ALSID ACADEMY

Episode 7

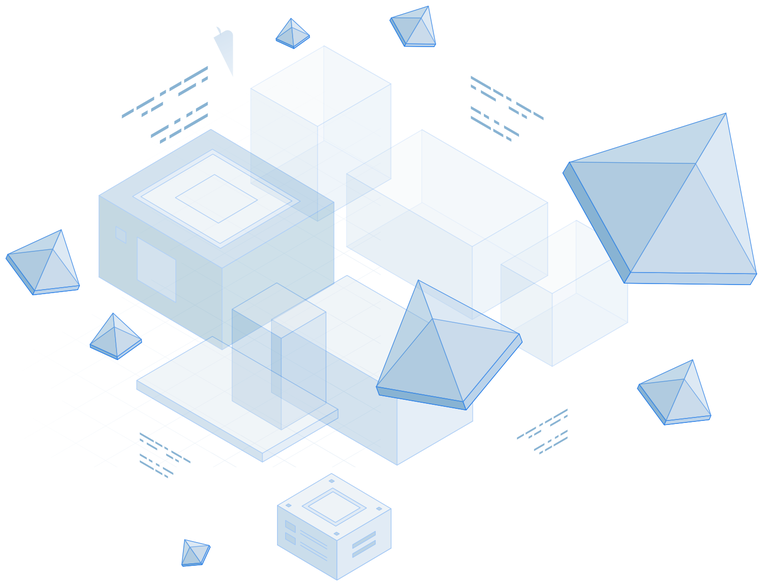
HACKERS VS. FINANCE: STRATEGIES CISOS CAN TAKE TO THE BANK

In recent years, financial and banking institutions worldwide have been the preferred targets of many cybercrime groups. Targeted attacks allow them to divert increasing sums of money, which impacts the production stability and reputation of the organizations targeted.

Both IT managers and security managers at these institutions must invest the time to study and understand the specific cyberthreats that affect them and then implement the countermeasures necessary to safeguard their banking or financial activity.

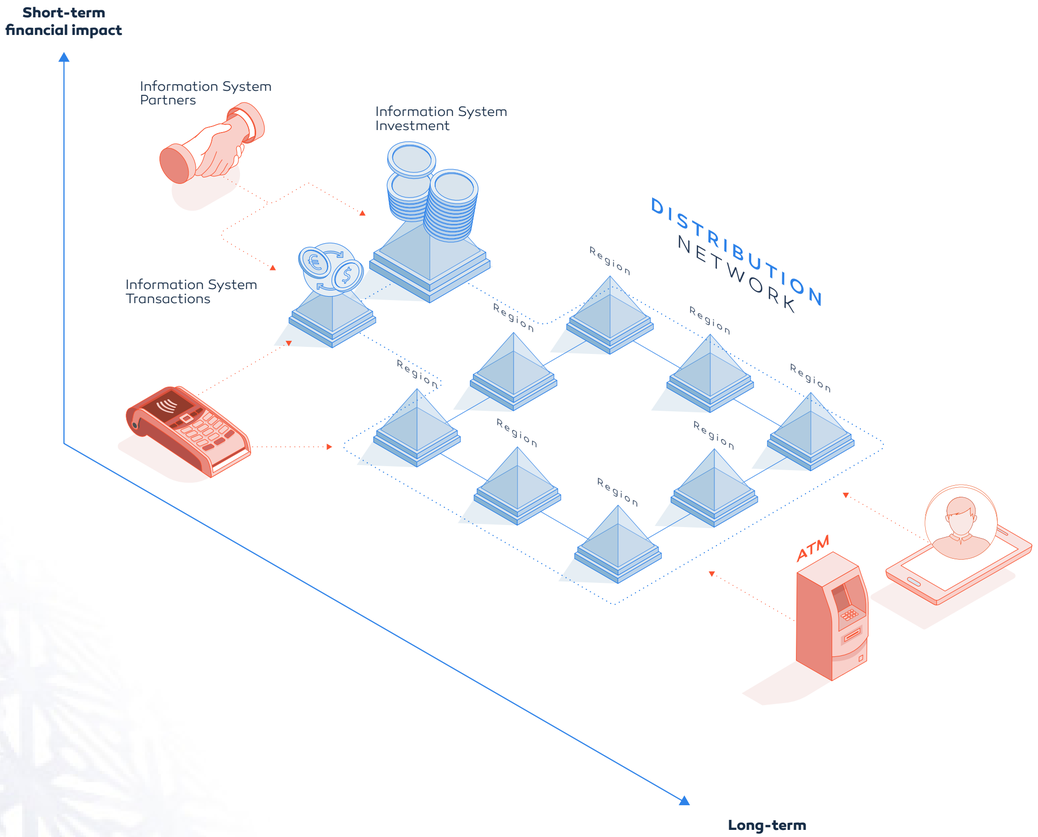
THE PARTICULARITY OF BANKING AND FINANCIAL INFORMATION SYSTEMS

- **Banking and financial information systems have particularities that tend to make their protection more complex than traditional IT environments.**



