemented by various financial institutions, and several major leaks of biometric data have already occurred. These two facts lay the foundation for the first POC (proof-of-concept) attacks on financial services using leaked biometric data.

- **The emergence of new local groups attacking financial institutions in the Indo-Pakistan region, South-East Asia and Central Europe**

The activity of cybercriminals in these regions is constantly growing: the immaturity of protective solutions in the financial sector and the rapid spread of various electronic means of payment among the population and companies in these regions are contributing to this. Now, all the prerequisites exist for the emergence of a new center for financial threats in Asia, in addition to the three already in Latin America, Korean peninsula and the ex-USSR.

- **Continuation of the supply-chain attacks: attacks on small companies that provide their services to financial institutions around the world**

This trend will remain with us in 2019. Attacks on software providers have proven effective and allowed attackers to gain access to several major targets. Small companies (that supply specialized financial services for the larger players) will be jeopardized first, such as the suppliers of money transfer systems, banks and exchanges.

- **Traditional cybercrime will focus on the easiest targets and bypass anti-fraud solutions: replacement of PoS attacks with attacks on systems accepting online payments**

Next year, in terms of threats to ordinary users and stores, those who use cards without chips and do not use two-factor authorization of transactions will be the most at risk. The malicious community has focused on some simple goals that are easy to monetize. However, this does not mean that they do not use any complex techniques. For example, to bypass anti-fraud systems, they copy all computer and browser system settings. On the other hand, this cybercriminal behavior will mean that the number of attacks on PoS terminals will decrease, and they will move towards attacks on online payment platforms instead.

- **The cybersecurity systems of financial institutions will be bypassed using physical devices connected to the internal network**

Due to the lack of physical security and the lack of control over connected devices in many networks, cybercriminals will more actively exploit situations where a computer or mini-board can be installed, specifically configured to steal data from the network and transfer the information using 4G/LTE modems.

Attacks like this will provide cybergangs with an opportunity to access various data, including information about the customers of financial institutions, as well as the network infrastructure of financial institutions.

- **Attacks on mobile banking for business users**

Mobile applications for business are gaining popularity, which is likely to lead to the first attacks on their users. There are enough tools for this, and the possible losses that businesses incur are much higher than the losses incurred when individuals are attacked. The most likely attack vectors are attacks at the Web API level and through the supply chain.

- **Advanced social engineering campaigns targeting operators, secretaries and other internal employees in charge of wires: result of data leaks**

Social engineering is particularly popular in some regions, for example Latin America. Cybercriminals keep targeting specific people in companies and financial institutions to make them wire big sums of money. Due to high amount of data leakages previous years this type of attacks becomes more effective, since criminals are able to use leaked internal information about targeted organization to make their messages look absolutely legit. Main idea remains the same: they make these targets believe that the financial request has come from business partners or directors. These techniques use zero malware, but demonstrate how targeted social engineering gets results and will become more powerful in 2019. This includes attacks like "simswap".