POSITIVE TECHNOLOGIES

BANK ATTACKS

2018

CONTENTS

INTRODUCTION

Judging by the media headlines, it's a golden age for bank robberies. The names of criminal gangs are often known to every security specialist, and some of these thieves have made off with millions on multiple occasions. High payoffs and the relatively low risk of detection are inspiring criminals to "go online." Some groups break up or are caught by law enforcement, but newer groups pop up with more sophisticated attack techniques and take their place.

Criminals quickly adapt to the changing environment; they constantly monitor newly published vulnerabilities and manage to exploit them much faster than bank security services are able to install updates. On underground web forums, anyone can freely purchase software to conduct an attack (with detailed "how to" instructions), as well as make the acquaintance of unscrupulous bank employees and money launderers. If properly prepared, an attacker with minimal technical knowledge can steal millions of dollars by penetrating a bank network, although it might seem that such networks should be protected quite well.

So what is the actual situation with IT security at banks? How do hackers bypass their security systems? What are the security flaws that allow hackers to entrench themselves in bank infrastructure and commit fraud, remaining unnoticed up to the very last moment?

This reporting draws upon security analysis of information systems performed by Positive Technologies for specific banks for the past three years. The findings indicated here do not necessarily reflect the current state of other companies in the same sector. Rather, this information is intended to promote a better understanding among information security specialists of the most relevant issues in a particular sector, as well as assist in timely detection and remediation of vulnerabilities. We will start with examples of attacks and known gangs that have been active in the past three years, as well as dissect the scheme of a standard attack on bank infrastructure. Then we will present the results obtained by Positive Technologies experts in penetration testing: their findings illustrate which vulnerabilities are common at banks, and which of them make attacks possible. In conclusion, we will attempt to estimate the potential for victimization of banks by criminal groups, taking into account the vulnerabilities observed on bank systems.

BANK ROBBERIES IN THE DIGITAL AGE

In early 2018, President of the World Economic Forum announced that worldwide losses from cyberattacks approached USD 1 trillion.

In the wild, we currently see attacks on interbank transfers, card processing, ATM management, e-banking, and payment gateways. The range of targets is broad—if intruders have the necessary knowledge and technical means, access to such systems can bring them more revenue than fraud against bank customers. To steal money, criminals need to penetrate the bank's infrastructure, which is usually quite well-guarded. Nonetheless, criminals still manage to bypass all protection mechanisms, and the media continue to report new bank cyberattacks and thefts.

Theft examples

$100 million

In early 2017, there was a surge of attacks targeting card processing in Eastern Europe. Having penetrated the bank's infrastructure, criminals obtained access to card processing systems and increased card overdraft limits. They also disabled antifraud systems that would ordinarily notify the bank of fraudulent transactions. Simultaneously, their accomplices were withdrawing cash from ATMs in another country. Money mules directly responsible for cash withdrawal had previously acquired bank cards with forged documents and traveled outside the country in which the victim bank was located. In each case, the average theft amount was approximately $5 million. Two years earlier, similar tactics were applied by the Metel gang. Having penetrated a bank's infrastructure, the criminals were able to cancel card transactions and reset balances while their accomplices moved from one ATM to another, stealing millions of rubles.

$60 million

In the fall of 2017, intruders attacked the Far Eastern International Bank in Taiwan by making transfers to accounts in Cambodia, Sri Lanka, and the U.S.

$4 million

While banks in Nepal were closed for holidays, criminals used SWIFT to withdraw money. The banks were able to track transactions and recover a significant portion of the stolen funds only due to timely response.

$1.5 million

In early December, public sources began to mention the MoneyTaker gang, which had attacked financial institutions in Russia and in the United States for a year and a half. Criminals attacked card processing and interbank transfer systems, with thefts averaging $500,000 in the U.S. and RUB 72 million (~$1.26 million) in Russia.

$100 thousand

In December 2017, reports surfaced about the first successful SWIFT attack on a Russian bank. The victim of the hacking attack was Globex, a subsidiary of VEB. The suspect is the Cobalt hacker gang, which specializes in cyberattacks on banks.

Criminal gangs

Some of the most active criminal gangs in the past three years are Cobalt (likely related to Buhtrap), Carbanak, Lazarus, and Lurk.

The Cobalt gang is known for its attacks on financial institutions in the CIS, Eastern Europe, and Southeast Asia. But in 2017, the group expanded its reach to attack Western Europe, and North and South America. Most of the attacked financial institutions are banks, but they also include stock exchanges, investment funds, and other specialized financial institutions. At banks, their objective is to take control of ATMs by sending cash dispensing commands at a certain time: the intruders empty ATMs of cash without having to physically interfere with ATM operation.

No less famous is the Lazarus gang, which is credited with one of the most audacious bank robberies through the SWIFT system. In 2016, the group attempted to take a billion dollars from the Central Bank of Bangladesh, but they were able to steal only $81 million because of a mistake in the payment documentation.

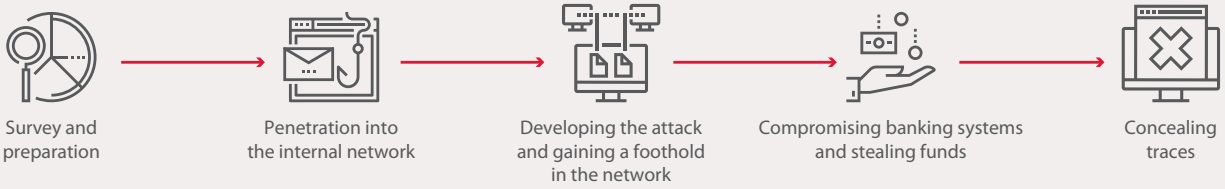
Media discussion of the Carbanak gang intensified after a series of thefts in 2014–2015. The group is notable for its broad specialization: they managed to steal money from any systems they accessed, even though they exclusively exploited security flaws on corporate networks. The total amount of stolen funds exceeded $1 billion.

