WHITEPAPER:

THE ONLINE BANKING KILL CHAIN

DataExpert

Better banks, better attacks

In the past 10 years, the use of online banking increased by fifty-six percent[1]. This fast adoption of digital and multi-channel client services in e-commerce triggered a growth in online banking fraud.

With all the improvements in infrastructure for online banking, attackers have not stayed behind. Since attackers have become more sophisticated and prolific, banks have come to the realisation that in order to keep up with these attacks, they need a more comprehensive approach in their defence and mitigation. This results in a need for a fraud strategy fully integrated into the bank's ecosystem, that not only makes the most of mitigating measures but is also geared towards a customer-friendly experience. To set up this type of fraud strategy, a clear view of the types of frauds existing and impacting the bank is important. To guide the bank in the right direction we would like to introduce the online banking kill chain.

1. https://ec.europa.eu , code: ISOC_BDE15CBC

The online banking kill chain

A kill chain is a concept used to identify the structure of an attack one wants to execute. In recent years many new kill chains have come into existence in the field of cyber security.

Therefore, by identifying an opponent's kill chain it can be used to find tactics of "breaking" their kill chain as a method of defence or mitigation. By identifying the steps in the kill chain of a cyber-attack, security analysts can identify which parts of their system need hardening and detection monitoring. There are multiple examples of cyber kill chains available, like the cyber kill chain by "Lockheed Martin[2]" and the "unified kill chain[3]". Online banking fraud holds a different structure, rendering the available cyber kill chains ineffective to mitigate online banking fraud risk.

This online banking kill chain is created specifically for fraud attempts on the online channels of a bank. Online channels are things such as a mobile banking application, third party providers utilising the bank's API or the online web application. It represents the different stages of any online banking attack, whether it is a phishing attack or malware based. In this paper, we will focus on using the online banking kill chain to improve your fraud strategy.

For the online banking kill chain, we adapted some of the steps seen in a cyber kill chain to fit online banking fraud. Because online banking fraud is more flexible in methods of attack, some of the stages have been combined, as well as a shift in focus regarding the attackers' method of cashing out during an attack. This is a stage which is not always seen in the cyber kill chains available. For the online banking kill chain, we have defined the following stages: Reconnaissance, Weaponization, Credentials Acquisition, Account Compromise and finally, Exfiltration.

2. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
3. https://www.unifiedkillchain.com

The steps in the online banking kill chain

Reconnaissance

The Reconnaissance stage is about gathering information about the target banks and collecting information on how to reach victims. Regarding the banks, actors will map out the login portals and their requirements, as well as investigate technologies running on the website which can be vulnerable to exploits. Personal information of possible victims is gathered or bought on criminal forums. Popular places to buy such information are channels on telegram or darknet marketplaces.

Weaponization

The next stage focusses on the Weaponization of the intelligence gathered in the previous stage. The attacker now sets up their systems for the upcoming attack. This includes setting up a server for the incoming stolen data (a Command & Control server, or “C&C”) and buying or building necessary fraud tools such as phishing kits and lists with PII (Personally Identifiable Information) data.

Credential Acquisition

In the third stage the attacker will make “contact” with their victim. The goal of this stage is to gain an entry to a victim’s banking account, either directly or indirectly. To gain direct access to a victim’s back account, an attacker may send phishing e-mails or SMS containing malware attachments or URLs to a phishing site, in order to obtain login credentials.

The attacker can also seek to gain indirect access to the bank account, by convincing the victim that they are a trusted party. They may be as bold as to call a victim pretending to be from the service desk of their bank or a trusted family member in need of money.

Account Compromise

In the Account Compromise stage, the attacker prepares for the exfiltration of funds. Having gained access to the victim's account in the last stage, the attacker can now use this access to further learn about the victim's personal details and to make changes to account settings and activity, to make the attack more profitable and likely to succeed. Sometimes, the attacker takes their time and increases transaction limits, changes the address book or refunds previous legitimate payments to increase the available funds in the account, to maximise profits. In other cases, the attacker wants to make a move quickly, and only checks the account balance before moving to the final stage.

