

Germany Automotive Sector Cybercrime Threat Landscape Report

KELA 

KELA Cybercrime Intelligence ©

German Automotive Sector Cybercrime Threats Landscape Report

Yael Kishon, Threat Intelligence Analyst

Introduction

The automotive sector is considered to be the largest sector in Germany, generating over [411 billion euro](#) in revenue. Germany is the largest automobile manufacturing country in Europe, [producing](#) 30% of all passenger cars in the EU in 2021. Automotive companies, their employees and users have frequently become targets of cybercriminals aiming to perform various attacks. One of the recent examples is [an info-stealing campaign](#) that targeted customers of German companies, mainly car dealers, with phishing emails aimed to infect the victims with info-stealing malware.

Another recent cyberattack that occurred in March 2022, targeted a German subsidiary of Denso, a Japanese automotive supplier. Pandora ransomware group announced that it compromised the network and shared screenshots of purchase orders, automotive technical diagrams, and emails on its blog. Moreover, the gang claimed to have stolen 1.4 TB of data from the company. Following the attack, Denso apologized for any inconvenience caused and confirmed that the German network was illegally accessed.

With more and more vehicles connected to the internet and using many digital functions, major automotive companies are exposing cars to additional malicious activities and increasing the risk of cyberattacks.

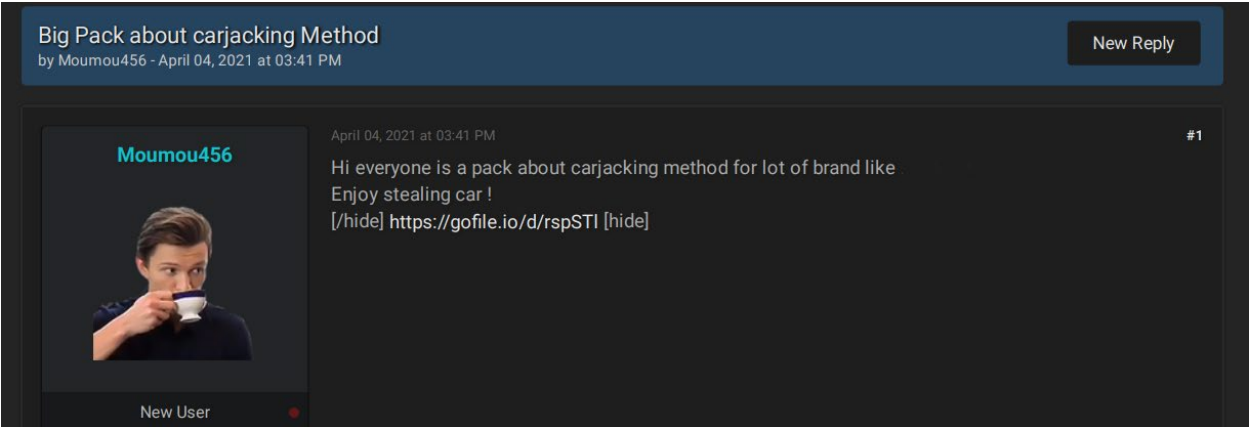
The recent cyber-attacks that have targeted the automotive industry in Germany drove KELA to investigate the level of exposure of the 15 largest German automotive manufacturers, suppliers, and dealers to shed light on cyber threats they faced from January 2021 to April 2022.

Below are the key findings of KELA in its research of cybercrime threats to Germany's automotive sector:

1. Threat actors are constantly looking for automotive hacking tools on cybercrime forums, aiming to exploit **keyless entry attacks** to steal cars. According to the General German Automobile Club e. V. (ADAC), **only 5%** of 501 tested vehicles are protected from keyless theft.
2. Sensitive data related to the automotive sector is being widely traded on cybercrime forums and markets: from **network access to automotive companies for sale** to **internal data, such as source code and databases**.
3. KELA researched **the exposure of 15 German automotive companies in cybercrime sources** and discovered that their credentials were mainly exposed in breaches not targeting the automotive sector (such as RedCappi and IndiaMart). Also, some sensitive internal services related to automotive companies were compromised (for example, enabling access to Jira and VPN accounts).
4. The data breach against **Volkswagen and Audi** in June 2021 exposed the data of 3.3 million customers and has been in high demand since then on cybercrime platforms.
5. Amidst the top targeted countries for ransomware attacks in the automotive sector, **Germany is the second most targeted victim**, following the US.