Information security specialists are also familiar with the Lurk Trojan, which has been used for several years to attack remote banking systems. Members of the relevant criminal gang were arrested in 2016. It is believed that in total, hackers withdrew more than RUB 3 billion (~$52.5 million) from banks.

Typical attack scheme

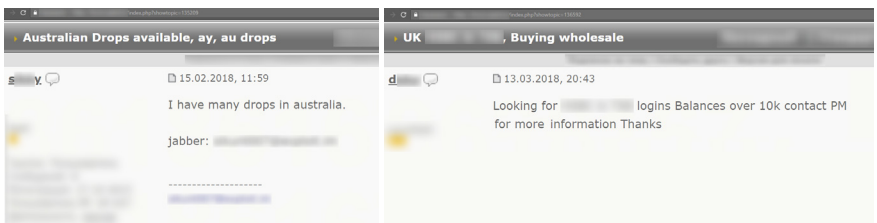
Intruders choose their target largely based on their technical expertise, available tools, and knowledge of internal banking processes. Each attack is slightly unique: for example, attackers may act differently at the money withdrawal stage. However, there are also common features that we will discuss in this section. Attackers operate according to rather simple scenarios consisting of the five main stages shown in the flowchart below.

Main attack stages

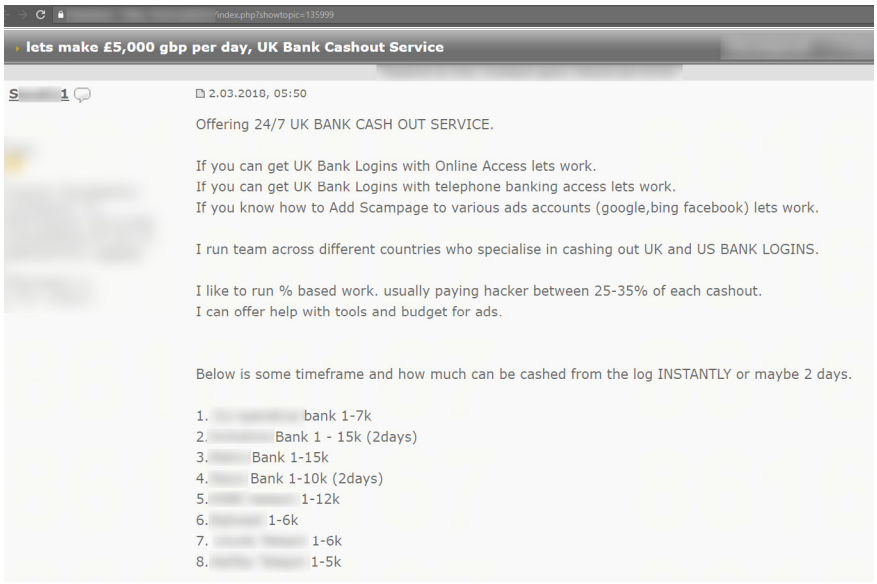


Stage 1. Survey and preparation

The first stage is rather lengthy and time-consuming: attackers are faced with the task of gathering as much information about the bank as possible to breach security systems and "case" the targeted bank. Since use of external resources can be detected by security systems, in order not to get caught during this initial stage, criminals resort to passive methods of obtaining information: for example, identifying domain names and addresses belonging to the bank. At the survey stage, unscrupulous bank employees are actively engaged as well. These insiders are prepared to disclose information for a fee, as shown by numerous offers on web forums.



Web advertisements to look for accomplices



lets make £5,000 gbp per day, UK Bank Cashout Service

2.03.2018, 05:50

Offering 24/7 UK BANK CASH OUT SERVICE.

If you can get UK Bank Logins with Online Access lets work.
If you can get UK Bank Logins with telephone banking access lets work.
If you know how to Add Scampage to various ads accounts (google,bing facebook) lets work.

I run team across different countries who specialise in cashing out UK and US BANK LOGINS.

I like to run % based work. usually paying hacker between 25-35% of each cashout.
I can offer help with tools and budget for ads.

Below is some timeframe and how much can be cashed from the log INSTANTLY or maybe 2 days.

1. bank 1-7k
2. Bank 1 - 15k (2days)
3. Bank 1-15k
4. Bank 1-10k (2days)
5. 1-12k
6. 1-6k
7. 1-6k
8. 1-5k

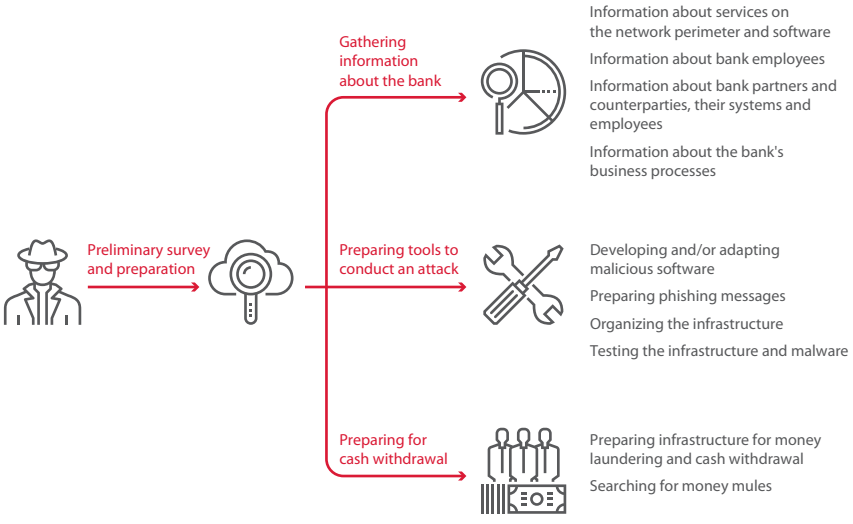
Web advertisements to look for accomplices

