



# Financial Industry Threat Landscape

GERMANY

*H1 2023*

# Outline

Executive Summary.....	3
Purpose and scope.....	5
State of the financial industry in Europe .....	6
Threats against the Financial Industry .....	7
Ransomware .....	8
Distributed Denial of Service (DDoS) .....	9
Supply chain attacks.....	10
Malware fraud .....	12
Business Email Compromise (BEC).....	13
Consumer Fraud.....	14
Threat Actor profiles .....	15
Nation-State .....	16
Cybercriminals .....	17
Hacktivists .....	18
Initial Access Brokers (IAB) .....	20
Emerging Threats to the Financial Industry .....	21
Steganography .....	22
Artificial Intelligence (AI).....	23
Deepfakes .....	24
Authorization and authentication bypass .....	25
Geopolitical and regulatory situation .....	26
Overview of international events .....	27
Regulatory changes.....	29
Mitigation strategies.....	31
References .....	32

# Executive Summary



## Threats

- ◆ The link between **ransomware** and the financial industry is called **big-game hunting**: cybercriminals are inclined to target the sector as it is a high-value vertical. Yet, the latter is known for robust and innovative security standards, so it is a high-stakes game.
- ◆ The goals of **Distributed Denial of Service** attacks are activity **inoperability** and **reputational damage**, often politically motivated. Groups have been focusing on those organizations where damage could reach peaks, which makes financial companies a relevant threat.
- ◆ A **supply chain** attack represents a **critical threat to businesses** as they rely on third parties with their own security. It is perpetrated by sophisticated threat actors that usually **exploit known or 0-day vulnerabilities** to grant access and control over the targeted network.
- ◆ **Malware distribution** has a wide spectrum against the financial sector and can focus on the user (**Android banking trojans**), the intermediate (**skimmers**), or the financial company itself (**ATM malware**).



## Threat Actors

- ◆ **Cybercriminals & Initial Access Brokers** (IABs) **seek an economic benefit** with their actions and pose a high risk to the financial sector. They can target **corporate assets** (selling access to the corporate network, extorting the company after a ransomware attack, or getting a fraudulent transaction done on their behalf) or directly the **company's clients** (stealing their banking credentials through phishing campaigns or malware distribution).
- ◆ Despite the noise generated by disruptive actions carried out by **hacktivist** groups, their **capabilities are limited**, and the attacks performed have not posed an elevated or rather unstoppable threat so far.
- ◆ **Nation-State** actors normally focus on targeting roles with access to **strategic information**, but those with a financial gain objective are becoming more frequent.



## Emerging Threats

- ◆ Some emerging threats are already being used to commit fraud against financial institutions: **steganography** to hide malicious payloads into images or **deep fakes** to enhance social engineering attacks.
- ◆ Newer **Artificial Intelligence** technologies and the lack of control that comes with these developments (as with ChatGPT), pose a risk to the financial industry.
- ◆ Efforts carried out by the financial sector to defend itself are fruitful and affectation numbers are lowering. However, efforts made by attackers for example, to bypass the robust **authentication and authorization methods** implemented also prove a non-ending fight against cybercrime.



## Geopolitics

- ◆ **Geopolitical events** have a greater effect on the financial industry than on other industries with events like the invasion of Ukraine having translated into attacks against public and private infrastructure being materialized within hours of relevant decisions being adopted.
- ◆ Behind the war curtain lies a more traditional approach: the continuous **fight for supremacy** pursued by figures like China, the United States, or again, Russia.
- ◆ At an international and, more specifically at a European level, countries are promoting **international collaboration** and the adoption of a single common position against all types of cyber threats.
- ◆ Each country is also trying to strengthen its cybersecurity with new regulations. **Germany's** efforts finally materialized in a **National Security Strategy** (NSS) that, unfortunately, is still fragile, most probably due to internal political negotiations.

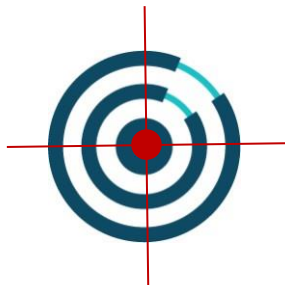
# Introduction

**Obtaining an economic benefit** is the most frequent answer that we get for the question “*What was the objective pursued in the commission of a cyberattack?*”, although it is true that we can also find objectives more linked to ideology. And if we consider that attackers fundamentally pursue financial gain, there is no better target to choose than the financial sector, and more specifically, one linked to prominent economies such as Europe.

The financial sector’s attractiveness translates into **sophisticated widespread threats** looking to compromise companies either through their technological or human infrastructure, or, at a lower level, through the customer base. Threat actors seek PII (personally identifiable information), financial account data, and anything else that can be monetized. Besides, threat actors could also be willing to just disrupt the day-to-day business or gather intelligence and information that favors a privileged position.

Along with the responsibility that comes from managing the financial system, comes a **greater development of protection measures** against threats and **stricter regulation**. That is why the financial sector has always been, and continues to this day, a benchmark in terms of cybersecurity.

## Purpose and scope



**In this whitepaper, Outpost24’s analysts will focus on the issues that confront companies in the financial industry, offering insight and guidance to meet the challenges they face today.**

Coverage was intended for a **strategic level**, so threats, actors, trends, and geopolitical aspects included have been summarized to provide just an overview on the matter. Moreover, and with the intention of not just staying at a theoretical plan on each issue, **real examples** of threats or threat actors that have recently affected the sector and region of interest have been included.

The reason behind the urgency to know the specific threats targeting our industry is that only then we are able to choose and implement the necessary security measures. And that is precisely what Outpost24’s **threat intelligence** analysts try to cover in this report: fundamental information on what is really happening out there against the financial services industry, **helping decision makers making informed business decisions**.

Moreover, as it was already mentioned, the financial industry establishes cybersecurity benchmarks, and, unfortunately, that also implies the biggest innovations in terms of the sophistication of threats or **new attack trends**. Luckily, it also translates into new **regulatory decisions**. Bearing this in mind, this report also tries to collect some of these trends and regulations that are already affecting the financial sector, as can be confirmed with some of the examples of real cases that have occurred, but whose impact will undoubtedly be greater in the coming months.

# State of the financial industry in Europe

ANALYSIS



A  
C  
T  
O  
R  
S

T  
O  
O  
L  
S

## DATA

## INFORMATION

## INTELLIGENCE

Specialized media & cybersecurity firm blogs

Social media & communities

Sandboxes

Dark web engines

Underground forums

Data Leak Sites

...

✓ **416 actors** included in Threat Context (TCx) target the European region, and **228 actors** of them target the **financial industry**.

✓ **112** of them have been updated in the last **12 months**.

✓ **165** have high levels (strategic, innovator, expert, or advanced) of **sophistication**.

✓ **82** tools included in TCx are categorized as **banking trojans**.

✓ **3** are defined as **skimmers**.

✓ **16** tools are described as **Point-of-Sale (POS) malware**.

The **European financial sector** is one of the most targeted ones, with **24.4%** of the threat actors Outpost24's analysts follow having it as a preferred target.

Almost half of these threat actors have been active recently and therefore, **still pose a real risk** to the industry.

Moreover, the risk is also high due to the level of sophistication of these groups, meaning they have great **chances of being successful** in their attacks.

Outpost24's analysts have observed **over 100 malicious tools** designed to target the financial sector and banking users.

**Banking trojans** are the most prevalent, representing around **80%** of the total.

**Prevention efforts** from the financial sector cannot end at a corporate level but should fight **all types of attacks**, bearing in mind for example, that its clients seem like a frequent target.

€1.53 billion worth of fraudulent card transactions were registered in 2021 in the European Union<sup>1</sup>.

DDoS attacks against the European financial sector increased by 73% in 2022. The sector represented 50% of all DDoS attacks in the region last year<sup>4</sup>.

The finance sector is the 5th most targeted sector in the EU from 2021 to 2022. It represented 8,64% of all cyber incidents in that period<sup>2</sup>.

The global annual cost of cybercrime was estimated to be €5.5 trillion in 2021<sup>5</sup>.

74 % of the European operators of essential services do not have cyber insurance<sup>6</sup>.

The finance sector is the most prone sector to internal server errors leading to data breaches<sup>3</sup>.

Every 11 seconds there is a ransomware attack<sup>7</sup>.

## KEY POINTS

*(Out of data recovered from TCx)*

**Ransomware:** out of the usual 47 threat groups that use ransomware to target the financial services sector in Europe, **15 conducted at least one attack in 2023.**

**Distributed Denial of Service:** there are **26 groups** targeting the European financial services sector conducting DDoS attacks in 2023.

**Supply chain attacks:** as a sophisticated category, fewer groups conduct supply chain attacks against the European financial sector - there are **10 threat groups** that fit the category.

In 2023, the “Clop ransomware group” **exploited a vulnerability** in Fortra’s GoAnywhere MFT, **impacting over 130 organizations**, including German insurer **Munich Re.**

**Malware fraud:** **30 threat actors** involved in malware fraud activities targeting the European financial sector – encompassing ATM/POS malware and banking trojans.

**Business Email Compromise:** particularities of the **financial services** sector - high levels of confidentiality and flux of assets - make it **more susceptible to being targeted.**

**Consumer Fraud:** there are **82 threat groups** that are involved in watering hole and phishing/vishing/smishing attacks against the European financial sector.








# Threats against the Financial Industry

# Ransomware

A ransomware attack is one in which the victim's files get encrypted – meaning that access is blocked and can only be regained if the victim pays the ransom demanded by the cybercriminals. The evolution of ransomware led to the adoption of **double, triple, and quadruple-extortion techniques**. Respectively, besides encrypting data: cybercriminals also exfiltrate sensitive files from the victim and threaten to publish them; on addition to that, in the triple phase, cybercriminals contact the victim's clients and employees; and on top of everything, the quadruple technique involves the threat of DDoS. These methods compromise the basis of information security: while encryption and DDoS risk the availability pillar, stealing sensitive information threatens the confidentiality aspect of information security.

The **financial services** sector is not isolated from the ransomware threat: based on Outpost24 KrakenLabs' research, in 2023, 1% of the victims made public by ransomware groups in Data Leak Sites (DLS) belonged to the European financial services sector<sup>ii</sup>. Based on our monitoring in Threat Context (TCx), out of the usual 47 threat groups that use ransomware to target the sector in Europe, at least 15 of these have conducted at least one attack in 2023. These figures might be observed through the lens of big-game hunting: ransomware operators are inclined to target the financial sector as it is a high-value vertical. Yet, the sector is known for its robust and often innovative security standards, so it is a high-stakes game for cybercriminals. A threat actor that attacks the finance industry is likely sophisticated, so the threat posed by them, although not frequent, is alarming.

Relevant techniques for threat actors in Outpost24's TCx using ransomware as attack method and focusing on financial services and Europe as targets<sup>i</sup> are:

Technique	Vulnerabilities and risks
 Spearphishing Attachment [T1566.001] and Link [T1566.002]	Compromise employee credentials or corporate resources. Distribution of first-stage malware or remote software tools.
 Exploit public-facing apps [T1190]	Gain access to the network. Distribution of first-stage malware or remote software tools.
 Valid accounts [T1078]	Escalation of privileges in the network. Distribution of first-stage malware or remote software tools.
 Automated Exfiltration [T1020]	Publication of compromised data. Sensitive information exposure.
 Data Encrypted for Impact [T1486]	Activity interruption. Potential data loss.