- Multiplicity of information systems: Banking Information Systems (IS) are essentially split into several related sub-IS, making end-to-end consistency extremely complex. This complexity and fragmentation, whether desired or merely tolerated, causes irreparable structural weaknesses.
- Opening the IS to the outside: Banking or insurance systems must be open to the outside, both to customers wishing to access their management interface and to trusted third parties and intermediation partners, to ensure financial or fiduciary transfers. The IS are interconnected with various external entities, which can be called «partners» in the broad sense of the term.
- This is a particularly attractive target for attackers: It is obvious that attackers will target the most vulnerable IS (reducing the complexity and the incubation period of the attack), as well as the IS with the best promise of profitability. Thus, a banking or financial system represents an especially attractive target.

We can simplify the representation of banking or financial systems with the following diagram:



The three main IS that make up financial institutions generally have the following characteristics:

- **Distribution Network IS:** Whether in the banking or the insurance world, this Information System is, by nature, connected to users and to the various ATMs. Furthermore, this IS very often comprises several regional IS, which historically have consisted of autonomous IS. Because of its visibility, should this IS be compromised in any way, the reputation of the institution can be jeopardized.

  Electronic banking & exchange IS: This IS manages the interaction with trusted third parties. Historically this IS has been centralized by the group and is subject to PCI-DSS controls. Usually of modest size, its proper operation nevertheless allows the smooth flow of payments and some financial exchanges with partners.

  Investment IS: In the banking world, the Investment IS bears weight in terms of risks. Indeed, even though user access is more restricted compared to the distribution network, this IS generally produces a large part of the organization's profits. It is usually centralized at the group level and follows specific rules of management and separation of powers.

Faced with this IS, or rather these multifaceted IS, the financial organization has a complex challenge to manage in terms of operational and strategic security. The IS security managers' duties are characterized by intense technical vigilance, a good understanding of the tactics used by attackers, and the ongoing development of adequate countermeasures to protect the systems. It is therefore essential to know the types of attacks that are executed on financial institutions.

WHAT TYPES OF ATTACKS TARGET FINANCIAL IS?

Obviously, most of the known «classic» attacks can be made against financial institutions' IS, but as we saw earlier, financial IS have their own characteristics that entail different risks and issues than the IS of industrials or large distributors, for example. Depending on the sub-IS targeted, the attacks may vary in the banking or insurance world. Still, it is possible to list the most common attacks:

- **Distributed Denial of Service (DDoS):** This is the most common type of attack, primarily impacting the IS of the distribution network, and has immediate impact, usually aimed at compromising the institution's reputation. It should be noted that some DDoS attacks have historically targeted the electronic payment system to block certain exchanges.
- **Malicious code on points of sale and withdrawal systems:** These attacks can take several forms, including specific malware to intercept data, data injections, copying payment methods, etc.
- **Malware on the information system:** Here, there is usually nothing specific to the banking or insurance environment, although recent attacks highlight the creation of malware specific to the financial environment to maximize the impact and efficiency of the attack. The intention here is to directly infect the sub-IS in question to access its data.
- **Insider threat:** Employees can carry out fraudulent transactions directly, whether voluntarily or involuntarily. In the case of a voluntary action, elevation of privileges and lateral movement on Windows systems are the strategies generally used.
- **Phishing:** This attack can come from two angles, with very different objectives: **(1)** Phishing aimed at users (extremely widespread) is an attack that directly targets users of financial services, flooding them with email, more or less accurately formatted, to harvest their digital financial identity and thus perform transactions in their name at a later date. **(2)** Phishing aimed at the financial institution's sub-IS, with the main objective of establishing a backdoor or installing malware to take control of a part of the sub-IS and exploit the business data within the institution.
- **Exploitation of vulnerabilities:** These attacks directly use the configuration weaknesses of the sub-IS, or the fact that it is not updated regularly. These attacks mainly target Windows and Active Directory vulnerabilities, again with the aim of maximizing the chances of success as well as the return on investment of the attack.