An attacker collects the following information about the bank:

+ Information about network perimeter systems and software
+ Employees (including email addresses, telephones, positions, and names)
+ Partners and contractors, as well as their systems and employees
+ Business processes

Examples of preparatory actions:

+ Developing or adapting malicious software for the software and OS versions used in the bank
+ Preparing phishing emails
+ Setting up infrastructure (including domain registration, server rental, and purchase of exploits)
+ Preparing the infrastructure for money laundering and cash withdrawal
+ Searching for money mules
+ Testing the infrastructure and malicious software

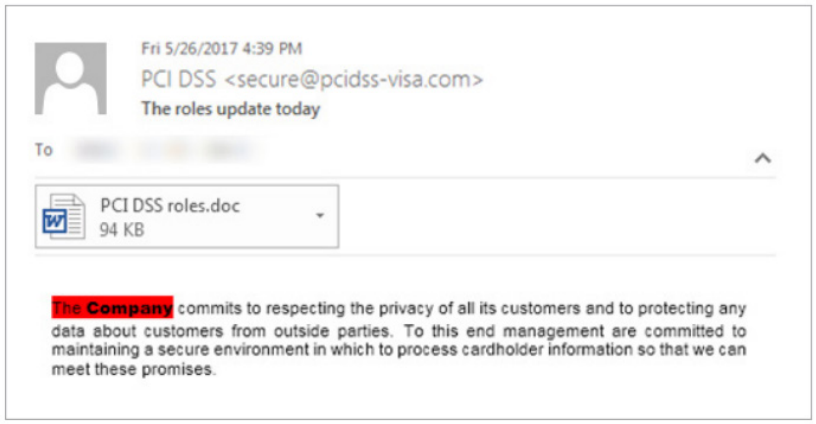


Stage 1. Survey and preparation

When building an infrastructure and preparing tools for an attack, attackers can both use their own knowledge (develop exploits in-house) or hire third parties. They can also buy ready-made tools and adapt them to their specific targets. For a group not planning to steal money from ATMs, connections with criminal groups active in large-scale money laundering would be essential.

Stage 2. Penetrating the internal network

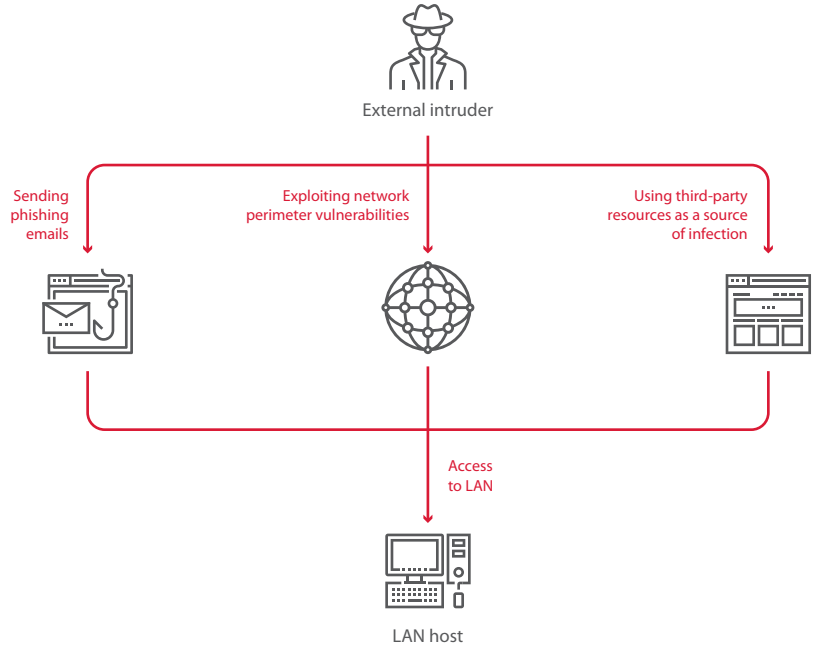
After thorough examination of the victim and preparation, attackers go on the offensive.



An example of a phishing email targeted at bank employees

Today, large and medium-sized banks pay plenty of attention to protecting their network perimeter. So it is both difficult and risky to organize attacks on servers or web applications, since the attackers are very likely to get caught. The most common and effective method of penetrating the bank's infrastructure is to send phishing emails to bank employees at either work or personal addresses. This method has been used by the Cobalt gang, for example, as well as Lazarus, Metel, and GCMAN.

Another way of initial target infection with malicious software is performed by hacking third-party companies that do not carefully protect their resources and infecting websites often visited by employees of the target bank, as we saw in the case of Lazarus and Lurk.