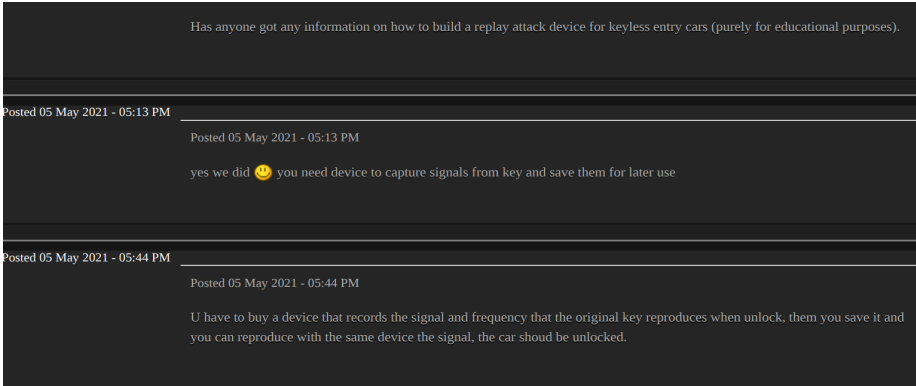
Demand for Automotive Hacking Tools

Before diving into the exposure of specific companies, KELA explored the demand for targeting the automotive industry in cybercrime sources. One of the known attack vectors affecting the automotive industry is a [keyless entry attack](#) that allows an attacker to unlock the car without relying on a physical key. For example, in November 2021, an [Audi S4 car was stolen following a keyless theft in Cambridge](#). Car hacking tools seem to be of interest among threat actors who buy and sell it on cybercrime platforms. For instance, on April 4, 2021, an actor shared a method that can be used for carjacking, claiming that it can help target different brands, among them a known German automotive manufacturer.



An actor providing a carjacking method to steal cars

A month later, on May 5, 2021, another actor was interested in a keyless entry vehicle hacking tutorial, saying that it's for educational purposes.



An actor asks to learn the keyless hacking capabilities and gets a detailed reply

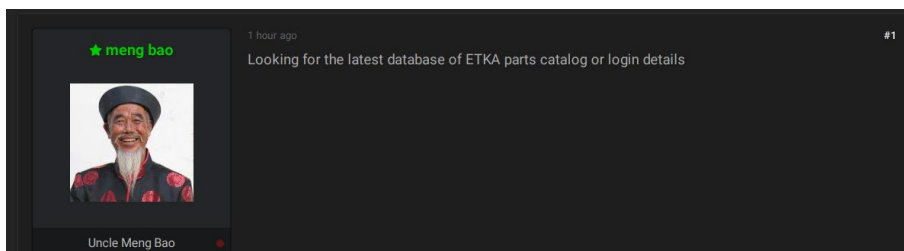
On August 28, 2021, an actor was interested in buying a keyless repeater, a device that allows opening a car remotely. The actor stated they had access to a German vehicle and were willing to pay up to 1000 euros for the device. Moreover, the actor claimed they were able to set up a fake German bank account to enable instant money transfer and complete the deal.



An actor is willing to buy a keyless repeater for unlocking a car

Interestingly, on February 10, 2022, the General German Automobile Club e. V. (ADAC) alerted that only 5% of 501 tested vehicles are protected from keyless theft. The affected cars include German brands (among others) such as Audi, BMW, Mercedes, Porsche, Opel, and Volkswagen.

In addition to hacking tools and devices, sensitive corporate information of German automotive companies is also in demand by cybercriminals on cybercrime platforms. This data can include corporate credentials, internal documents (such as financial), source code, customers' personal identifiable information (PII), and more. For example, on December 31, 2021, a threat actor was interested in buying a database of ETKA (the official electronic parts catalog for Volkswagen Group motor vehicles) or login credentials, most likely to internal resources, of the company's brands.