Affection to Confidentiality  Integrity  Availability 

Based on the data observed by Outpost24 KrakenLabs analysts<sup>8</sup>, a significantly higher level of activity from the **"LockBit Group"** in comparison with other groups is more than evident. They are a Ransomware-as-a-Service (RaaS) group and affiliates to the double extortion technique, meaning they maintain a DLS where they publish information from victims that have decided not to establish negotiations with them. Among the companies listed as victims, on February 10, 2022, was German service provider **HEUBECK AG**<sup>9</sup>, a company focused on solving actuarial and financial issues relating to old-age provision. The impact of the incident has not been publicly disclosed and no public statements have been found, so it is not possible to confirm the reach of the incident. Moreover, the DLS where they were listed has been filled with newer victims, so HEUBECK AG's information is no longer available.

<sup>i</sup> See the complete Attack Patterns Matrix in TCx using the following query: *attack\_patterns:~"data encrypted for impact" AND targets:"Europe" AND targets:"financial-services"*

<sup>ii</sup> Up to early May 2023, Outpost24 tracked 1,125 victims shared in DLS, of which 35 belonged to the financial services sector (representing 3,1% of the total victims). Of these 35 financial sector victims, 10 were European (representing 28,6% of the attacks against the financial sector).



# Distributed Denial of Service (DDoS)

DDoS attacks are a subclass of Denial of Service (DoS) attacks in which multiple connected online devices (botnet) are used to overwhelm a target website with traffic, slowing or even disabling it altogether for legitimate users<sup>10</sup>. Normally, these types of attacks can be solved in a short period of time, so consequences could be placed more on a reputational aspect. Moreover, because these botnets have turned more profitable for renting than for mining to their owners, the as-a-service business model has also impacted the DDoS panorama, flooding the underground markets with services aimed at simplifying the carrying out of these types of attacks.

Bearing these ideas in mind, it is not out of place that **hactivist groups** are currently the ones who primarily choose this type of threat over their victims, as they plan to cause some reputational damage to their victims, and they do that with limited resources. Hactivism ties itself to a political agenda, and Europe's political agenda has been quite agitated with the Ukrainian-Russian conflict since 2022.

However, hactivists are not the only groups that employ DDoS attacks: in TCx, there are 12 adversaries classified as hactivists targeting the **European financial sector** – however, there are 26 groups with this same target that conduct DDoS attacks. Moreover, since the final goal to be achieved is certain reputational damage, groups have been focusing on those institutions and organizations where that damage could reach peaks, ending up with financial companies as the losers in this unequal match.

Relevant techniques observed for threat actors included in Outpost24's TCx using DDoS as an attack method and focusing on financial services and Europe as targets<sup>iii</sup> are:

	Technique	Vulnerabilities and risks
●	Botnet [T1584.005]	Block the availability of websites or online resources
● ●	Exploit public-facing apps [T1190]	Gain access to the network.
●	Network denial of service [T1498]	Block the availability of websites or online resources.
● ●	Defacement [T1491]	Block the availability of websites or online resources. Access to internal information. Potential disinformation.

Affectation to Confidentiality ● Integrity ● Availability ●

During end-January 2023, various hactivist groups with the **"Killnet Group"** as the most prominent among them, carried out multiple DDoS attacks against German institutions. The attacks were likely motivated in retaliation for Germany's supply of war material (Leopard tanks) to Ukraine. The collective campaign was initiated by the **Killnet Group** through Telegram, where they published a message on January 24, calling (Google translated by the original Russian) *"all hack groups supporting the mission of the Russian Federation in the fight against the Nazis"*. In their message, they launched the hashtag **#ГерманияRIP**, which translates to **#GermanyRIP**, and published a list of targeted web services, which included airports, financial services, and government services. The **Killnet Group** itself claimed to have carried out several attacks against major financial institutions, including **Deutsche Bank and Giropay**, sharing some images on their channel. Despite these accusations, it is relevant to say that the affectation was not confirmed by either of the companies.

<sup>iii</sup> See the complete Attack Patterns Matrix in TCx using the following query: *(description:~"ddos") AND targets:"Europe" AND targets:"financial-services"*

# Supply chain attacks

A supply chain attack is one that targets weaker and/or foundational links of an interconnected chain of networks to acquire access and subsequent control to other higher-value ends in the chain. Usually, this type of attack targets widely used software aiming to hit multiple clients of such vendors. A supply chain attack represents a **critical threat to businesses** as they rely on third parties with their own security, which proves to be a delicate situation. Due to the intricate nature of supply chain attacks, they tend to be perpetrated by sophisticated threat actors that usually exploit known or 0-day vulnerabilities to grant access and control over the targeted network.

The level of sophistication is illustrated by the relatively low number of actors involved in supply chain attacks against the **European financial sector**: in TCx, Outpost24 currently tracks 10 threat groups that fit the category. The nature of said threat actors might vary between cybercriminals with financial motivations to nation-states seeking organizational gain and/or espionage reasons. The financial services sector, progressively relying on third-party vendors to manage its IT structure, and being a high-value sector, must be especially alert for supply chain attacks that might compromise corporate security, financial resources, business and client's sensitive information, and others. A supply chain attack disrupts activities, causes financial damage (either because of heists or to the costs of interrupting and resuming operations), generates mistrust in the financial institution, and damages the image of the targeted institution.

The European Union Agency of Cybersecurity (ENISA) proposed<sup>11</sup> a **taxonomy** to characterize supply chain attacks with two separate sections, one focused on the attack techniques used to compromise the supply chain, and a different one with attack techniques used to compromise the customer:

## Techniques used to compromise the supply chain

### Vulnerabilities and risks

● Social engineering	Compromise employee information. Distribution of first-stage malware or remote software tools. Gain access to the network. Facilitate further steps in the compromise.
● Malware infection	Compromise employee credentials or corporate resources. Lateral propagation through the network.
● Brute-force [T1110]	Gain access to the network. Lateral propagation through the network.
● Exploit software vulnerability	Gain access to the network. Gain access to third-party clients. Distribution of first-stage malware or remote software tools.
● Exploiting configuration vulnerability	Sensitive information exposure. Gain access to third-party clients.
● Open-source intelligence	Gain access to the network. Facilitate further steps in the compromise.

## Techniques used to compromise the customer

### Vulnerabilities and risks

● Trusted Relationship [T1199]	Distribution of first-stage malware or remote software tools.
● Drive-by Compromise [T1189]	Distribution of first-stage malware or remote software tools.
● Phishing [T1566]	Compromise employee information. Distribution of first-stage malware or remote software tools.
● Malware infection	Compromise employee credentials or corporate resources. Lateral propagation through the network.
● Physical attack or modification	Sensitive information exposure. Gain access to third-party clients. Activity interruption.
● Counterfeiting	Gain access to third-party clients.

Affection to Confidentiality ● Integrity ● Availability ●

---

On February 2023, the “**Clop ransomware group**” (also known as “*FIN11*”) exploited a zero-day vulnerability (later identified as CVE-2023-0669) in Fortra’s GoAnywhere MFT secure file transfer tool. The vulnerability allowed a remote attacker to perform remote code execution (RCE) on GoAnywhere MFT instances and could only be exploited after gaining access to the administrative console of the application, typically only accessible from the private company network, through VPN, or whitelisted IP addresses<sup>12 13</sup>.

Clop operators managed to exploit the vulnerability in instances from over 130 organizations<sup>14</sup> and decided not to deploy ransomware for encrypting purposes but only to only exfiltrate data stored on the servers. After a few days, the threat actors began coercing the victims into paying them for not exposing the exfiltrated information on their Data Leak Site. One of the companies listed as a victim on their DLS was Germany’s leading global provider of reinsurance, primary insurance, and insurance-related risk solutions, **Munich Re**.

The company published a statement<sup>15</sup> confirming that they had indeed identified an information security incident at an external service provider. On this occasion though, Munich Re’s impact was limited since they did not have a contractual relationship with the company affected, with which they had only shared test files with meaningless content. However, this luck was not on other victims’ roofs whose sensitive information ended up leaked on the group’s website.

---

# Malware fraud

The higher the levels of data confidentiality and potential for financial loss, the greater the interest of threat actors, and malware distribution has always been one of the easier and more effective ways to achieve compromise. Moreover, because financial companies are mainly service providers, malware distribution has a wider spectrum against this sector and can focus on the **user** (banking trojan, with special emphasis on Android banking trojans), on the **intermediate** (skimmers), or on the **financial company** itself (ATM malware).

When talking about **banking trojans**, phishing or smishing remain the most widespread forms of distribution along with other entry vectors such as malvertising or exploit kits embedded in web pages. On the other hand, **skimmers** or **ATM malware** require a rather vulnerable aspect from the victim, either through the exploitation of vulnerable software or through the physical exploitation of the hardware.

However, despite the attractiveness of the sector, the effort made to reduce malware impact (both through public education and through implementing additional security measures and strong regulatory standards) has made some progress. Even if banking trojans are still a reality, fraud-related numbers associated with this threat are decreasing<sup>16</sup>, as are also fraud numbers related to ATMs and POS terminals. In general, based on the European Central Bank's findings<sup>17</sup>, the overall value of fraudulent card payment schemes, both card-not-present and card-present, operating in the euro area has decreased in recent years. Still, in TCx, one can find 30 threat actors involved in malware fraud targeting the European financial sector.

Relevant techniques observed for threat actors included in Outpost24's TCx using skimmers, banking trojans, or ATM malware as attack methods and focusing on financial services and Europe as targets are:

Technique	Vulnerabilities and risks
● Spearphishing Attachment [T1566.001]	Get access to the victim's device. Compromise the device with malware.
● User execution [T1204]	Get access to the victim's device.
● Masquerading [T1036]	Get access to the victim's device.
● Input capture [T1056]	Compromise credentials and card data.
● Screen capture [T1113]	Compromise credentials and other sensitive data.

Affection to Confidentiality ● Integrity ● Availability ●

In early 2023, the German Federal Financial Supervisory Authority (BaFin) issued a warning about the rise of **Godfather banking trojan** infections targeting German banking users<sup>18</sup>. The malware masquerades as legitimate financial applications, targeting over 400 applications across 215 international banks, 94 cryptocurrency wallets, and 110 cryptocurrency exchange platforms since early 2022<sup>19</sup>. Other notable European targets include Spain – with 30 Spanish financial institutions being targeted by the banking trojan<sup>20</sup> -, France, Poland, Italy, and the United Kingdom. Godfather is adapted to the latest security measures implemented by financial institutions, as it can bypass two-factor authentication by exfiltrating push notifications and SMS texts, besides forwarding calls. This type of attack exemplifies how financial institutions must closely follow the cyber threat landscape to be able to block the advance of cyber criminals that generate financial loss and distrust.