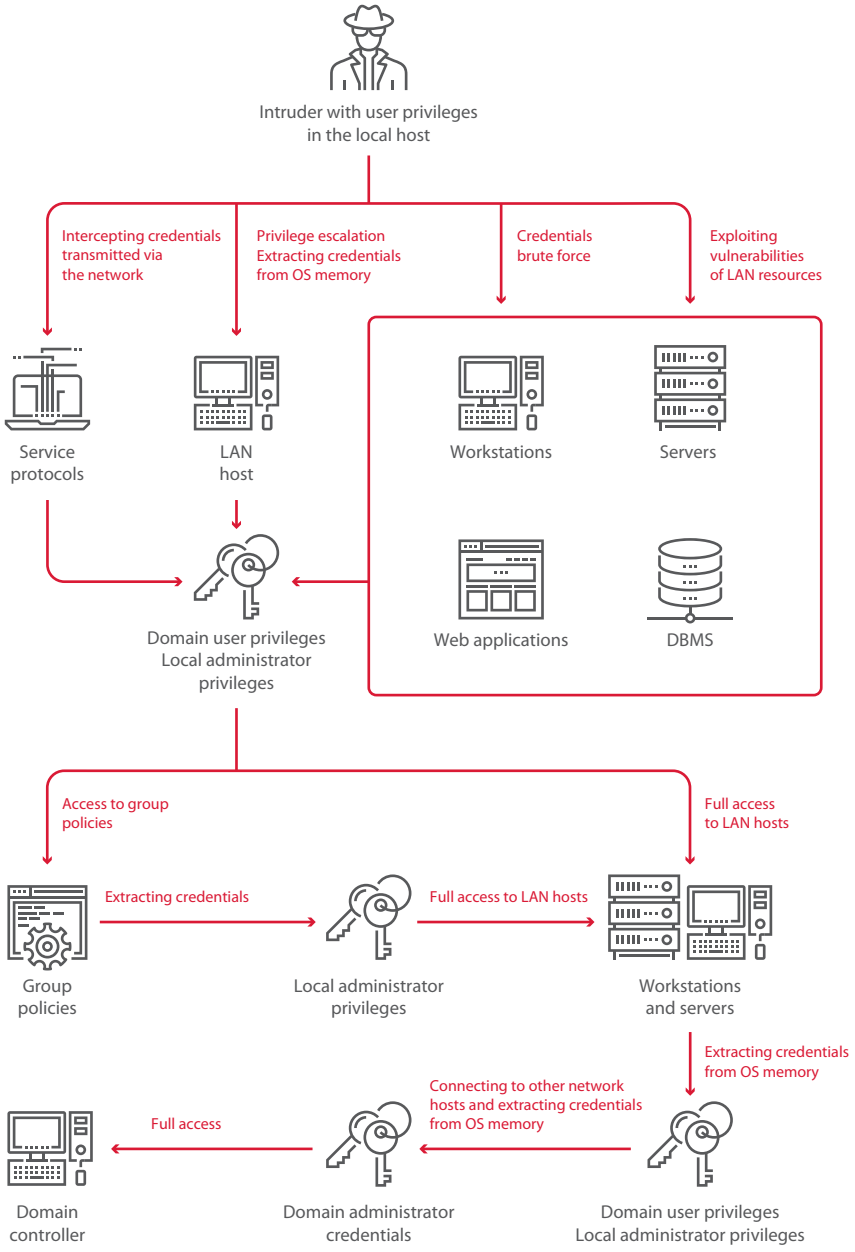
Stage 2. Penetrating the internal network

Stage 3. Developing the attack and gaining a foothold in the network

Once criminals have gained access to the bank's intranet, they need to obtain local administrator privileges on employee computers and servers to continue their attack. Success of attacks is due to insufficient system protection against internal intruders. Common vulnerabilities are as follows:

+ Use of outdated software versions and failure to install OS security updates
+ Configuration errors (including excessive user and software privileges, as well as setting local administrator passwords through group policies)
+ Use of dictionary passwords by privileged users
+ Absence of two-factor authentication for access to critical systems

After gaining maximum privileges on the host, criminals can access the OS memory in order to learn the credentials of all logged in users (usernames, passwords, or hash values of passwords). This data is then used to connect to other computers on the network.



Stage 3. Developing the attack and gaining a foothold in the network

Moving among hosts is usually done with legitimate software and built-in OS functions (for example, PsExec or RAdmin). Since these are tools used by corporate system administrators on a daily basis, they are unlikely to cause suspicion. The Cobalt gang also resorted to use of phishing messages within the bank by sending letters from real employees' workstations.

Local administrator privileges are used according to a typical scheme: an attacker copies memory of the lsass.exe process and uses it to extract passwords of OS users (or their hash values) using the mimikatz tool. Such actions are not detectable by antivirus software because legitimate tools are used to copy memory (for example, ProcDump) while mimikatz runs on the attacker's laptop. In addition, attackers can use Responder to attack network protocols and intercept credentials. Such methods of spreading throughout the network are given in more detail in our previous report.

If attackers manage to gain domain administrator privileges, they can continue to navigate freely through the network and monitor employees' computers, servers, and infrastructure services of the bank. With this level of privileges, it is very easy to gain access to the organization's business systems and banking software—it is enough to identify workstations of employees who have such access and connect to them. Using the golden ticket technique, attackers can safely gain a foothold in the corporate system and stay there for a long time.

To disguise their presence, attackers often use bodyless malicious code that resides in RAM only. Attackers retain remote control after computer restarts by adding malicious software to the list of startup programs.