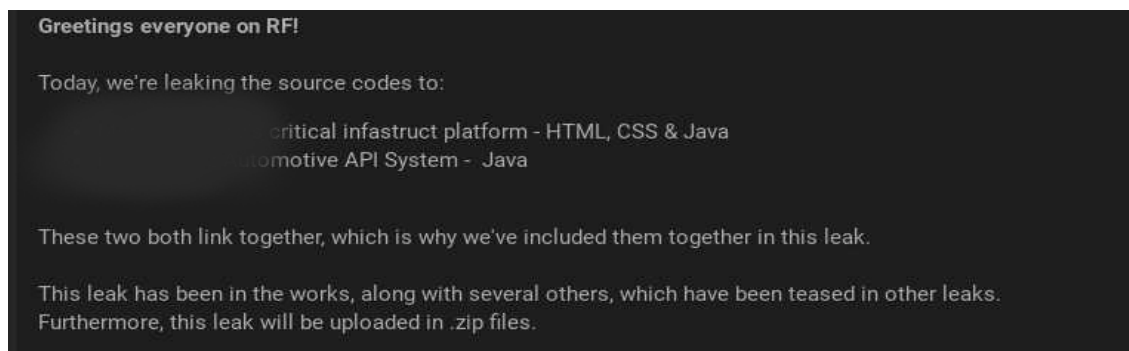


An actor is interested in an Automotive parts database

Supply of Automotive Brands' Data

Following the demand, cybercriminals were seen offering for sale different kinds of data related to the automotive sector. On October 11, 2021, a threat actor offered to sell a German automotive manufacturer database. The actor claimed that the data was divided into two parts: one with users' information and the other with private corporate data related to the car design.

A few weeks later, another threat actor leaked the source code of the same manufacturer, related to the company's critical infrastructure platform and the API system of one of the company branches.



A threat actor leaked the source code of a German automotive company on RaidForums

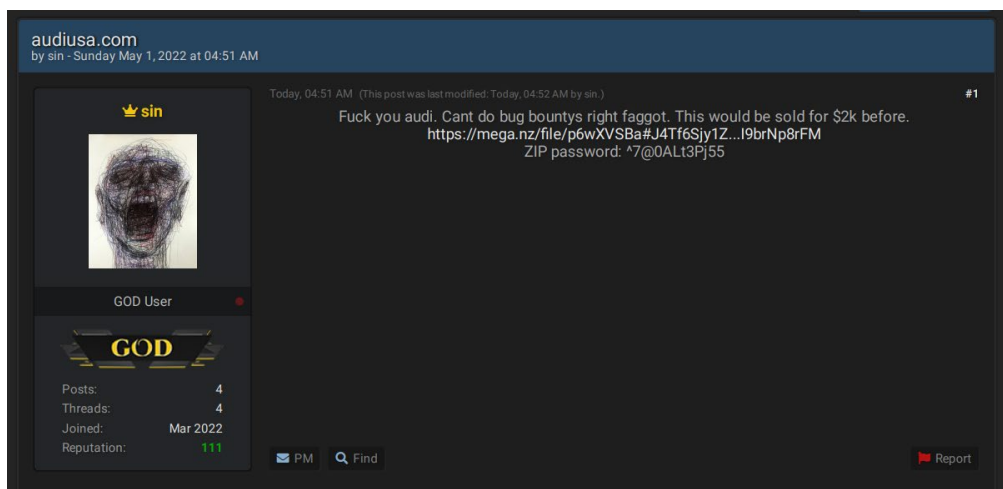
On February 12, 2022, KELA observed a threat actor offering to sell internal information about an alleged SQLi vulnerability on a German automotive manufacturing company's subdomain. The actor shared a list of seven internal databases that can be extracted following the exploitation of the vulnerability.

```
SQLi // AVAILABLE
https://en.wikipedia.org/wiki/
DB NAMES:
available databases [7]:
[*] dv2_jf3233
[*] dv_jf3233
[*] information_schema
[*] mysql
[*] opst_jf3233
[*] performance_schema
[*] tbl_jf3233
```

20:09

A threat actor sells an SQLi vulnerability on a Telegram channel

One of the recent examples is a threat actor sharing a database of Audi USA in May 2022. Based on KELA's research, the leak exposed approximately 2.7 million unique records, including customers' email addresses, names, phone numbers, physical addresses, driver details and vehicle information.