Exfiltration

The final stage of the kill chain is the Exfiltration. In this stage, the attacker will cash out on the account. It is important in this stage to make the distinction between victim-initiated fraud and attacker-initiated fraud. When the attacker chooses for a quick action plan, it is likely that the attacker themself logs into the victim's account and makes a transaction (this can be to a mule account, or it can be done by buying crypto or by a purchase in a web shop). In victim-initiated fraud, the attacker will attempt to convince the victim to make a transaction, using information gained in the account compromise stage.

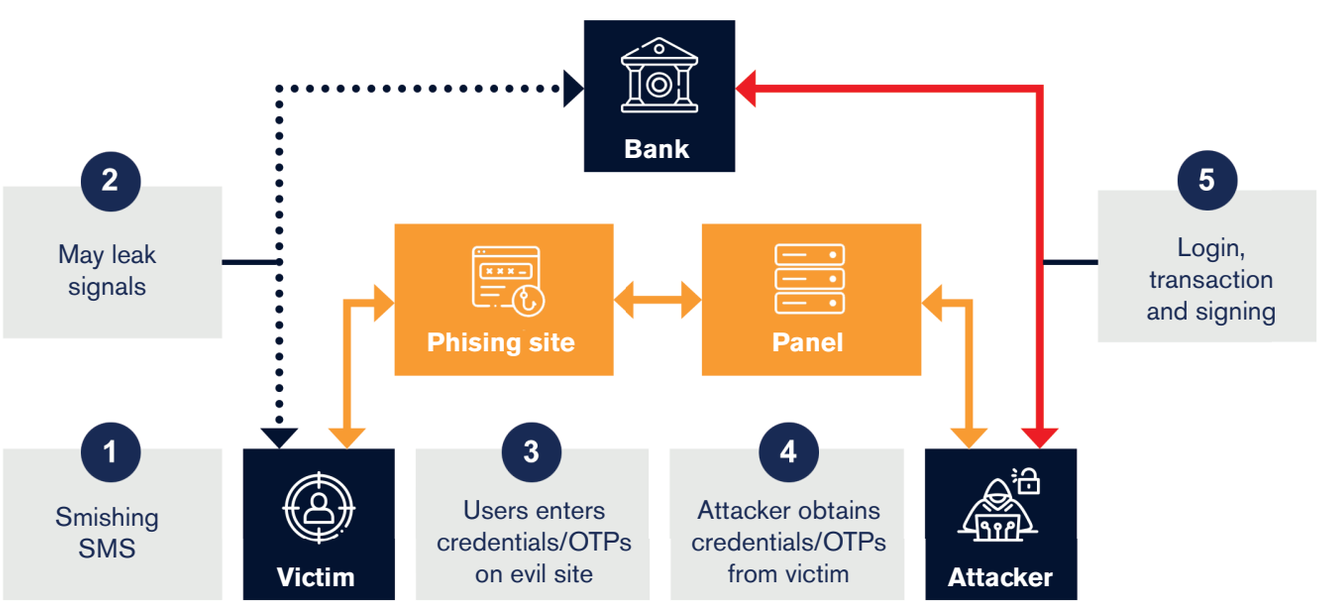
Smishing through the kill chain lens

To clarify the usage of the online banking kill chain for improving the fraud strategy we will use "smishing", a common method of attack, as an example. We will go through each stage, and identify a potential attacker's actions, and explain mitigatory countermeasures. Smishing can have many goals, below we will focus on a form of smishing where the end goal is to register a payment card to a digital wallet.

Smishing

A very popular method of fraud utilised by attackers is smishing. The word smishing is a portmanteau of SMS and phishing. As the name implies, the attackers use SMS instead of email to draw in victims. This SMS often contains a story along the lines of a security update of the mobile app, a notification of suspicious activity on the victim's account or a notification that a payment card needs to be renewed. Usually there is some form of urgency in the SMS by adding a deadline or the possibility of a fine when the victim does not comply. The SMS will contain a link to a phishing site, where the victim needs to perform actions that provide the attackers with credentials and an OTP (one-time password, often necessary for two-factor authentication, or "2FA"). While the victim is active on the phishing site, the actor will log in on the legitimate bank site, using the victim's credentials and login OTP. They will then require from the victim a second OTP to register a payment card to an online wallet. This enables the actor to make payments using the wallet without needing authentication from the victim. This can then be used for anything, from buying crypto coins to prepaid gift cards.