Stage 4. Compromising banking systems and stealing funds

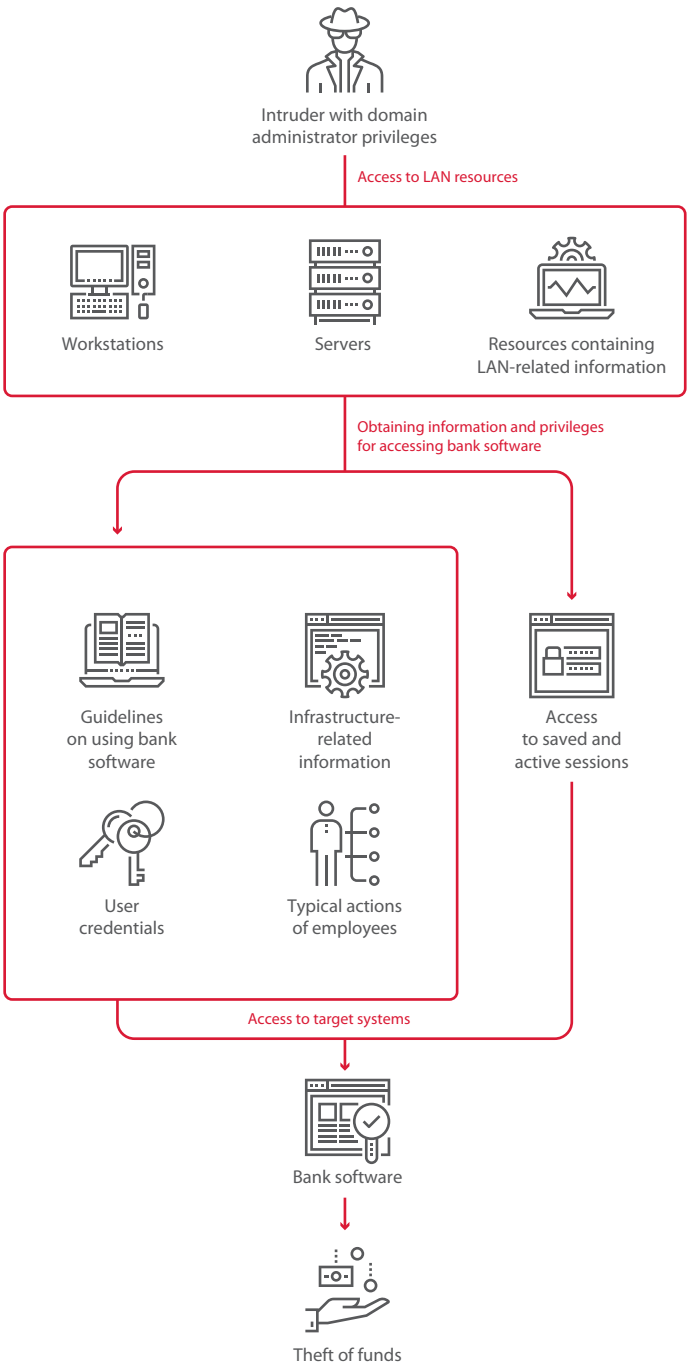
After gaining a foothold in the network, criminals need to understand on which hosts the target banking systems are located and find the most convenient ways to access them. Criminals examine users' workstations in search of files indicating that a particular workstation has worked with bank applications. To store passwords for critical systems on corporate networks, specialized software is usually used. An intruder with local administrator privileges can copy the memory dump of this process, extract passwords for accessing application or encrypted databases, and then obtain cleartext passwords to all critical bank applications, including the core banking system, SWIFT, and ATM management workstations.

Such an attack scenario is very effective and has been successfully implemented during penetration testing on multiple occasions. Additional support for criminals can be provided by resources that contain information about the infrastructure: for example, monitoring systems that administrators use in their work or technical support resources for users. This data increases the confidence of intruders in their knowledge of the internal network structure and helps them to take into account operational details of the bank's business processes during the attack, so as not to raise suspicions or trigger detection.

Criminals can lurk in a bank's infrastructure for months or even years, remaining stealthy as they collect information about the infrastructure and processes, leisurely examine the systems selected for attacks, and observe employees' actions. This means that theft can be prevented if compromises are detected quickly, even after criminals have already penetrated the bank network and gained a foothold.

The main methods of theft are:

+ Transferring funds to fictitious accounts through interbank payment systems
+ Transferring funds to cryptocurrency wallets
+ Controlling bank cards and accounts
+ Controlling ATM cash dispensing



Stage 4. Compromising banking systems and stealing funds

Stage 5. Concealing traces

To impede investigation of incidents, criminals conceal their traces. Although many attackers use RAM-resident malware, signs of their presence in the system still remain: entries in event logs, changes in the registry, and other hooks. Therefore, some intruders prefer to take a less surgical, and rather more blunt, approach by erasing boot records and hard disk partition tables on network hosts, disabling them entirely. The surge of cryptoware attacks in 2017 is one prominent example of how a large company's data can be easily destroyed. Currently, hackers' arsenals include virus modifications that can spread to network workstations and encrypt the hard disk. Since it is usually not possible to recover the encrypted data, the bank suffers damages caused by the forced downtime of business processes, which may actually far exceed the losses caused by the theft of funds itself. Since, by this point in the attack, the criminals likely have the highest privileges and thorough knowledge of the system, stopping them at this stage is next to impossible.

PENETRATION TEST RESULTS

We have looked at how intruders attack banks. In this section, we will share the vulnerabilities that are typically detected during penetration tests and discuss the probability of the attacks described above.

Penetration testing assesses the actual (as opposed to theoretical) level of an organization's security by simulating the actions that a real intruder would perform. Depending on the initial level of the intruder's privileges, external testing determines the probability of breaching the network perimeter, while internal testing aims to gain full control over the infrastructure or obtain access to critical systems. Every year, we perform dozens of penetration tests for various organizations. In this study, we will share the 12 most instructive penetration tests that we have carried out for banks over the past three years in which our experts were able to apply a wide range of methods.