A threat actor shared Audi USA database, accusing the company for not having bug bounty program

[Initial Access Brokers](#) (the actors who attempt to gain access to compromised networks and sell it to other users giving them the chance to perform various attacks, from espionage to deploying ransomware) were also seen targeting automotive companies. One of the most valuable offers was made on May 8, 2022, when KELA observed the threat actor apollo12 selling access to a Germany-based automotive parts manufacturer with USD 2 Billion in revenue. The actor claimed the access is provided through Citrix. Based on the chatter, the access was most likely sold on the same day by the actor focusing on buying network access to large companies from all over the world.

Observing these demand and supply which pose an immediate risk to automotive manufacturers, suppliers and dealers, KELA compiled a list of the top 15 German automotive makers, suppliers, and dealers and explored the exposure of their corporate credentials.

Leaked Credentials and Top Breaches

Leaked credentials

Leaked credentials are email logins to different third-party platforms (with or without passwords) that are usually leaked or sold by threat actors on underground forums in the form of databases to enable various malicious activities.

KELA researched domains associated with Germany's top automotive companies, including manufacturers, suppliers and dealers. The focus was on the exposure of the assets related to the German companies and not to all subsidiaries and other business forms of German automotive companies worldwide. For large manufacturers, the research included global (.com) and local (.de) domains. The analysis was performed on data obtained from January 2021 to April 2022.

For the given domains, KELA discovered over 5000 leaked credentials appearances that have been exposed via third-party breaches and posted in cybercrime sources, of which close to 4800 were identified as unique. The credentials included several email addresses of senior management as well as a former CEO.

It seems that there is no correlation between the number of employees and the number of leaked credentials — for each company, regardless of its size, around 1% or less was exposed on the cybercrime underground. For example, one of the top automotive brands that ranked as the most targeted company based on KELA analysis, with more than 170,000 employees, suffered a relatively small data leakage, with only 1% (2179) credentials exposed on the cybercrime underground.

Only 1% of the total amount of credentials leaked per researched companies included passwords presented as plain text in a readable format. It means they can be easily used for unauthorized access. 21% had different types of passwords. Although the rest of the credentials (78%) did not include passwords, they could still be exploited by cybercriminals for phishing campaigns, targeted of brute-force attacks, and other illegal activities.

Top breaches

Below are the top 3 data breaches, containing around 60% of the credentials leaked during the research period:

6. RedCappi

RedCappi is an email marketing service based in the US. The majority of the credentials (27%) were leaked in the RedCappi data breach, which occurred in December 2021. The leak exposed over 177 million records, including names, email addresses, phone numbers, physical addresses, occupations, and more.

7. IndiaMART

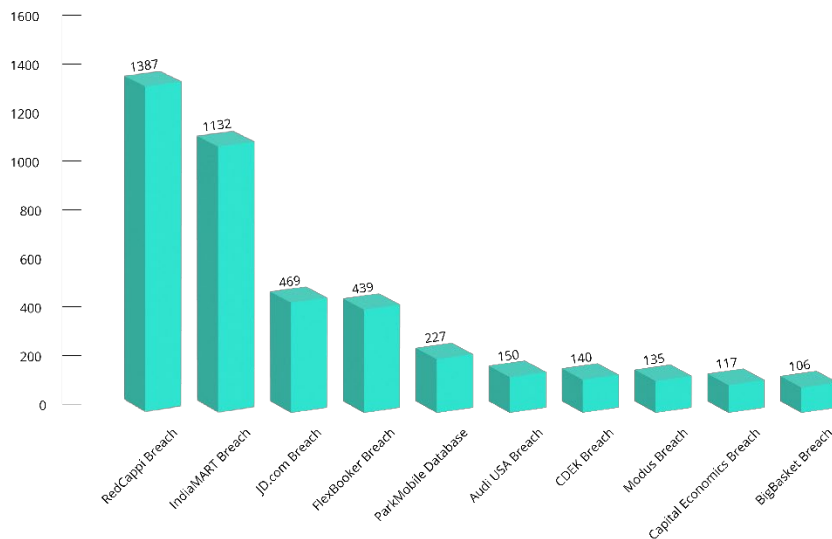
Another breach that led to the exposure of many credentials (22%) is related to IndiaMART. IndiaMART is an online B2B marketplace based in India, connecting buyers with suppliers. The threat actor shared a database containing 38 million records with 20 million unique email addresses, company names, physical addresses, countries, and mobile numbers.