Each of these different methods of attack have been executed over the last three years, irrespective of country, irrespective of company size.

SOME RECENT EXAMPLES

The financial world is inherently discreet regarding the precise mechanics of observed or identified attacks. There are, however, known examples of attacks that have significantly impacted certain organizations:

- In 2018, the malicious codes FASTCash and ATMJackPot allowed attackers to steal cash directly from ATM-type withdrawal systems.
- In 2018, Carbanak and Cobalt malware targeted more than one hundred financial institutions in more than forty countries, resulting in the theft of over a billion euros. This malware had extensive coverage; it was installed on the IS and sub-IS of organizations and made it possible to manipulate bank accounts, establish fraudulent transfers, and take control of certain withdrawal points (ATMs).
- In 2019, the US bank Capital One was the subject of a personal data breach revealing information on more than one hundred million customers (names, income, phone numbers, emails, etc.).
- In 2019, the financial corporation Mouvement Desjardins revealed that an internal attack by an employee resulted in the theft of information concerning almost three million individual or corporate members.
- In 2019, Dutch Bangla Bank Limited was the victim of an external attack through the withdrawal systems in Russia and the Ukraine, resulting in the theft of more than three million dollars and delivering a devastating blow to its reputation.

And the list goes on...

WHAT COUNTERMEASURES SHOULD BE IMPLEMENTED?

Considering the distributed model of financial IS, it is highly complex to deploy a comprehensive security policy across the organization. We can nevertheless suggest the immediate implementation of the following actions:

- Study the attack models in your sector and invest in Red Team-type exercises that will simulate targeted attacks in line with the specificities of the banking or insurance sector. Train your teams, update their skills, and perform regular intrusion and theft of data tests.
- Integrate the MITRE ATT&CK model into your study schema. This model is currently the most complete and most adapted to modern attacks; it will allow you to better understand the complexity of attacks and to build your own adapted schema of countermeasures.
- Deal with the most common vulnerabilities: patch your systems, audit changes on sensitive systems, and monitor the actions of administrator accounts.
- Manage the Active Directory: Most Active Directory designs were built about 10 years ago, at a time when targeted malware attacks and modern phishing methods did not exist. The Active Directory case needs to be managed through a specific action plan.

THE SPECIFIC CASE OF ACTIVE DIRECTORY

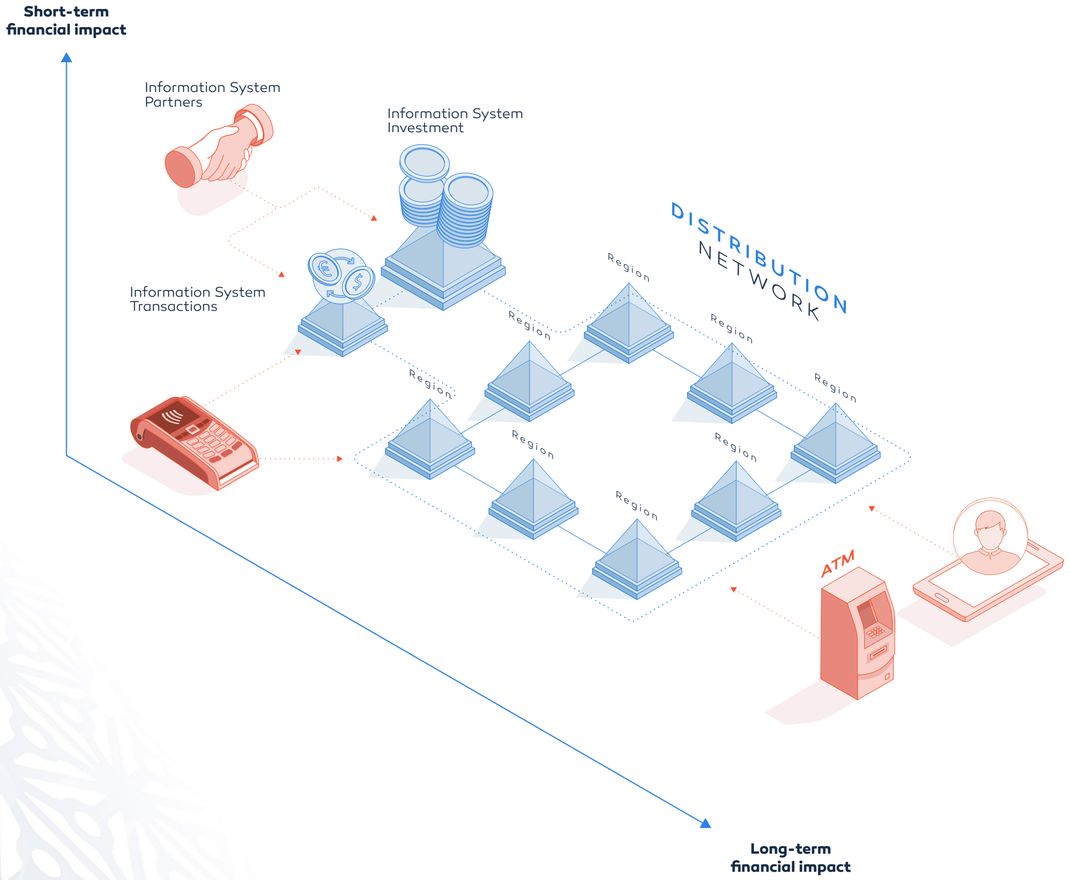
Why is Active Directory a latent threat to most organizations?