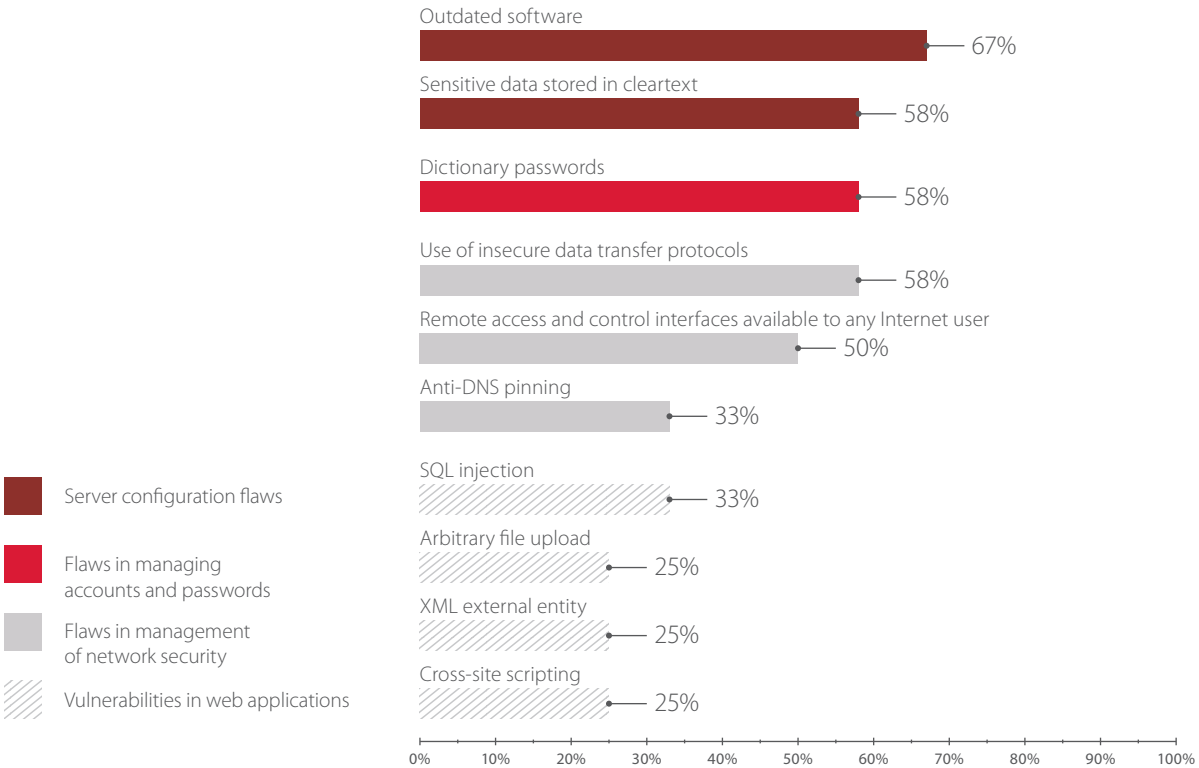
At 100% of banks,
we found:

+ Vulnerabilities in web applications
+ Insufficient network security
+ Server configuration flaws

At 58% of banks,
we found deficiencies in user account and password management

Network perimeter vulnerabilities

The main vulnerabilities and flaws in security mechanisms common on the bank network perimeter can be divided into four categories: vulnerabilities in web applications, insufficient network security, server configuration flaws, and deficiencies in user account and password management.



Ten most common vulnerabilities on the network perimeter (percentage of banks)

At 22% of banks, experts successfully breached the network perimeter in external penetration testing

Note that the presence of vulnerabilities on the system perimeter does not necessarily mean that their exploitation would allow penetrating the internal network. Overall, the network perimeter of banks is much better protected than in other industries. In the last three years in external penetration testing, access to the internal network was obtained in 58 percent of tests; for banks, this figure was a mere 22 percent. In all these cases, access was facilitated due to vulnerabilities in web applications that made it possible for an intruder to reach their goal in only one step. At one bank, two penetration vectors were identified, both of which involved exploiting vulnerabilities in web applications and web server configuration flaws.

Consequently, criminal gangs planning to penetrate a bank's internal network by exploiting vulnerabilities in the network perimeter could reach their goal at 22 percent of banks. Such methods have been used by various gangs, including ATMitch and Lazarus.

This percentage may be an underestimate, however. The testers do not exploit vulnerabilities that could damage the customer's infrastructure. For example, the use of outdated software at 67 percent of banks has the potential to allow breaching the perimeter, but actually exploiting these vulnerabilities could cause denial of service (for instance, CVE-2012-2386, CVE-2013-6420, and CVE-2015-5343).

The external network perimeter also demonstrates flaws related to network security. The most hazardous are remote access and control interfaces, which can often be easily accessed by any external user. Among the most common are the SSH and Telnet protocols, which occur on the network perimeter at 58 percent of banks, as well as protocols for access to file servers, present at 42 percent of banks.

As already noted, most banks have a rather secure network perimeter, but staff are usually the weakest link in any organization's security stance.

75% of banks
are vulnerable to social engineering attacks

In our testing of staff security awareness, employees at 75 percent of banks clicked the link in a phishing message; at 25 percent of banks, employees entered their credentials in a fake authentication form, and at 25 percent of banks, at least one employee ran a malicious attachment on their work computer. On average, about 8 percent of bank users clicked a phishing link, 2 percent ran a malicious file, and less than 1 percent of users entered their credentials.

Although security awareness among bank employees is still higher than in other industries, it takes only one confused or harried user to inadvertently give corporate network access to an intruder. The results of our testing show that three quarters of banks are vulnerable to social engineering attacks, which have been used to breach the perimeter by virtually every criminal gang, including Cobalt, Lazarus, and Carbanak.

Regular security training coupled with awareness testing brings excellent results. The experience at a client bank provides an encouraging example. Testing in 2016 revealed that some users had entered their credentials in a fake authentication form; if the attack had been real, criminals would have been able to obtain the information needed to access the bank's resources. In testing a year later, the situation changed drastically: not a single employee entered their credentials.