8. JD

The JD data breach contains 9% of all exposed credentials. In April 2021, a threat actor shared the database of a popular Chinese shopping platform named JD.com, which was originally breached in 2013. The data leak exposed approximately 90 million emails, and included email addresses, names, phone numbers, usernames, and hashed passwords.

The breaches that exposed most of the credentials are unrelated to the automotive industry nor to German companies. That emphasizes the importance of tracking the exposure of third-party vendors and educating employees not to use corporate emails on non-corporate resources. Otherwise, sensitive information can be leaked by third parties and, if not tracked timely, used by cybercriminals for further attacks against those companies.

Breach sources of leaked credentials



Top 10 breaches exposing the largest amount of credentials from January 1, 2021 to April 30, 2022

While most of the credentials of the researched companies were exposed via breaches affecting a wide range of industries, a small percentage (2%) was leaked as part of data breaches pertaining to the automotive industry. For example, on June 11, 2021, it was [reported](#) that Volkswagen Group suffered a data breach, exposing 3.3 million customers' data, 97% of those affected were related to customers and interested buyers of Audi, which is owned by Volkswagen group. The data breach occurred due to a third-party vendor used by Audi, Volkswagen and some authorized dealers in the US and Canada leaving data in an unsecured file.

Based on Volkswagen's statement, the company [was alerted](#) that "an unauthorized third-party" may have accessed this information on March 10, 2021. The company claimed that the data breach impacted 3.3 million customers, but only 90,000 of the records included sensitive information of Audi's customers, such as driver's license numbers and social security numbers.

Four days after the data breach disclosure, the data started to circulate on cybercrime platforms and has been in high demand since then. Even recently, on April 23, 2022, an actor was interested in buying the Audi US database.

SELLING audiusa.com 2019 5m
by 000 - June 15, 2021 at 02:42 AM

June 15, 2021 at 02:42 AM · This post was last modified: June 17, 2021 at 03:12 PM by 000 · Edited 4 times in total · #1

I'm back from my break and got some leaks init fam

Shoutout @[badhou3a](#) for helping

<https://www.zdnet.com/article/volkswagen...ed-buyers/>
<https://www.vice.com/en/article/xgxaq4/h...volkswagen>


Audiusa.com Analytics Dump
 Has VINS Emails Names and more
 2 Files & Backup

Leads.csv
 Lines: 3,862,231
 Sample: <https://skidbin.net/paste?t=Pbl8llmn>
 Sample with numbers: <https://skidbin.net/paste?t=J2T48ixB>
 Data: Created,FirstName,LastName,Address1,Address2,City,State,ZipCode,HomePhone,EmailAddress & more

Sale.csv
 Lines: 1,792,278
 Sample: <https://skidbin.net/paste?t=lcYZArWo>

Data

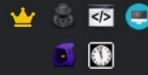
000



30 mg

Posts 830
 Threads 65
 Joined Nov 2017
 Reputation 2,143

3 YEARS OF SERVICE




A threat actor selling the Audi database in June 2021

LOOKING FOR AUDI USA DATABASE
by hellokitty - Sunday April 24, 2022 at 03:47 AM

11 hours ago · #1

Looking to buy the Audi USA database - as described on HavelBeenPwned. I know it was for sale on RF (RIP), so maybe the same dude is on this site now and is still willing to sell it. Or, maybe someone else has it and is willing to sell it. LMK in PMs. Middleman will be used, so don't try to scam and say you have it.