# Business Email Compromise (BEC)

*Fraud targeting corporate directly.*

Business Email Compromise (BEC) is a type of social engineering attack where a scammer, which is often a trusted figure, tricks their victim into carrying out an action. Said action usually involves an economic transaction divulging confidential info or, to a lesser extent, downloading and executing malicious software. BEC scams could have many different faces<sup>21</sup>. A victim could be facing an email from the **HR or finance department** asking to fill out some personal information, which would be later used in other attacks. It can impersonate **the company's CEO** asking for a financial transaction to be made as soon as possible (this specific case is known as **CEO Fraud**). It could pretend to be a **legitimate vendor or supplier** that the company works with asking for some payments or specific data (sometimes covered as **Vendor Email Compromise (VEC)**). All these variants pursue the same goals: an economic transaction that has the attackers as beneficiaries or divulging some confidential information either personal or from the company.

This type of fraud would traditionally take place through phishing emails sent from compromised, legitimate, or spoofed business email accounts. However, attackers adapted to real-world changes, like the working from home increase, and have incorporated using virtual meeting platforms to conduct BEC-related scams<sup>22</sup>.

**Financial institutions** are as susceptible as those of other sectors to this type of attack. However, certain particularities such as the fact that financial employees are more used to dealing with invoices and requests for wire transfers or that the information that is usually dealt with implies high levels of confidentiality, make them even more susceptible to ending up victims<sup>23</sup>.

When it comes to BEC attacks, the most relevant techniques focus on those associated with the first stages of a cyberattack and basically affect the confidentiality of the information:

Technique	Vulnerabilities and risks
<ul style="list-style-type: none"> <li>Gather Victim Identity Information: Email Addresses [T1589.002] and Employee Names [T1589.003]</li> </ul>	<ul style="list-style-type: none"> <li>User impersonation.</li> <li>Greater probability of success in later stages as they will be endowed with greater legitimacy.</li> </ul>
<ul style="list-style-type: none"> <li>Gather Victim Org Information: Business Relationships [T1591.002], Identify Roles [T1591.004], and Identify Business Tempo [T1591.003]</li> </ul>	<ul style="list-style-type: none"> <li>User impersonation.</li> <li>Greater probability of success in later stages as they will be endowed with greater legitimacy.</li> </ul>
<ul style="list-style-type: none"> <li>Compromise Accounts: Email Accounts [T1586.002]</li> </ul>	<ul style="list-style-type: none"> <li>User impersonation.</li> <li>Greater probability of success in later stages as they will be endowed with greater legitimacy.</li> </ul>
<ul style="list-style-type: none"> <li>Establish Accounts: Email Accounts [T1585.002]</li> </ul>	<ul style="list-style-type: none"> <li>User impersonation.</li> </ul>
<ul style="list-style-type: none"> <li>Phishing [T1566]</li> </ul>	<ul style="list-style-type: none"> <li>User impersonation.</li> </ul>

Affectation to Confidentiality ● Integrity ● Availability ●

Active since early 2022, **"Water Dybbuk"** is a threat group that specializes in **BEC fraud**. The adversary mainly targets the finance department of extremely high-revenue companies, and in a campaign that lasted from April 2022 until late that year, it targeted companies in the Americas and Europe<sup>24</sup>. Out of 110 victims, three were from Germany. The campaign starts with a tailored spearphishing email containing an HTML file with malicious JavaScript that redirects the victims to a Microsoft phishing page that is set up to steal credentials and session cookies from Microsoft Office 365 accounts. Then, upon acquiring access to the key target's email credentials, **Water Dybbuk** proceeds with the BEC fraud. As this threat actor is opportunistic in nature and interested only in profits, it is not surprising that it would also target financial services organizations.



# Consumer Fraud

*Fraud targeting the corporate client.*

Consumer fraud is any type of scheme or technique that aims to deceive users and obtain financial advantages over them. Cyber-enabled consumer fraud includes social engineering techniques that trick victims into exposing their own credentials and/or financial information. One example is **watering hole attacks**, which consist of compromising legitimate websites by injecting a malicious code payload into the website to spread malware. Other examples of consumer fraud are **phishing** and its similar manifestations such as **smishing** and **vishing**: while phishing relies on emails and malicious links, smishing tries to obtain consumers' sensitive data through text messages or messaging applications, and vishing relies on phone calls.

All of these examples represent consumer fraud attacks that aim to trick the victim into handling their own personal information to the attackers. The acquired information can be used to facilitate further attacks (through the use of credentials), withdraw funds from the victim's banking accounts, make financial transactions on the victim's behalf, and others.

Except watering hole attacks, which tend to require a slightly higher level of technical sophistication, phishing/vishing/smishing attacks tend to be relatively simple to pursue, and that is reflected in the number of threat groups that employ consumer fraud techniques against the **European financial sector** tracked by Outpost24<sup>v</sup>: in TCx, there are 82 threat groups that fit in these categories.

Relevant techniques observed for threat actors included in Outpost24's TCx employing vishing, smishing, and watering hole as attack methods and focusing on financial services and Europe as targets<sup>iv</sup> are:

	Technique	Vulnerabilities and risks
●	Spearphishing Attachment [T1566.001] and Link [T1566.002]	Get access to the victim's device. Compromise the device with malware.
●	Drive-by Compromise [T1189]	Compromise the device with malware.
●	Credentials from Web Browsers [T1555.003]	Compromise credentials.
●	Keylogging [T1056.001]	Compromise credentials and other sensitive data.
●	Screen capture [T1113]	Compromise credentials and other sensitive data.
●	Input capture [T1056]	Compromise credentials and other sensitive data.

Affection to Confidentiality ● Integrity ● Availability ●

**BatLoader** is an initial access malware that utilizes malvertising techniques to spread. It primarily relies on batch and PowerShell scripts to gain unauthorized access to victims' machines and deploy additional malware. To carry out its malvertising campaigns, threat actors have employed Google Ads and the Keitaro Traffic Direction System (TDS) for their malicious activities. The majority of BatLoader infections have been detected in the United States, Canada, and Germany<sup>25</sup>. Interestingly, BatLoader is commercialized as a Malware-as-a-Service (MaaS) by **"Malsmoke"**. Notably, one of its clients is the **"Royal Group"**, which employs BatLoader to distribute the infamous Royal ransomware.

<sup>iv</sup> See the complete Attack Patterns Matrix in TCx using the following query: (description:~"watering hole" OR description:~"smishing" OR description:~"vishing" OR description:~"phishing") AND targets:"Europe" AND targets:"financial-services"

<sup>v</sup> In TCx, there are currently 113 threat groups involved in consumer fraud targeting the financial services sector globally. Therefore, groups targeting the European region represent 72,6% of the consumer fraud adversaries that target the sector globally.

### KEY POINTS

*(Out of data recovered from TCx)*

**Nation-State** actors might target the European financial industry for **economic espionage**, **destabilization** of a target country's economy, or to fund operations through **theft** as in the case of **North Korea**.

**Cybercriminals**, aiming for financial gain, resort to the **theft of personally identifiable information, credentials, and sensitive corporate documents**.

**Hacktivists** are involved in DDoS attacks and file leakage. As the financial sector plays key role in **policymaking**, it can be a prime target for **politically motivated** hacktivist groups to spread their message by targeting this critical sector.

**Initial Access Brokers (IAB)** aim to acquire access to a network using previously compromised credentials, brute force attacks, or using known **exploits over vulnerable infrastructure**. **Network access is resold** to other adversaries, such as ransomware groups.

In 2022, IAB "OxCee" offered **network access belonging to Deutsche Bank** for 7.5BTC (around **US\$132,000**).



## Threat Actor profiles

# Nation-State

Nation-state threat actors perform malicious activities on behalf of a government or military of a nation-state, mostly espionage operations to obtain strategic intelligence that will put the specific country in an advantage position. They can also operate as semi-independent groups that receive support or direction from a government<sup>27</sup>. Often described as Advanced Persistent Threat (APT), these cyber proxies have extensive access to funding, resources, and capabilities. They design and orchestrate highly sophisticated long-term campaigns by using an extremely evasive infrastructure to remain undetected for years and often even cover their tracks by planting ‘false flags’.

Nation-state actors target the *financial industry in Europe* for various reasons including economic espionage, destabilization of a target country’s economy, or to fund their own operations through theft as in the case of North Korea. Through long-term espionage campaigns, they can gain a competitive edge by stealing trade secrets and intellectual property and eavesdropping on policy discussions.

There are 32 active nation-states targeting the European financial sector according to TCx data, mainly operating from:

 China (11)  Russia (7)  Iran (5)  North Korea (4)

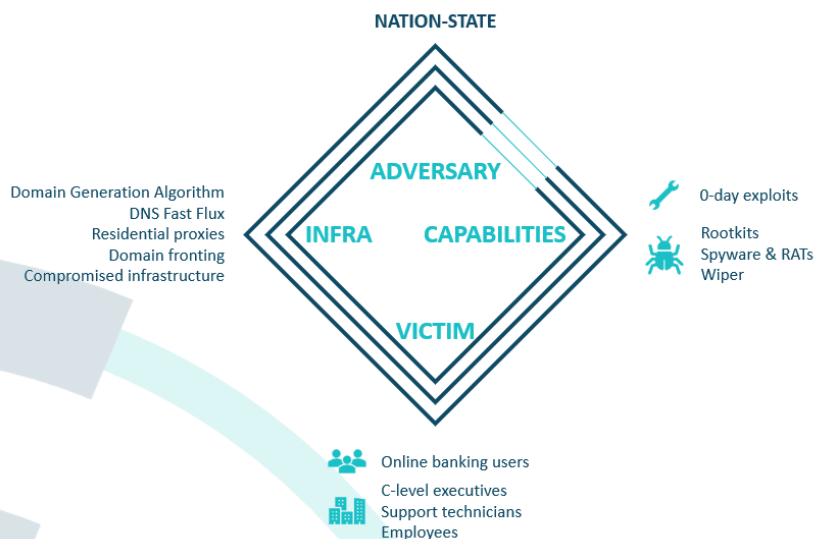


Figure 1. Diamond Model adapted<sup>vi</sup> to the elements related to Nation-State actors. Source: Outpost24’s analysts.

<sup>vi</sup> The Diamond Model is traditionally used to represent the key elements in a cluster of malicious activity. In this report we are including a general one with the main elements related to each type of threat actor.

## APT27

In January 2022, the German Bundesamt für Verfassungsschutz (BfV)<sup>26</sup> reported the *Chinese* state-sponsored threat actor “APT27” exploited vulnerabilities in Zoho ManageEngine ADSelfService Plus and Microsoft Exchange Server to infiltrate German companies. After gaining initial access, APT27 installed the HyperBro Remote Access Trojan (RAT) to steal business secrets and intellectual property.

The specific vulnerabilities exploited were CVE-2021-40539 in Zoho ManageEngine ADSelfService Plus and CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 in Microsoft Exchange Server.



# Cybercriminals

*Ransomware, traffers, BEC, hackers-for-hire groups, etc.*

Cybercriminals are motivated by the pursuit of financial gain, making them a significant threat to the financial services industry. Their tactics frequently involve the theft of various types of data, such as personally identifiable information (PII), credentials<sup>32</sup>, and sensitive corporate documents, which they then sell to the highest bidder on underground markets<sup>33</sup>. Furthermore, they employ more direct methods to illicitly obtain or generate revenue, including carding attacks, which involve compromising credit and debit cards and the use of multiple methods to cash out, deceiving employees and clients of banking institutions to execute fraudulent transactions, hijacking computer resources for cryptocurrency mining, or resorting to extortion through ransomware attacks. Depending on their degree of sophistication, these actors may initiate relatively straightforward social engineering schemes or engage in complex exploitations such as targeting software vulnerabilities within a banking system. There are 55 active threat actors classified as crime-syndicate in TCx targeting the European financial services sector.