Internal network infrastructure

At 100% of banks,
full control over infrastructure was obtained

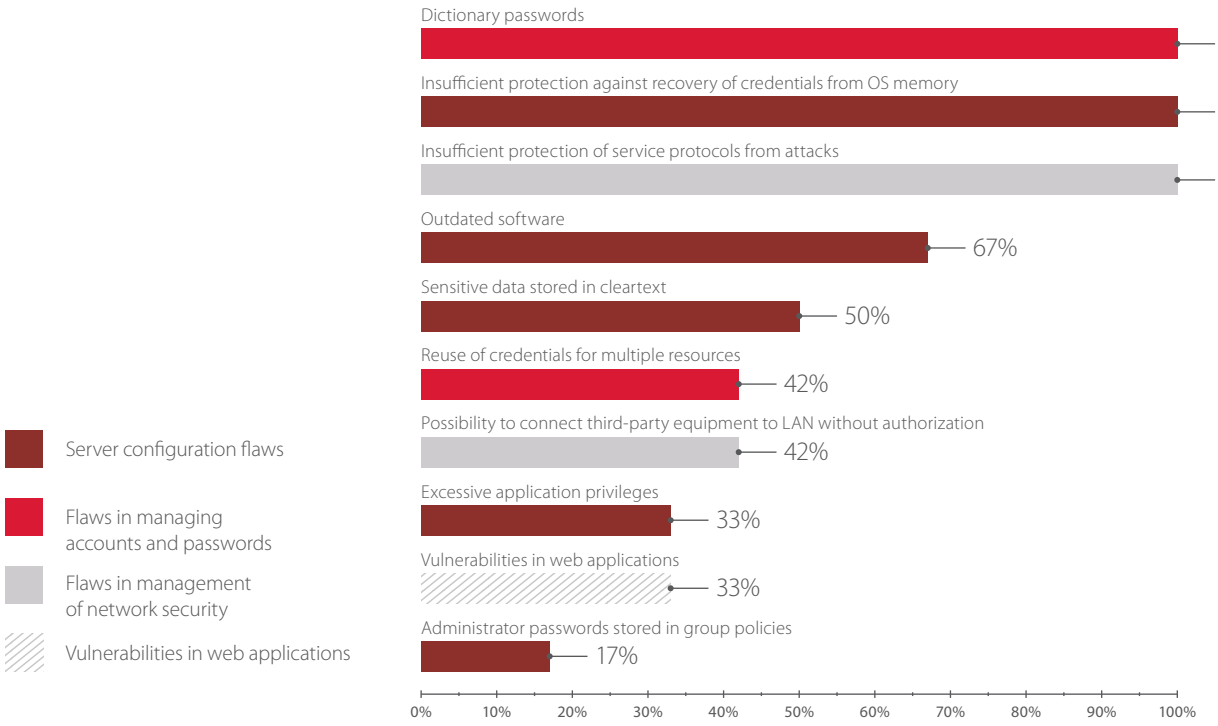
While banks are focused on protecting the network perimeter, internal network security is far from perfect. Their internal networks suffer from the same problems as at other companies. Full control over infrastructure was obtained at all tested banks. At the same time, at 33 percent of banks, intruders do not even need to have maximum privileges to obtain access to the hosts that control ATMs, interbank transfer and card processing systems, and payment gateways.

Which security flaws allow criminals to pursue their attacks deep into the banking infrastructure? The following chart shows the frequency of vulnerabilities exploited to gain complete control over domain infrastructure during internal penetration testing. Percentages refer to the percentage of tested systems that contained a given vulnerability.

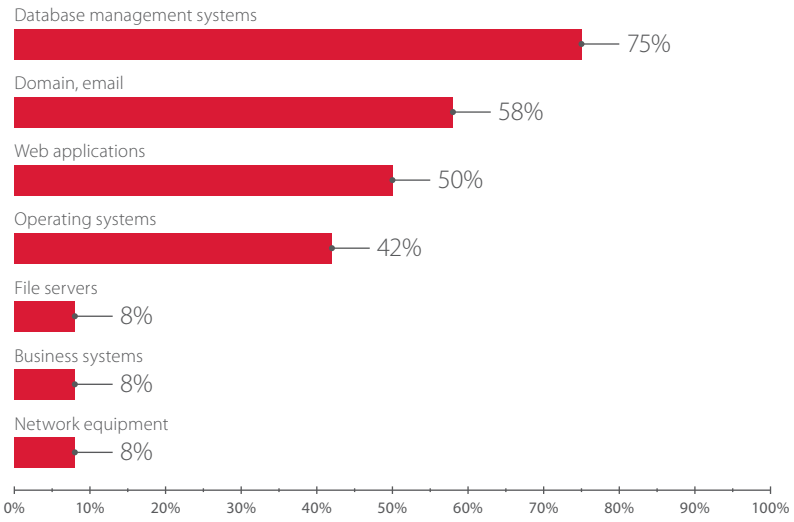
Typical attack vectors stem from two major flaws—a weak password policy and insufficient protection against password recovery from OS memory.

While dictionary passwords are used on the network perimeter at 50 percent of banks, each system suffers from a weak password policy on the internal network. In this regard, banks are similar to almost any other industry. On about half of the systems, weak passwords are set by users. However, we increasingly come across default accounts (with predictable passwords) left by administrators after installing database management systems, web servers, or operating systems or creating

corporate accounts. Very often, applications either have excessive privileges or contain known vulnerabilities. As a result, intruders have the opportunity to obtain administrative rights in just one or two steps.