The Active Directory environment offers a favorable playing field for attackers or malware, for several reasons:

- Incomplete communication from Microsoft about Active Directory security, including late release of documents describing Tier-model design.
- Most Active Directory designs currently in production are more than a decade old, and regular update of domain controllers does not correct initial design.
- Since 2015, the explosion of malware specific to Active Directory during targeted attacks is combined with the increasing efficiency of hacking groups.
- Active Directory coverage is exceptional for an attacker because this directory is used in more than 95% of organizations with more than 50 PCs.

To complement your IS evaluation, we recommend you read the compelling article, **“Why Hackers Abuse Active Directory,”** on the BankInfoSecurity.com website. This article explains in detail why attackers target Active Directory to achieve their goals, especially against financial institutions. You can find this article here:

https://bit.ly/2LS34gT



Active Directory: A favorite target in the banking world

- We can visualize the use of Active Directory in the different financial sub-IS with the following schema:

There are therefore usually many Active Directory forests in different sub-IS, and in most cases these have trust relationships which provide the SSO mechanism to certain users.

Often, the distribution network has many forests, historically inherited from old regional organizations. These Active Directory forests sometimes have extremely heterogeneous levels of maturity and security. These are usually the largest and most complex Active Directory databases because many people work on these distributed entities.

Generally, the Investment IS encompasses one or more forests, usually on a global scale, to manage, in particular, different marketplaces or investment locations. It is not uncommon to find one forest per continent: America, Europe, and Asia, with inbound and outbound approvals for each forest.

Finally, the Electronic Banking IS usually has its own forest, to be able to specifically manage the mandatory features of the PCI-DSS compliance rules, a highly structured axis in payment systems. The electronic banking forest is very often cut off from the rest of the IS, avoiding approval relationships with other Active Directory environments in the organization.

All these characteristics specific to financial and banking institutions, namely multiplicity of sub-IS, distributed Active Directory model, multiplicity of forests, numerous approval relationships, and sometimes old Active Directory designs, represent fertile ground for attackers wishing to take control of your information system.

Securing Active Directory is of the utmost urgency for organizations in the banking or insurance sector

The diversity of activities and the distributed model of financial institutions make them extremely appealing to attackers; adequate countermeasures should therefore be put in place so that they are properly protected.

Financial institutions must consider three dimensions in their Active Directory protection:

- Check the upstream configuration: Check the correct configuration of the Active Directory service on an ongoing basis; with several thousand changes per day in the directory, it is an indispensable background task.
- Implement an attack detection plan. The Active Directory is susceptible to specific and sophisticated attacks; it should be able to detect these targeted attacks using solutions dedicated to the Active Directory environment.
- Have knowledge of all the changes made in the directory in case a remediation plan needs to be executed. In case of proven attack, the institution must be able to ascertain all the changes made during the attack period in order to execute a remediation plan and trace the attack back to the source (patient zero).

WHAT IS THE NEXT STEP?

As we have mentioned throughout this document, the specificities of financial institutions' information systems make them particularly sensitive to attacks using Active Directory. Protection against these attacks will be a major pillar of bank and insurance security in the coming months.

This paradigm should be considered and an action plan should be implemented to avoid data leakage or, worse, a loss of confidence in the institution itself.

To take your research a step further and improve your ongoing security plan, the Alsid website, www.alsid.com, provides many insights and guides for additional inspiration.