As of 2023, one of the most significant threats impacting the **financial services industry** is digital skimming. In these instances, the adversary injects a malicious script—often referred to as a skimmer—into the payment cart of an e-commerce site to steal credit card data and other personal information introduced by the client. According to Visa’s biannual threats report<sup>34</sup>, skimming cases globally increased 174% in the June-November 2022 period when compared to December 2021-May 2022.

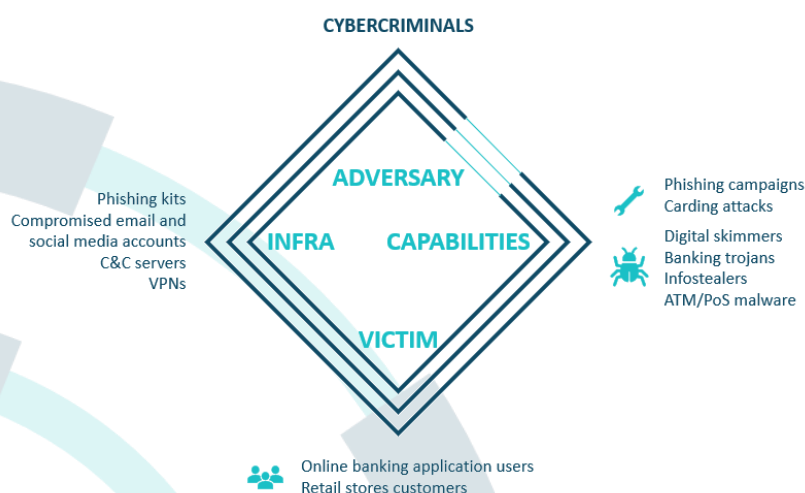


Figure 2. Diamond Model adapted to the elements related to Cybercriminals.

## DeathStalker

One clear example of cybercriminals are the **hackers-for-hire** groups, which are nothing else than groups focused on compromising accounts and exfiltrating data as a service<sup>28</sup>.

One of these groups targeting the financial services sector, specifically companies dealing with trading and compliance in the UK and Europe is known as “DeathStalker”<sup>29</sup> (or “Evilnum”<sup>30 31</sup>). The group’s main goal would be obtaining financial information from both the targeted companies and their customers.

To do so, they mainly use spear-phishing emails sent to technical support representatives and account managers working in the targeted companies. These emails include links to ZIP files hosted on cloud services which, in turn, contain malicious files that end up downloading malware families, either deployed by them or purchased from other groups. This last idea proves for the group both developing capabilities as well as a presence and collaboration in the cybercriminal underground.

# Hacktivists

As briefly discussed previously in the DDoS section, hacktivists are groups that pursue an ideological agenda – be it political, religious, cultural, or economic – and use cyberattacks in the most diverse forms to advance these objectives. A hacktivist cyberattack implies that the group aims the disruption of services, but the group does not intend to cause harm – especially because hacktivist groups tend to be less sophisticated in nature, as they simply want to make a statement with their actions and pressure stakeholders to take actions that align with the hacktivist group and its allies' objectives. This is illustrated by the observed capabilities and infrastructure leveraged by such actors in the custom diamond model found below. There are currently only 12 adversaries classified as hacktivists targeting the European financial services sector in TCx, but these represent 66,7% of the number of hacktivists targeting the sector globally.

As highlighted in the [Distributed Denial of Service](#) section (page 9), hacktivists are not the only adversaries that conduct DDoS attacks. However, it is notable how some of the most relevant techniques employed by hacktivists consist of DDoS-related techniques. Yet, hacktivists are also interested in obtaining access to the targeted network to be able to collect files that might later be leaked online in Telegram channels or other platforms.

These groups represent a threat to the [financial services sector](#) as these companies play key roles in policymaking, so it is interesting for hacktivist groups to spread their message by targeting this critical sector. The financial services sector might be impacted either by the theft and exposure of employees' credentials, theft and exposure of clients' personable identifiable information and/or financial information, interruption of activities as online resources become unavailable to clients, and more.

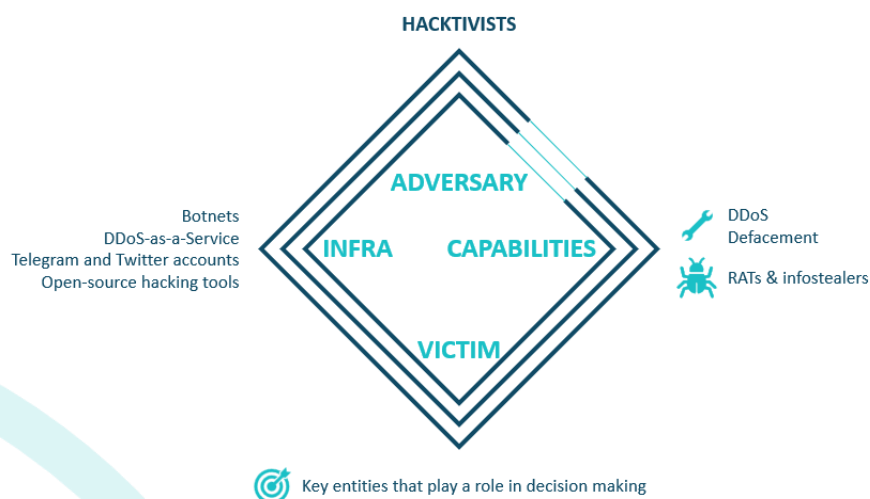


Figure 3. Diamond Model adapted to the elements related to Hacktivists.

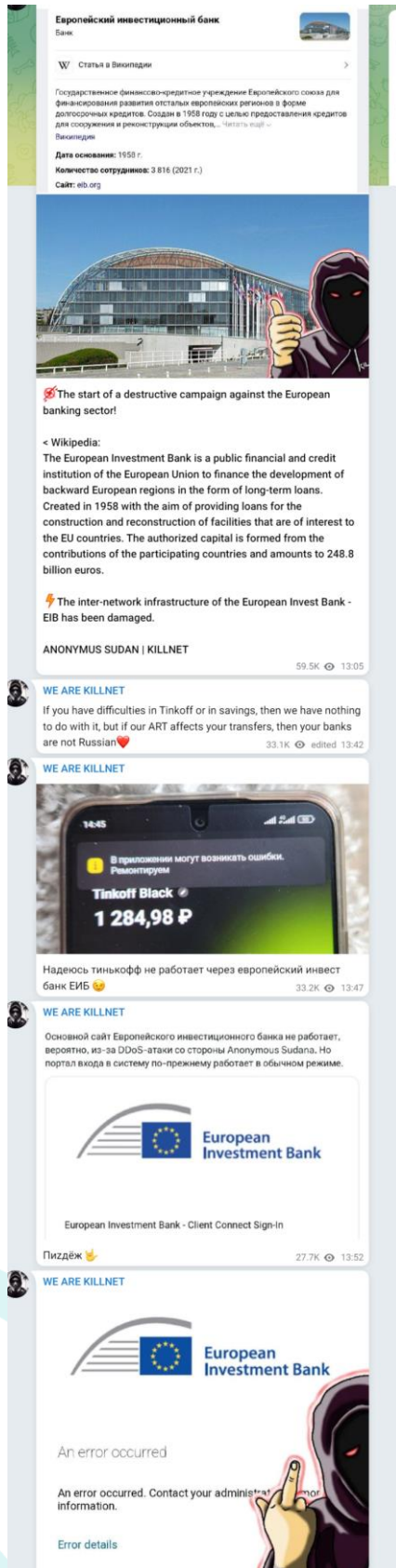


Figure 4. Hacktivist group "KillNet" exposes its DDoS attack against the EIC (automatically translated from Russian).

## KillNet

An especially relevant illustration of a hacktivist attack against the European financial services sector is one from early June 2023, in which the hacktivist group "KillNet", together with "Anonymous Sudan", declared to have decided to target the "European banking transfer systems SEPA, IBAN, WIRE, SWIFT, WISE". On June 19, through its Twitter account, the European Investment Bank (EIC) confirmed<sup>35</sup> that it was undergoing a cyberattack that impacted two of its websites: eib.org and eif.org. KillNet advertised its mischief through its Telegram channel.

# Initial Access Brokers (IAB)

Initial Access Brokers (IAB) are users who seek to procure access to a network and sell it to other threat actors for them to continue with their malicious activities; therefore, IABs mainly pursue an economic benefit with their activities. They try to gain access to a network in every possible way, but the most common methods observed would be using previously compromised credentials, brute force attacks, or using known exploits over vulnerable infrastructure. Some of these techniques require previous phases, launching phishing campaigns or watering hole attacks to compromise the users' credentials, or actively scanning for vulnerable public-facing applications in open-source engines. Currently, 18 threat actors described as Initial Access Brokers targeting the European financial services sector have been evaluated as relevant enough to be included in TCx.

They have an **active presence in underground markets** and forums, where they advertise the access achieved to potential buyers. Their publications tend to give hints about the access and the company compromised but do not give exact details, which are reserved for the buyers. IABs usually sell to the best buyer, and one of these clients that usually go for the higher bid are Ransomware-as-a-Service groups<sup>36</sup>.

IABs not only try to gain access to a network but also gain access to whatever network they can. However, even if they try to compromise anything, they do tend to prioritize those accesses that will report a greater benefit for belonging to companies with significant benefits or in significant geographic locations. Bearing this in mind, there is no need to say that **financial companies located in Europe** are among the crown jewels for them.

## OxCee

One IAB that hit the jackpot recently was the one behind the nickname "OxCee", when in November 2022 offered for 7.5BTC, access to the internal network of a particular bank. Even if the bank's name was not mentioned, the text was shared along with an image in which German's Deutsche Bank logo was shown. OxCee runs the private Telegram channel dubbed "Ox\_dump" since at least July 2022, in which it not only sells access to company networks but also offers for sale databases of important international companies, shares vulnerability information, hacking tutorials, credit and debit cards, and source code of malware.

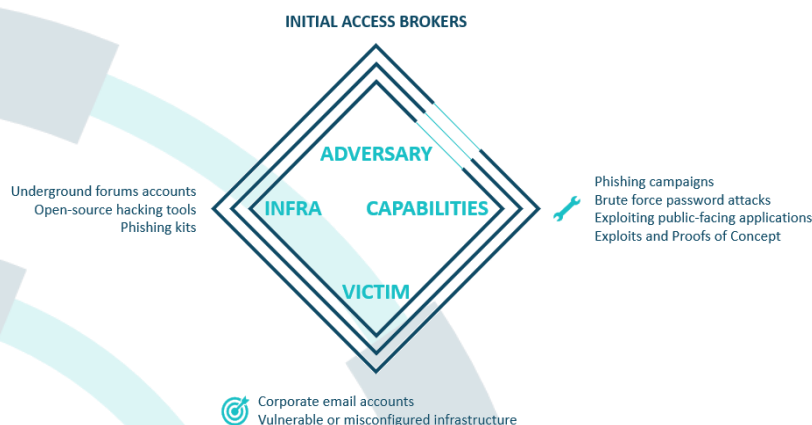


Figure 5. Diamond Model adapted to the elements related to Initial Access Brokers.