Most common vulnerabilities on the internal network (percentage of banks)



Internal network components for which dictionary passwords are used (percentage of banks)

As we found, a quarter of banks used the password "P@ssw0rd" as well as such common combinations as "Qwerty123," empty passwords, and default passwords (for example, "sa" or "postgres").

We detected insufficient security measures and, frequently, their complete absence when it comes to protecting service protocols. Protection against attacks on the NBNS protocol was not at place at a single bank, while protection against LLMNR attacks was missing at 70 percent of banks. Some 80 percent of banks were exposed to ARP Poisoning attacks. At the same time, interception of credentials transmitted over the network can be successfully used by intruders for collecting information about the system. For example, at some banks, penetration testing managed to intercept several NetNTLMv2 hash values of domain user passwords in

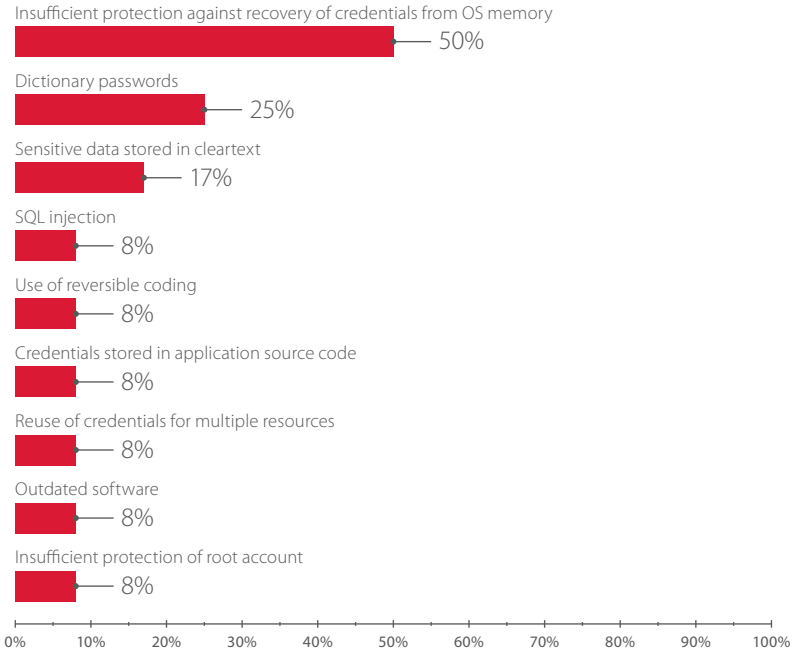
At 58% of banks,
experts obtained access to banking systems

Challenge–Response format. Then, using those hash values we discovered domain account passwords.

At the stage of spreading and getting a foothold in the network, intruders' actions are quite similar because they are the exploiting vulnerabilities of any corporate system. Based on the above results, we can safely assume that any criminal group would be able to gain full control over the domain infrastructure at each of the tested banks. Therefore, although banks are sufficiently well protected from the outside, intruders are likely to succeed in attacking banking systems if they obtain access to the internal network. Such access can be obtained in different ways: for example, an accomplice can get a job at a bank as an employee with minimal network privileges or merely physical access to the network (such as a janitor or security guard).

We managed to obtain access to banking applications at 58 percent of banks. Operating within the agreed scope of work, the testers did not develop attacks on the critical hosts of other banks. However, domain administrator privileges would allow an attacker to gain a foothold in the system and perform attacks on targeted resources.

Below are the vulnerabilities that made it possible to gain access directly to bank software.



Vulnerabilities used to access banking software

At 25 percent of banks, the hosts from which ATMs were controlled became compromised, so Cobalt could withdraw money from such ATMs.

Transferring funds to criminal-controlled accounts through interbank transfer systems, as done by Lazarus and MoneyTaker, was possible at 17 percent of banks.

At 17 percent of banks, card processing systems are not sufficiently protected, which allows manipulating the balance on intruders' card accounts, as we saw in early 2017 in the case of attacks on Eastern European banks.

4 steps
are required for an intruder to obtain access to bank software

The Carbanak gang, capable of attacking nearly any banking application, could have made off with funds from 58 percent of banks.

On average, an attacker who has penetrated the bank's internal network needs to take only four steps to gain access to the banks' electronic crown jewels.

CONCLUSION

Today, banks have built effective barriers for protection against external attacks, but they have not done nearly as much work to fight the threats on their internal networks.

Knowing this, attackers can easily bypass the network perimeter with a simple and efficient method: phishing delivers malware into the corporate network to unwitting employees. Criminals carefully monitor publication of new vulnerabilities and quickly modify their tools to take advantage. For example, in 2017, Cobalt hackers used vulnerabilities in Microsoft Office (CVE-2017-0199 and CVE-2017-11882), expecting that banks had not managed to install appropriate security updates. Inside the network of a target bank, the intruders are able to move freely using known vulnerabilities and legitimate software while remaining unnoticed by administrators. Taking advantage of flaws in corporate network security, the intruders are able to gain full control over the bank's infrastructure within a short period.

The key is to remember that if an attack is detected and stopped in time, intruders can be thwarted. Preventing losses is possible at any stage as long as appropriate protective measures are taken. Email attachments should be checked in an isolated environment (sandbox), instead of relying solely on endpoint antivirus solutions. It is critical to configure notifications from protection systems and react to notifications immediately. This is why security events must be monitored by an internal or external security operations center (SOC) with use of security information and event management (SIEM) solutions, which significantly facilitate and improve processing of information security events. Cybercrime is continuing to evolve and advance quickly, making it crucial that instead of hiding incidents, banks pool their knowledge by sharing information on industry attacks, learning more about relevant indicators of compromise, and helping to spread awareness throughout the industry.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com