The SMS that is send to the victim is only a small part of the entire attack process as described in the kill chain. The beginning of this process can fly fully under the radar of the victims. However, there are mitigating measures a bank can take to identify smishing attacks early on. By using the online banking kill chain as a basis, a bank can start to identify actions to mitigate the risk of a smishing attack.



Reconnaissance

In Reconnaissance, gathering intelligence can inform a bank pre-emptively what type of attack may take place. For smishing, this stage in the kill chain could consist of gathering phone numbers from possible victims. These can come from leaked sources or are bought on black marketplaces. Preventive actions can range from awareness campaigns to targeted intelligence gathering on such phone number lists.

Weaponization

The next stage, Weaponization, is all about preparing for the attack by setting up servers and tooling. An example is building a phishing site visually equal to the bank site, which can be used when an attacker attempts to convince the victim to click on a phishing link in the SMS. Understanding this stage allows a bank to build detection in their systems for fake sites by, for example, monitoring domain registrations, observing referrers for specific images on the bank's site (phishing sites often use authentic images that still have unique characteristics that refer back to the place of origin), utilising notice and takedown procedures and online phishing reporting.

Credential Acquisition

Once the attacker has convinced the victim to click the phishing link, the phishing site will instruct the victim to log in. When the victim enters their credentials on the phishing site, a handler will be alerted and will, in turn, log in on the actual bank site and make a parallel session. This can be an initial signal in bank traffic of malicious intent. This session will likely show behaviour that does not match the victim's regular behaviour.

Account Compromise

Once the attacker has logged in on the victim's bank account using the stolen credentials, the attacker needs a secondary OTP to register an e-wallet. The victim is still logged in on their "bank account" on the fake website, and believing that they need to apply for a new payment card, they fill in the required information. The attacker in turn uses this information (such as the secondary OTP) to finalise their e-wallet card registration of the real bank account. It might be regular behaviour for the victim to log in on an IP they have not used before to check their balance. However, making an e-wallet registration may stand out, making it an opportunity for the bank to detect the fraud before a cash out has taken place.

Exfiltration

After the e-wallet registration has taken place, the attacker will start the exfiltration stage. Using an e-wallet allows making transactions without further needing the victim's own input. By identifying an e-wallet as an exfiltration method, it is possible to harden the systems on this level by, for example, giving the customer an extra alert through email that a card has been registered on a digital wallet.

The previous paragraphs show the steps of the online banking kill chain in detail.
The stages Reconnaissance, Weaponization, Credential Acquisition, Account Compromise and Exfiltration can be applied to different types of attacks targeting online banking. Using the stages in the online banking kill chain to identify the methods used by attackers, a bank is able to identify where in their fraud strategy they need additional monitoring, security measures and even more awareness with both customers and employees. In the current times where the use of online banking is thoroughly integrated in society, not only for legal use but also for illegal use, it is very important to keep up with new developments surrounding e-commerce and online banking.

A balanced fraud strategy that protects a bank's customer, as well as maintains a friendly environment regarding online banking, can be achieved by combining a good view on user friendly design as well as efficient mitigating actions. By focusing on the online banking kill chain, it is possible todetermine the necessary mitigation actions to stop a fraudulent transaction before it happens.

Sources

1. https://ec.europa.eu , code: ISOC_BDE15CBC
2. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
3. https://www.unifiedkillchain.com/

About DataExpert and DetACT: No more fraud

DataExpert's mission is to empower banks, law enforcement, military, intelligence agencies, customs, other government organizations, telecommunication companies, insurance companies, and other commercial enterprises to fight (cyber)crime and fraud and protect organizations against (cyber)criminals. To this aim, DataExpert delivers a wide portfolio of digital forensics, analytics, and cybersecurity solutions and services to its customers. DataExpert's managed service solution "DetACT" has over 15 years of experience protecting European retail banks from fraud.

Powered by its team of fraud analysts and investigators, DetACT serves as the "eyes and ears" of the bank in its channels, predicting and preventing fraud before it takes place. Our experts work closely with our clients and actively exchange knowledge and best practices with like-minded parties.

More information and questions:

DataExpert BV
Vendelier 65
3905 PD Veenendaal
The Netherlands
+31 (0)318 543173
info@dataexpert.nl
www.dataexpert.eu

DataExpert