## KEY POINTS

**Steganography** is a form of digital deception where **information is hidden in digital media** such as images, audios, videos, or text documents. APTs are increasingly using it due to its potential to **bypass traditional standard detection systems**.

**Artificial Intelligence** misuses include the **craft of convincing phishing emails** or automatically generating **improving malware code** and obfuscation techniques. Another risk is **prompt injection attacks**: manipulating the AI model using prompts that make it ignore previous instructions and perform unintended actions.

**Deepfakes** associated risks are **corporate fraud** (the spread of disinformation about the brand or product) and **social engineering attacks** (impersonating relevant corporate figures or clients to bypass security measures).

In 2022, **Binance's CCO was impersonated** by a deepfake to trick clients to set up meetings with him.

### **Authentication and authorization bypass**

Despite being a relatively simple social engineering attack, in 2022, **Microsoft fell victim** to the "LAPSUS\$" group and **Cisco** to the "Yanluowang Group" in **MFA fatigue attacks**.



# Emerging Threats to the Financial Industry

# Steganography

Steganography is a form of digital deception where secret information is hidden in digital media such as images, audio files, video files, text documents, or even network control protocols, with the intent of communicating without revealing the existence of the communication<sup>37</sup>. Steganography is used by the financial sector to hide and secure transaction data and personally identifiable information (PII) from customers. Academic research is focusing nowadays on innovations to exchange encoded information safely<sup>38</sup>.

## WHY IS THE RISK INCREASING?

- **New extortion methods:** attackers can use steganographic techniques to hide sensitive data exfiltration and establish a covert control channel<sup>39</sup>, which is a greater concern since more and more ransomware groups exfiltrate data from targeted organizations prior to encryption. As ransomware gangs become more sophisticated, they could invest resources to implement advanced steganographic capabilities.

## CAN IT BE A RELEVANT THREAT?

- 🔴 **Hide malicious payloads:** Threat actors have already used it to hide malicious payloads into images or to exfiltrate sensitive information stolen from the victim.
- 🔴 **Bypass traditional systems:** Sophisticated groups like Advanced Persistent Threats (APTs), are increasingly using steganography to bypass standard detection systems<sup>40</sup>. It allows attackers to infiltrate networks undetected, exfiltrate sensitive data, and cause damage from the inside before the intrusion is even noticed. Financial institutions, given their vast store of sensitive data and high-volume digital transactions, are attractive targets for such attacks<sup>41</sup>.

In September 2022, ESET reported the espionage-focused threat actor “**Worok**” developed a steganographic loader dubbed PNGLoad<sup>42</sup> that uses bytes from PNG files to create a payload to execute. It uses a steganographic technique called least-significant bit (LSB) encoding<sup>43</sup> to extract hidden data from PNG files and convert it into executable code.

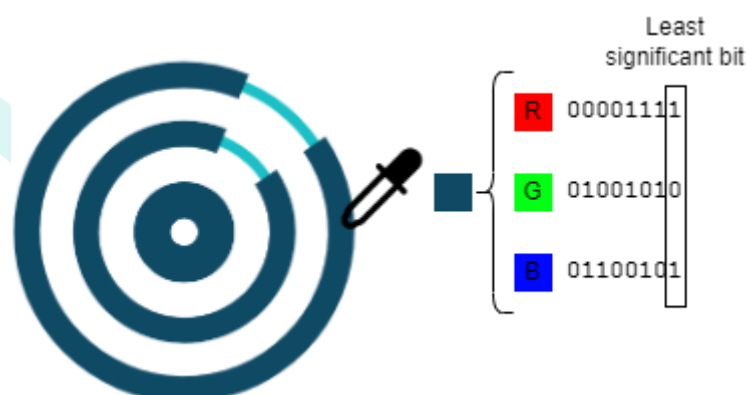


Figure 6. Example of what would be the least-significant bit (LSB) in Outpost24's logotype.




# Artificial Intelligence (AI)


AI is the field that combines computer science and robust datasets to enable problem-solving<sup>44</sup>. Sub-fields like machine learning and deep learning are comprised of AI algorithms that seek to create expert systems that make predictions or classifications based on input data.

## WHY IS THE RISK INCREASING?

- **New launches:** ChatGPT is an artificial intelligence chatbot that offers answers to inputs (prompts) understood thanks to the use of machine learning and natural language processing algorithms. It is built on different foundational models from the OpenAI's GPT-n series, which are no other than large machine learning models trained on a vast quantity of data. Perhaps because of the simplicity of its use and the wide range of possibilities that it offers, ChatGPT has become one of the most popular and fastest-growing apps<sup>45</sup>.
- **More uses:** The financial services industry has been taking advantage of AI for some time since it helps with the prediction of future outcomes by leveraging historical data sets to increase efficiency and enable new customer experiences<sup>46</sup>. AI is helping companies to improve customer services through virtual assistants, guarantees the safety of transactions by identifying consumption patterns, reduces missed payments using automatic notifications, or optimizes loan management, among other benefits<sup>47</sup>.

## CAN IT BE A RELEVANT THREAT?

 **Enhance attacks:** Attackers are using AI applications like ChatGPT to enhance their attacks by creating convincing **phishing emails**<sup>48</sup> or by automatically generating or **improving malware** code and obfuscation techniques so that it can better evade traditional security measures<sup>49 50</sup>.

 **More surface of attack:** Applications like ChatGPT are vulnerable to **prompt injection attacks**<sup>51</sup>. These attacks allow bypassing filters or manipulating the models using carefully crafted prompts that make the model ignore previous instructions or perform unintended actions. An example of what a prompt attack could be, for example, eliciting an unintended response from the tool and then achieving unauthorized access to the system<sup>52</sup>.

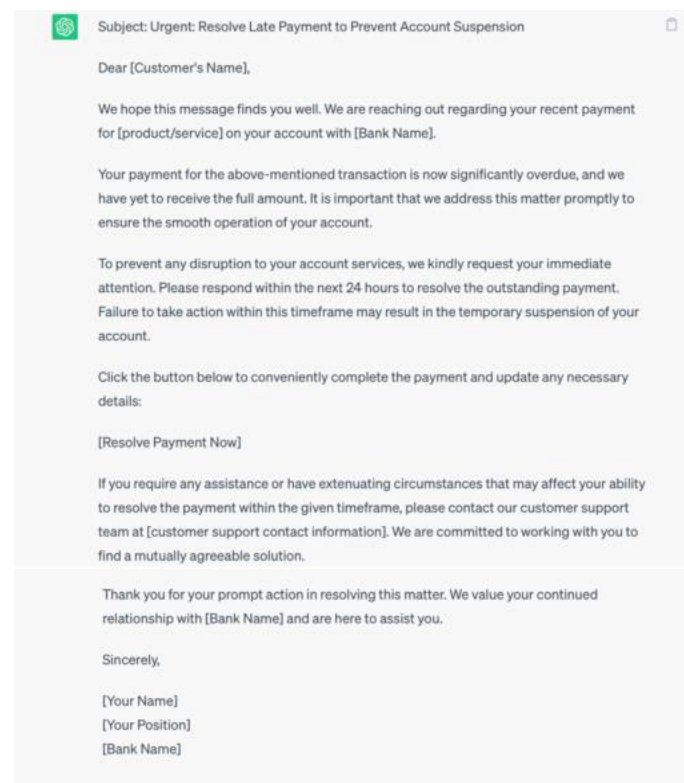


Figure 7. Example of a phishing email posing as a bank written by ChatGPT<sup>53</sup>.

# Deepfakes

Deepfakes are an emergent threat in which artificial intelligence/machine learning (AI/ML) is used to create believable videos, pictures, audio, and text of events that never happened<sup>54</sup>.

- **Face swap** implies altering an image to put a person's face or head onto another person's body.
- **Lip-syncing** involves mapping voice recording from one or multiple contexts to a video recording in another to make the subject of the video appear to say something authentic.
- **Puppet deepfake** allows the user to make the targeted individual move in ways they did not actually move, including facial movements or whole-body movements.

## WHY IS THE RISK INCREASING?

- **New technology**: Technology used to create deepfakes has evolved from the simple use of image editing software to new types of machine learning like deep learning or, more recently, adopting generative adversarial network (GAN) models<sup>55</sup>. Moreover, these techniques have turned out to be more accessible, increasing the risk deepfakes pose to the general population.
- **Simplicity**: Since the financial sector guarantees to a greater extent an immediate financial gain, it is seen as one of the most likely affected by low and mid-level cybercriminals taking advantage of deepfakes in their attacks and sharing their knowledge in underground forums<sup>56</sup>.

## CAN IT BE A RELEVANT THREAT?

- 🔴 **Spread misinformation**: One possible scenario in which threat actors could use deepfake with malicious intentions would be to **achieve corporate fraud** by using deepfake technology to spread misinformation about a company's product, place in the market, executives, overall brand, etc.
- 🔴 **Enhance attacks**: Another possible situation implies the use of deepfakes to enhance the success of **social engineering attacks** like impersonating a relevant figure like the CEO to get a financial transaction done (CEO Fraud) or simply impersonating a client to bypass the financial institution's verification policy.
- 🔴 **Legal risk**: Besides traditional risks, financial institutions could also be facing an increased legal risk due to affected consumers seeking damages and compensation derived from these attacks.

A real and recent example that proves that whatever is said about deepfakes is not mere science fiction anymore but can become a reality is what happened to the cryptocurrency exchange company **Binance**. In August 2022 Patrick Hillmann, the company's Chief Communications Officer, published a statement<sup>57</sup> describing how cybercriminals had created a deepfake impersonating him using previous news interviews and TV appearances and used it to trick people into maintaining meetings.




# Authorization and authentication bypass


Authorization is the function of specifying access rights/privileges to resources, while authentication is the act of proving an assertion, such as an identity.

## WHY IS THE RISK INCREASING?

- **Technological development:** The financial services sector is known for its state-of-the-art technological development, so targeting banking technology requires higher sophistication.
- **Robust security measures:** Blended methods such as overlay attacks [T1417.002]<sup>58</sup> together with the ability to intercept push and SMS notifications are known for allowing operators to harvest banking credentials and bypass 2FA. As a result of traditional security measures being vulnerable, banking institutions try constantly to implement more robust controls such as **biometric authentication**.

## CAN IT BE A RELEVANT THREAT?

 **Theoretical attacks:** Academics at Zhejiang University<sup>59</sup> were able to overcome attempt limits and liveness detection that protect mobile phones against brute-force attacks, by exploiting two vulnerabilities in smartphone fingerprint authentication systems. This brute-forcing fingerprint authentication technique was named **BrutePrint** but there are no pieces of evidence that indicate that is nothing more than a proof-of-concept.

 **New types of attacks: Multi-Factor Authentication (MFA) fatigue** (also known as MFA bombing or MFA spamming) attacks relies on the previous acquisition of credentials, so cybercriminals attempt to log into the victim's account uncountable times and therefore they bombard the victim with multiple push notifications asking for a sign-in confirmation. Initially, the victim will not approve the request, but after numerous notifications, they will eventually approve believing it was a mistake and end up giving access to their account to cybercriminals.

In the [Malware fraud](#) section (page 12), we discussed malware fraud in the form of ATM and POS malware. **Prilex** is a malware family developed for ATMs that later evolved into POS malware, and its latest iteration has Near-Field Communication (NFC)-related capabilities. NFC payments, popularly understood as contactless payments, are ever more common in POS across the world, and that would make the life of POS malware operators more difficult, as it (used to be) uncommon that this type of malware is able to capture payment data through NFC. Yet, Prilex turns the table around: since late 2022 it implements an option to block NFC-based transactions in compromised POS<sup>60</sup>. This way, the malware requests the card to be inserted into the payment device and the PIN – allowing operators to acquire banking information and credentials from victims. This is a great example of how even the most sophisticated banking security measures set in place to minimize threats can be bypassed by adversaries, who are still able to achieve their objectives.

### KEY POINTS

The **digital Euro** is a political move to promote the Euro's relevance in the international financial system, also in **response to the Chinese digital Yuan** and the aggressive expansion of China's influence worldwide.

**North Korea's bank and cryptocurrency heists**: the country historically resorted to financial heists as a revenue source for the country's nuclear and ballistic missile program, besides the need to surmount sanctions.

Emerging developments in the financial sector such as Decentralized Finance platforms will likely be targeted by North Korea.

**China's new regulation on 0-day vulnerability reporting** first to the Chinese government is likely aimed at **bolstering Chinese state-sponsored threat actors' offensive capabilities**.

The Russia-Ukraine war called for the new **German National Security Strategy** (NSS), **raising annual military expenditure** from 1,3% in 2021 to 2% of the country's GDP.

The German involvement in the Ukrainian cause led to an **increase in detected espionage activities and disinformation campaigns from Russia**.

**China is a partner, a competitor, and a systemic rival of Germany**. The Chinese ambition to use soft power to reshape the international order in its favor poses a threat to German security.



## Geopolitical and regulatory situation

# Overview of international events

*Having an impact on the financial industry in Europe*

## Key financial aspects

### Digital currency

The European Central Bank's research phase on the **digital Euro** will be finished by October 2023<sup>61</sup>. The Chinese Central Bank is more advanced than its European counterpart on this matter, with public sector workers from the Chinese city of Changshu started getting paid fully with the **digital Yuan** (e-CNY)<sup>62</sup> since May 2023.

🔗 Some Western stakeholders see the e-CNY as an urgent matter to respond to due to its potential global impact. Therefore, launching the Digital Euro is also a political move that intends to further internationalize and promote the Euro's relevance in the international financial system.

### Currency supremacy

The **Cross-Border Interbank Payment System** (CIPS), launched by the Chinese Central Bank in 2015, also aims to boost the liquidity of the Chinese currency by providing an alternative financial system to the ones that employ the US dollar. The ratio of success of the promotion can be seen with the share of Yuan in Chinese trade transactions going from about 10% in 2017 to about 20% in late 2022<sup>63</sup>.

🔗 Both Europe and China are questioning the US dollar's supremacy in the global financial system. Therefore, dynamic initiatives such as the digital Euro rise as a response to the aggressive expansion of China's influence and power worldwide.

### Currency fraud

The intersection between currency, digitalization, and avoiding currency supremacy has yet another facet. **North Korea** historically resorts to financial heists against cryptocurrency exchanges as an important revenue source for the country's nuclear and ballistic missile program<sup>64</sup>. Moreover, aside from cryptocurrency theft being the most common, in 2016, North Korea almost succeeded in a bank heist: they planned a US\$1 billion raid on Bangladesh's National Bank.

🔗 Pyongyang also wishes to surmount sanctions, so it is in its best interest to exploit vulnerabilities in technologies employed by financial institutions to secure large amounts of financial assets. Moreover, not focusing only on cryptocurrency allow hypothesizing that emerging developments in the financial sector such as Decentralized Finance (DeFi) platforms will likely be targeted by North Korea to economically support the regime and its projects<sup>65</sup>.

## Russia

From a security, economic, and political point of view, the **Russia-Ukraine war** represents a challenge for the European bloc.

↳ As one consequence of the war, Germany announced in the new National Security Strategy (NSS)<sup>66</sup> that it will raise its annual military expenditure: from 1,3% in 2021<sup>67</sup>, it will soon be raised to 2% of the country's GDP.

In June 2023, the Kiel Institute for the World Economy<sup>68</sup> ranked Germany in third place in the global ranking of total commitments to Ukraine (which comprises humanitarian, financial, and military aid): €2 billion in 2022, €5.4 billion in 2023, and additional authorizations for an additional €10.5 billion in the near future<sup>69</sup>.

The German involvement in the Ukrainian cause is not overlooked by the opposition: Germany's Federal Office for the Protection of the Constitution reported in June 2023 an increase in detected espionage activities and disinformation campaigns from Russia<sup>70</sup>, aiming at creating chaotic domestic environments abroad.

## China

Germany describes **China** in the NSS as a partner, a competitor, and a systemic rival.

↳ Although acknowledging the fundamental economic partnership Germany holds with China, the former understands that the Chinese ambition to use its soft power in a way to reshape the international order in its favor poses a threat to German security.

In September 2021, the Chinese government established a new regulation called "Provisions on Security Loopholes of Network Products"<sup>71</sup> that requires Chinese companies to report discovered **0-day vulnerabilities** first to the government.

↳ The measure is seen as aimed at bolstering Chinese state-sponsored threat actors' offensive cyber capabilities. Chinese state-sponsored cyber espionage groups exploited<sup>72</sup> at least 8 zero-day vulnerabilities in 2022, more than any other nation-state.

## Kazakhstan

In its rush to balance Chinese and Russian influence abroad, Germany seeks previously overlook partnerships, as is the case of **Kazakhstan**, which, in addition, figures amongst the 15 top global crude oil reserves<sup>73</sup>.

↳ Central Asia is a key region for Europe to set its presence and minimize the traditional influence of Russia in the region. Therefore, it comes as no surprise why the European Union and Germany would like to deepen relations with the Central Asian country and with the region in general – which is a welcoming open door into Asia and its giant powers China and Russia.



# Regulatory changes

*And their influence on the threat landscape*

## International

### **International Counter Ransomware Initiative (CRI)**

Led by the United States since 2021, with 17 European Union (EU) members associated + the EU. Aims to fight ransomware cooperatively at an international level:

- Establishing an International Counter Ransomware Task Force (ICRTF).
- Working with the private sector to stop malicious use of the cryptocurrency ecosystem.

### **Insurance coverage for cyberattacks**

**Ransomware:** Some countries discuss the possibility of establishing a ransom payment ban. However, insurance companies and organizations in the UK and Australia have been vocal against it<sup>74 75</sup>, arguing that the impact that such a ban could have on small and medium businesses could be bigger, as the ransom payment is often less of a burden than the cost of recovery and remediation.

**State-sponsored attacks:** Despite the insurers' position on the ransom payment ban being favorable to businesses, this is not the case in the topic of nation-state cyberattack coverage. Since 2021, the Lloyd's of London does not cover any loss from a cyberattack if it has a major detrimental impact on an essential service in that state – including the financial infrastructure<sup>76</sup>.

## European Union

### **NIS 2 Directive<sup>77</sup>**

Adopted in January 2023. States must transpose measures into national law by October 2024.

- ✓ Creates a cyber crisis management structure (CyCLONe).
- ✓ Harmonizes security requirements and reporting obligations.
- ✓ Introduces new areas of interest such as supply chain, vulnerability management, core internet, and cyber hygiene into national cybersecurity strategies and the creation of a European vulnerability database.

### **Digital Operations Resilience Act (DORA)<sup>78</sup>**

Sets new rules for digital safety in the EU in the context of the financial industry. Requires financial institutions and third-party suppliers to be prepared for digital threats and disruptions, being able to prevent, manage and effectively recover from cyber-related disruptions. Encourages sharing cyber threat intelligence.

### **Threat Intelligence-Based Ethical Red Teaming European Framework TIBER-EU<sup>79</sup>**

Meant to improve financial institutions' cyber resilience by simulating the tactics, strategies, and procedures of real-world attackers based on threat intelligence.

Multiple teams are involved in the assessment: blue team (detection and response), threat intelligence provider, red team (executing the simulated attack), white team (administering the test internally), and TIBER cyber team (overseeing the process).

### EU Cyber Resilience Act<sup>80</sup>

- ✓ Aims to minimize the vulnerabilities in digital products sold within the EU by imposing continuous cybersecurity responsibilities on manufacturers.
- ✓ Promotes transparency in the security of hardware and software products and enhances protection for consumers and businesses.
- ✓ Sets a new standard for the manufacturers involved in the supply chain.

### Artificial Intelligence Act<sup>81</sup>

Expected to be approved by the end of 2023, will classify the different types of risk of AI, from minimal to unacceptable, and technologies deemed as an unacceptable risk will be banned.

### European Chips Act<sup>82</sup>

Aims to strengthen European competitiveness and resilience via research and technological leadership, building and reinforcing Europe's capacity to innovate in the design, manufacturing, and packaging of advanced chips.

## Germany

The long-awaited *German National Security Strategy (NSS)*, in the works since late 2021, was released in June 2023<sup>83</sup>. The document establishes Germany's vision and ambitions for its future in terms of national security but does not set out a specific plan of action or establish the applicability of the defined priorities. Despite being a general guideline on the all-encompassing national security theme the NSS impacts all organizations within the German territory. The NSS highlights a few focal points for the cybersecurity realm, in which Outpost24's analysts observe fragilities:

1. *The threat of ransomware is believed to pose a national security-level of threat to public, private, and critical infrastructure German institutions.* It does not specify how to fight ransomware, in defense but also organizational terms within the German state.
2. *Criminal prosecution of cyber attackers, expanding the legal basis for that purpose by working on amendments to the Basic Law (Grundgesetz).* It does not detail the nature of the envisioned amendments or clarify if and how bodies of authority will hold more responsibilities and powers to combat cyber threats. In the legal realm, the NSS only suggests that when cyberattacks are perpetrated by foreign actors, the German state shall sanction them<sup>84</sup>.
3. *The pursuance of allied cyber defense in similar terms as the existing shared defense basis for NATO member countries.* This point is especially controversial, as the NSS claims that cyberattacks may be equivalent to armed conflicts. NATO states that an armed conflict calls for an immediate collective response<sup>85</sup>, so the point could imply that Germany understands that cyberattacks might be transposed to the military realm, following International Humanitarian Law principles on armed conflicts<sup>86</sup>. However, in a later paragraph, the NSS rejects the idea of using hack-backs as a means of cyber defense. Thus, all these pieces of information are contradictory.
4. *Creating Computer Emergency Response Teams (CERTs) for specific sectors.* This point does not define the sectors envisioned for the thematic CERTs.
5. *Establishing information sharing channels between critical infrastructure companies and the Federal Office for Information Security.* Not suggesting what form these channels should take.



# Mitigation strategies

All the highlighted threats pose an elevated risk to the financial sector nowadays. Some of them like DDoS, ransomware, supply chain, or BEC attacks might have a more direct impact on the business and must be confronted to avoid **legal, financial, security, or reputational consequences**. On the other hand, threats like malware or consumer fraud tend to be the most frequent ones against the client baseline and must be confronted to avoid the reputational and economic damage they pose.

<i>Ransomware</i>	<ul style="list-style-type: none"> <li>Establish <b>training plans</b> for employees for early and proactive detection.</li> <li><b>Avoid exposure</b> to remote access and follow a systems and services maintenance policy focusing on system <b>security updates</b>.</li> <li>Reduction of <b>users' permissions</b>, trying to limit admin roles.</li> <li>Establish <b>monitoring plans</b> for early detection of possible intrusions.</li> <li>Define a policy of frequent and incremental <b>backups</b> on isolated systems.</li> </ul>
<i>Distributed Denial of Service</i>	<ul style="list-style-type: none"> <li>Implement <b>bot traffic detection</b> system as well as <b>Anti-DDoS services</b>.</li> <li><b>Avoid</b> unnecessary <b>exposure</b> of the infrastructure and follow a systems and services maintenance policy focusing on system <b>security updates</b>.</li> <li>Have a <b>DDoS response plan</b>.</li> <li>Maintain and <b>update</b> company websites <b>and restrict</b> modify permissions.</li> </ul>
<i>Supply chain attacks</i>	<ul style="list-style-type: none"> <li>Define security <b>requirements and obligations</b> for the products and services required and include them in contracts.</li> <li>Demand <b>periodic controls</b> for suppliers, such as obtaining certifications or technical reviews of security control designs and their fourth-party vendor dependencies.</li> <li>Establish an effective and well-protected <b>Privilege Access Management (PAM)</b> framework, reducing the number of privileged access roles and controlling the level of access from vendors to sensitive data.</li> </ul>
<i>Malware fraud</i>	<ul style="list-style-type: none"> <li>Direct an effective communication strategy that establishes <b>periodic warnings and training plans</b> for customers and the general population through public channels.</li> <li>Periodically maintain and <b>update</b> resources like POS terminals or ATMs.</li> </ul>
<i>Business Email Compromise</i>	<ul style="list-style-type: none"> <li><b>Avoid unnecessary exposure</b> of company and employee data.</li> <li>Establish <b>monitoring plans</b> for early detection of data leakage or spoofing domain registration.</li> <li>Implementing <b>email security solutions and rules</b> on mail servers to reject or quarantine emails that do not verify record checks like SPF and DKIM.</li> <li>Assess and define the roles within the company with the biggest risks and establish <b>training plans</b> for employees adjusted to their risk level.</li> </ul>
<i>Consumer fraud</i>	<ul style="list-style-type: none"> <li>Direct an effective communication strategy that establishes <b>periodic warnings and training plans</b> for customers and the general population through public channels.</li> <li>Study <b>alternatives to passwords</b> as security measures for clients.</li> </ul>

Risk associated: **High** | **Medium** | **Low**

# References

- <sup>1</sup> European Central Bank (2023, May). Report on card fraud in 2020 and 2021. Retrieved July 25, 2023, from <https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.es.html>
- <sup>2</sup> ENISA (2022, November 3). ENISA Threat Landscape 2022. Retrieved on 2023, July 25, from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>
- <sup>3</sup> Ibid.
- <sup>4</sup> FS-ISAC & Akamai (2023, January). The Evolution of DDoS: Return of the Hacktivists. Retrieved July 25, 2023, from <https://www.fsisac.com/hubfs/Reports/EvolutionOfDDoS-ReturnOfTheHacktivists.pdf?hsCtaTracking=f9b1f8bc-c11b-43a0-bd28-ff6680aba49c%7C7e8b3e7b-bb01-4d7c-8e43-e226aaa8c980>
- <sup>5</sup> European Commission (2022, September 15). Cyber Resilience Act – Factsheet. Retrieved July 25, 2023, from <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet>
- <sup>6</sup> ENISA (2023, February 23). Cyber Insurance: Fitting the Needs of Operators of Essential Services? Retrieved July 25, 2023, from <https://www.enisa.europa.eu/news/cyber-insurance-fitting-the-needs-of-operators-of-essential-services>
- <sup>7</sup> European Commission (2022, September 15). Cyber Resilience Act – Factsheet. Retrieved July 25, 2023, from <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet>
- <sup>8</sup> Outpost24 (2023, February 7). Ransomware Report 2023: Targets, Motives, and Trends. Retrieved June 12, 2023, from <https://outpost24.com/blog/ransomware-report-2023>
- <sup>9</sup> Redpacketsecurity (2022, January 29). LockBit 2.0 Ransomware Victim: heubeck[.]de. Retrieved June 12, 2023, from <https://www.redpacketsecurity.com/lockbit-2-0-ransomware-victim-heubeck-de/>
- <sup>10</sup> FS-ISAC & Akamai (2023, February). The Evolution of DDoS: Return of the Hacktivists. Retrieved June 14, 2023, from <https://www.fsisac.com/hubfs/Reports/EvolutionOfDDoS-ReturnOfTheHacktivists.pdf>
- <sup>11</sup> ENISA (2021, July 29). Threat Landscape for Supply Chain Attacks. Retrieved June 16, 2023, from <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>
- <sup>12</sup> Huntress (2023, August 2). Investigating Intrusions From Intriguing Exploits. Retrieved June 19, 2023, from <https://www.huntress.com/blog/investigating-intrusions-from-intriguing-exploits>
- <sup>13</sup> BrianKrebs [@briankrebs@infosec.exchange] (2023, February 2). Message. Mastodon. Retrieved June 19, 2023, from <https://infosec.exchange/@briankrebs/109795710941843934>
- <sup>14</sup> Techcrunch (2023, March 22). New victims come forward after mass-ransomware attack. Retrieved June 19, 2023, from <https://techcrunch.com/2023/03/22/fortra-goanywhere-ransomware-attack/>
- <sup>15</sup> Munich RE (2023, March 27). Information security incident at an external service provider. Retrieved June 19, 2023, from <https://www.munichre.com/en/company/media-relations/statements/2023/information-security-incident-external-service-provider.html>
- <sup>16</sup> SecureList by Kaspersky (2023, March 29). Financial cyberthreats in 2022. Retrieved June 16, 2023, from <https://securelist.com/financial-cyberthreats-in-2022/109219/>
- <sup>17</sup> European Central Bank (2023, May). Report on card fraud in 2020 and 2021. Retrieved June 16, 2023, from <https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.es.html>
- <sup>18</sup> BaFin Federal Financial Supervisory Authority. (2023, January 9). Warning: Current malware "Godfather" attacks banking and crypto apps. Retrieved June 15, 2023, from [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/weitere/2023/meldung\\_2023\\_01\\_09\\_warnung\\_aktuelle\\_schadsoftware.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/weitere/2023/meldung_2023_01_09_warnung_aktuelle_schadsoftware.html)
- <sup>19</sup> Group-IB. (2022, November 9). Godfather: A banking Trojan that is impossible to refuse. Retrieved June 15, 2023, from <https://www.group-ib.com/blog/godfather-trojan/>
- <sup>20</sup> Ibid.
- <sup>21</sup> Microsoft. What is business email compromise (BEC)? Retrieved June 20, 2023, from <https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec>
- <sup>22</sup> FBI (2022, February 16). Business Email Compromise: Virtual Meeting Platforms. Retrieved June 20, 2023, from <https://www.ic3.gov/Media/Y2022/PSA220216>
- <sup>23</sup> Scmagazine (2022, September 7). How financial institutions can mitigate business email compromise risks. Retrieved June 20, 2023, from <https://www.scmagazine.com/analysis/email-security/how-financial-institutions-can-mitigate-business-email-compromise-risks>
- <sup>24</sup> Trend Micro. (2023, February 2). What SOCs need to know about water dybbuk. Retrieved June 23, 2023, from [https://www.trendmicro.com/en\\_us/research/23/b/what-socs-need-to-know-about-water-dybbuk.html](https://www.trendmicro.com/en_us/research/23/b/what-socs-need-to-know-about-water-dybbuk.html)



- <sup>25</sup> TrendMicro (2023, January 17). Batloader Malware Abuses Legitimate Tools, Uses Obfuscated JavaScript Files in Q4 2022 Attacks. Recovered June 26, 2023, from [https://www.trendmicro.com/en\\_us/research/23/a/batloader-malware-abuses-legitimate-tools-uses-obfuscated-javasc.html](https://www.trendmicro.com/en_us/research/23/a/batloader-malware-abuses-legitimate-tools-uses-obfuscated-javasc.html)
- <sup>26</sup> Bundesamt für Verfassungsschutz (BfV) (2022, January). Cyberangriffskampagne gegen deutsche Wirtschaftsunternehmen. Retrieved June 23, 2023, from <https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2022/2022-01-26-cyberbrief.html>
- <sup>27</sup> Outpost24 (2023, June 13). ICS attack classifications: differentiating between cyberwarfare, cyberterrorism, and hacktivism. Retrieved June 12, 2023, from <https://outpost24.com/blog/ics-attack-classifications/>
- <sup>28</sup> Google (2022, June 30). Countering hack-for-hire groups. Retrieved June 12, 2023, from <https://blog.google/threat-analysis-group/countering-hack-for-hire-groups/>
- <sup>29</sup> Kaspersky (2020, August 24). Lifting the veil on DeathStalker, a mercenary triumvirate. Retrieved June 12, 2023, from <https://securelist.com/deathstalker-mercenary-triumvirate/98177/>
- <sup>30</sup> Zscaler (2022, June 27). Return of the Evilnum APT with updated TTPs and new targets. Retrieved June 12, 2023, from <https://www.zscaler.com/blogs/security-research/return-evilnum-apt-updated-ttps-and-new-targets>
- <sup>31</sup> ESET (2020, July 9). More evil: A deep look at Evilnum and its toolset. Retrieved June 12, 2023, from <https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/>
- <sup>32</sup> Outpost 24 KrakenLabs (2023, March 28). Traffers and the growing threat against credentials. Retrieved June 21, 2023, from <https://outpost24.com/blog/traffers-and-the-growing-threat-against-credentials/>
- <sup>33</sup> Outpost24 KrakenLabs (2023, February). Dark Commerce: Exploring the Cybercrime Industry. Retrieved June 21, 2023, from <https://outpost24.com/resources/threat-intelligence-dark-commerce/>
- <sup>34</sup> Visa Payment Fraud Disruption (2022, December). Biannual Threats Report. Retrieved June 21, 2023, from [https://cdn.visa.com/dam/visa/vgb/visanotification/PFD-Biannual\\_Report\\_December\\_2022\\_Public-ACCESSIBLE.pdf](https://cdn.visa.com/dam/visa/vgb/visanotification/PFD-Biannual_Report_December_2022_Public-ACCESSIBLE.pdf)
- <sup>35</sup> European Investment Bank [EIB]. (2023, June 19). Retrieved June 20, 2023, from <https://twitter.com/EIB/status/1670783791600656384>
- <sup>36</sup> Outpost24 (2021, June 28). Use of Initial Access Brokers by Ransomware Groups. Retrieved June 20, 2023, from <https://outpost24.com/blog/Use-of-initial-access-brokers-by-ransomware-groups>
- <sup>37</sup> ESET (2023, August 2). What is steganography? Definition and explanation. Retrieved June 22, 2023, from <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>
- <sup>38</sup> M. Shirali-Shahreza, "Improving Mobile Banking Security Using Steganography," Fourth International Conference on Information Technology (ITNG'07), Las Vegas, NV, USA, 2007, pp. 885-887. Retrieved June 22, 2023, from <https://doi.org/10.1109/ITNG.2007.108>
- <sup>39</sup> Hildebrandt, Mario & Altschaffel, Robert & Lamshöft, Kevin & Lange, Mathias & Ding, Yongjian & Vielhauer, Claus & Dittmann, Jana. (2020). Threat Analysis of Steganographic and Covert Communication in Nuclear I&C Systems. International Conference on Nuclear Security 2020. Retrieved July 27, 2023, from [https://conferences.iaea.org/event/181/contributions/15608/attachments/8569/11404/CN278\\_478-stealth\\_v006.pdf](https://conferences.iaea.org/event/181/contributions/15608/attachments/8569/11404/CN278_478-stealth_v006.pdf)
- <sup>40</sup> Unit42 (2020, July 22). OilRig Targets Middle Eastern Telecommunications Organization and Adds Novel C2 Channel with Steganography to Its Inventory. Retrieved July 27, 2023, from <https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/>
- <sup>41</sup> India Tech Online (2023, July 25). A threat to online financial transactions: steganography. Retrieved June 22, 2023, from <https://www.indiatechonline.com/special-feature.php?id=287>
- <sup>42</sup> ESET WeLiveSecurity (2022, November 10) Worok: The big picture. Retrieved June 22, 2023, from <https://www.welivesecurity.com/2022/09/06/worok-big-picture/>
- <sup>43</sup> Avast (2022, November 10) PNG Steganography Hides Backdoor. Retrieved June 22, 2023, from <https://decoded.avast.io/martinchlumecky/png-steganography/>
- <sup>44</sup> IBM. What is artificial intelligence (AI)? Retrieved June 20, 2023, from <https://www.ibm.com/topics/artificial-intelligence>
- <sup>45</sup> Forbes (2023, February 2). ChatGPT Is The Fastest Growing App In The History Of Web Applications. Retrieved June 20, 2023, from <https://www.forbes.com/sites/cindygordon/2023/02/02/chatgpt-is-the-fastest-growing-ap-in-the-history-of-web-applications/>
- <sup>46</sup> Intel. AI in Financial Services. Retrieved June 20, 2023, from <https://www.intel.com/content/www/us/en/financial-services-it/fintech/ai-in-financial-services.html>
- <sup>47</sup> Santander (2023, April 28). What is artificial intelligence and how does it affect banking? Retrieved June 20, 2023, from <https://www.santander.com/en/stories/artificial-intelligence>
- <sup>48</sup> Sayak Saha Roy, S., Vamsi Naragam, K., & Nilizadeh, S. Generating Phishing Attacks using ChatGPT. Retrieved June 20, 2023, from <https://arxiv.org/pdf/2305.05133.pdf>

- <sup>49</sup> Hyas (2023, March 7). BLACKMAMBA: USING AI TO GENERATE POLYMORPHIC MALWARE. Retrieved June 24, 2023, from <https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware>
- <sup>50</sup> Malwarebytes (2023, March 28). ChatGPT happy to write ransomware, just really bad at it. Retrieved June 24, 2023, from <https://www.malwarebytes.com/blog/news/2023/03/chatgpt-happy-to-write-ransomware-just-really-bad-at-it>
- <sup>51</sup> OWASP. OWASP Top 10 List for Large Language Models version 0.1. Retrieved June 23, 2023, from <https://owasp.org/www-project-top-10-for-large-language-model-applications/descriptions/>
- <sup>52</sup> Cobalt (2023, May 31). Prompt Injection Attacks: A New Frontier in Cybersecurity. Retrieved June 23, 2023, from <https://www.cobalt.io/blog/prompt-injection-attacks>
- <sup>53</sup> NameShield (2023, June 15). ChatGPT, can you write a phishing email? Retrieved July 26, 2023, from <https://blog.nameshield.com/blog/2023/06/15/chatgpt-can-you-write-a-phishing-email/>
- <sup>54</sup> DHS (2022, October 6). Increasing Threat of Deepfake Identities. Retrieved June 23, 2023, from [https://www.dhs.gov/sites/default/files/publications/increasing\\_threats\\_of\\_deepfake\\_identities\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf)
- <sup>55</sup> Europol (2022, April 28). Facing reality? Law enforcement and the challenge of deepfakes. Retrieved June 23, 2023, from [https://www.europol.europa.eu/cms/sites/default/files/documents/Europol\\_Innovation\\_Lab\\_Facing\\_Reality\\_Law\\_Enforcement\\_And\\_The\\_Challenge\\_Of\\_Deepfakes.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf)
- <sup>56</sup> TrendMicro (2022, September 27). How Underground Groups Use Stolen Identities and Deepfakes. Retrieved June 23, 2023, from [https://www.trendmicro.com/en\\_us/research/22/i/how-underground-groups-use-stolen-identities-and-deepfakes.html](https://www.trendmicro.com/en_us/research/22/i/how-underground-groups-use-stolen-identities-and-deepfakes.html)
- <sup>57</sup> Binance (2022, August 17). Scammers Created an AI Hologram of Me to Scam Unsuspecting Projects. Retrieved June 23, 2023, from <https://www.binance.com/en/blog/community/scammers-created-an-ai-hologram-of-me-to-scam-unsuspecting-projects-6406050849026267209>
- <sup>58</sup> MITRE ATT&CK®. (2023). Input capture: GUI input capture, sub-technique T1417.002 - Mobile. Retrieved June 27, 2023, from <https://attack.mitre.org/techniques/T1417/002/>
- <sup>59</sup> Chen, Y., & He, Y. (2023, May 18). BRUTEPRINT: Expose Smartphone Fingerprint Authentication to Brute-force Attack. Retrieved June 27, 2023, from <https://arxiv.org/pdf/2305.10791.pdf>
- <sup>60</sup> Kaspersky. (2023, January 31). New versions of Prilex POS malware blocking NFC transactions. Retrieved June 27, 2023, from <https://securelist.com/prilex-modification-now-targeting-contactless-credit-card-transactions/108569/>
- <sup>61</sup> European Central Bank. (2023, June 28). ECB welcomes European Commission legislative proposals on digital euro and cash. Retrieved July 3, 2023, from <https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230628~e76738d851.en.html>
- <sup>62</sup> CNN. (2023, April 24). China makes major push in its ambitious digital Yuan project | CNN business. Retrieved July 4, 2023, from <https://edition.cnn.com/2023/04/24/economy/china-digital-yuan-government-salary-intl-hnk/index.html>
- <sup>63</sup> Bloomberg. (2023, March 30). Brazil Takes Steps to Transact in Yuan as China Ties Grow. Retrieved July 4, 2023, from <https://www.bloomberg.com/news/articles/2023-03-30/brazil-takes-steps-to-transact-in-yuan-as-ties-with-china-grow>
- <sup>64</sup> BBC News. (2022, February 6). North Korea: Missile programme funded through stolen crypto, UN report says. Retrieved July 4, 2023, from <https://www.bbc.com/news/world-asia-60281129>
- <sup>65</sup> The Diplomat. (2021, December 22). What will North Korean cybercrime look like in 2022? Retrieved July 5, 2023, from <https://thediplomat.com/2021/12/what-will-north-korean-cybercrime-look-like-in-2022/>
- <sup>66</sup> Federal Government of Germany. (2023, June 14). German National Security Strategy. Retrieved June 28, 2023, from <https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf>
- <sup>67</sup> The World Bank. (n.d.). Military expenditure (% of GDP) - European Union. Retrieved June 28, 2023, from <https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?locations=EU>
- <sup>68</sup> Kiel Institute for the World Economy. (2023, June 6). Ukraine support tracker. Retrieved June 29, 2023, from <https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/>
- <sup>69</sup> Federal Government of Germany. (2023, June 21). Military support for Ukraine. Retrieved June 29, 2023, from <https://www.bundesregierung.de/breg-en/news/military-support-ukraine-2054992>
- <sup>70</sup> DW. (2023, June 20). Germany sees 'more aggressive' Russian spy activity. Retrieved June 29, 2023, from <https://www.dw.com/en/germany-sees-more-aggressive-russian-spy-activity/a-65970734>
- <sup>71</sup> Ministry of Industry and Information Technology, the Cyberspace Administration of China, and the Ministry of Public Security (2021, November 28). Notice on Printing and Distributing the Regulations on the Management of Network Product Security Vulnerabilities. Retrieved June 30, 2023 from [https://www.gov.cn/gongbao/content/2021/content\\_5641351.htm](https://www.gov.cn/gongbao/content/2021/content_5641351.htm)
- <sup>72</sup> Mandiant (2023, March 20). Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace. Retrieved July 30, 2023, from <https://www.mandiant.com/resources/blog/zero-days-exploited-2022>

- <sup>73</sup> Organisation of the Petroleum Exporting Countries. (2022). Annual statistical bulletin 2022. Retrieved June 29, 2023, from <https://asb.opec.org/index.html>
- <sup>74</sup> The Stack. (2023, May 24). Government must avoid banning ransomware payments say insurers. Retrieved July 5, 2023, from <https://www.thestack.technology/government-must-avoid-banning-ransomware-payments-say-insurers/>
- <sup>75</sup> Cyber Security Connect. (2023, April 18). Insurers hesitant for government to outlaw ransomware payments. Retrieved July 5, 2023, from <https://www.cybersecurityconnect.com.au/policy/8935-insurers-hesitant-for-government-to-outlaw-ransomware-payments>
- <sup>76</sup> Lloyd's Market Association. (2021, November 25). Cyber War and Cyber Operation Exclusion Clauses. Retrieved July 6, 2023, from [https://www.lmalloyds.com/LMA/News/LMA\\_bulletins/LMA\\_Bulletins/LMA21-042-PD.aspx](https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx)
- <sup>77</sup> ENISA (2023, January 16). NIS Directive. Retrieved July 6, 2023, from <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new>
- <sup>78</sup> Official Journal of the European Union (2022, December 27). REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Retrieved July 5, 2023, from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=en>
- <sup>79</sup> European Central Bank (2018, May). TIBER-EU FRAMEWORK: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. Retrieved July 5, 2023, from [https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber\\_eu\\_framework.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf)
- <sup>80</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Retrieved July 5, 2023, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454>
- <sup>81</sup> Foreign Policy (2023, June 14). EU Lawmakers Pass Landmark AI Regulation Bill. Retrieved July 6, 2023, from <https://foreignpolicy.com/2023/06/14/eu-ai-act-european-union-chatgpt-regulations-transparency-privacy/>
- <sup>82</sup> European Commission (2023, April 18). Commission welcomes political agreement on the European Chips Act. Retrieved July 7, 2023, from [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_2045](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2045)
- <sup>83</sup> Germany's Federal Government. (2023, June 14). German National Security Strategy. Retrieved June 28, 2023, from <https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf>
- <sup>84</sup> Ibid.
- <sup>85</sup> NATO. (1949, April 4). The North Atlantic Treaty. Retrieved June 29, 2023, from [https://www.nato.int/cps/en/natolive/official\\_texts\\_17120.htm](https://www.nato.int/cps/en/natolive/official_texts_17120.htm)
- <sup>86</sup> Ibid.