hellokitty



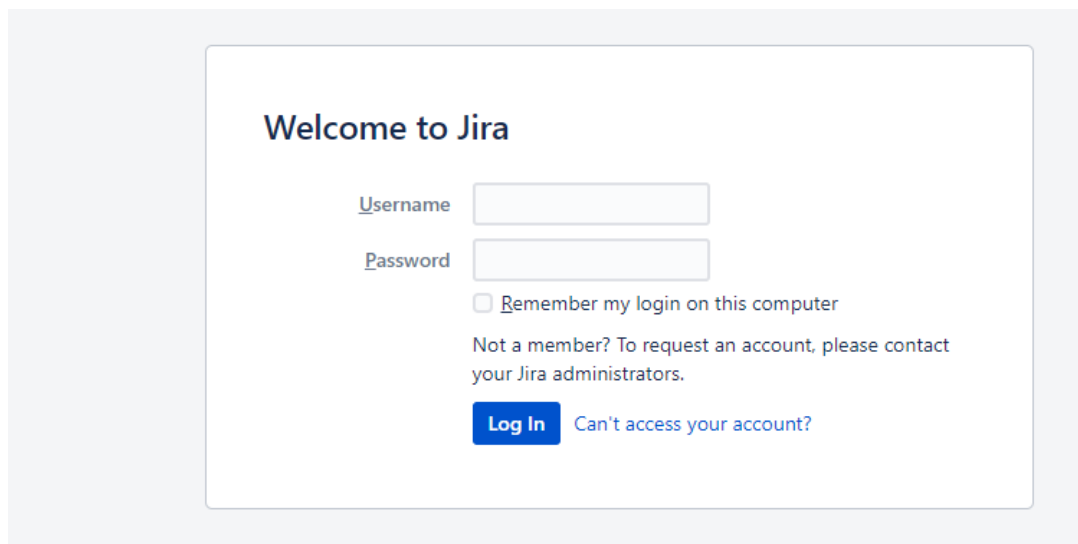
An actor is willing to buy the Audi US database

Compromised Accounts

KELA performed a similar analysis of compromised accounts belonging to top German automotive companies. From January 2021 to the end of April 2022, KELA identified over **5600** compromised accounts listed on different botnet markets.

Those botnet markets sell access to data from machines (PCs, laptops, smartphones) infected with information-stealing trojans. These machines contain saved credentials and personal information belonging to either employees, clients, or partners. Therefore, compromised accounts that are purchased by threat actors can put organizations at serious risk. KELA monitored various botnet market sources and discovered several compromised portals associated with the given domains.

Among these compromised portals and services, KELA detected sensitive corporate resources, such as an internal collaboration platform; the stolen credentials, if bought, would enable to log in to a Jira account of one of the automotive companies, as seen on the screenshot below:



Login page to Jira's account that can be accessed via credentials found on the TwoEasy botnet market

Accessing the company's Jira account would allow the attacker to access important business information, including new releases or source code, and can also expose sensitive information about suppliers, partners, and customers.

Another example of a potentially highly dangerous compromised resource is an internal email service related to one of the given domains, as seen in the screenshot below:

Login

Email address

Password [Forgot password?](#)

Log in

[Request public key](#)

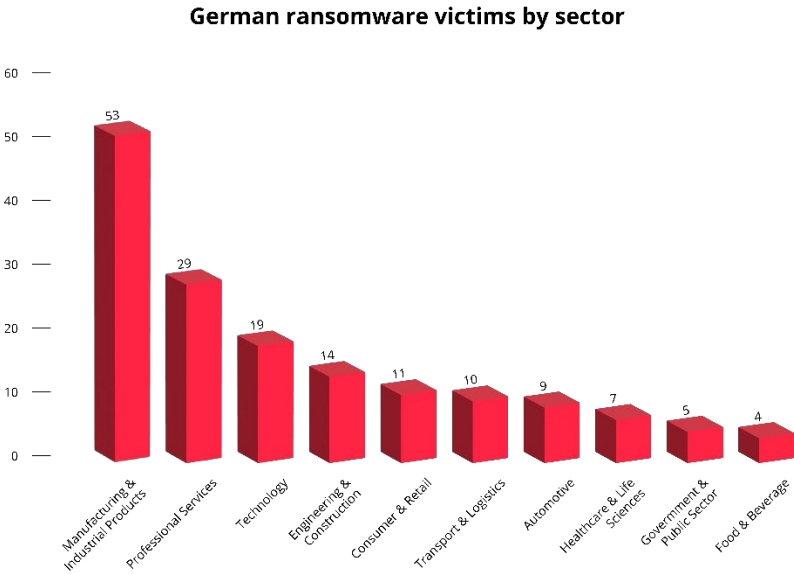
A mail service that could be accessed via credentials found on the Genesis botnet marker

These credentials, if bought, can provide the attacker with visibility into corporate information and an opportunity to launch phishing campaigns, BEC attacks, and more.

KELA also found several bots containing credentials to virtual private networks (VPN) – these accounts enable the buyers to log in to Citrix SSL VPN and FortiClient VPN web portals of several automotive companies. Typically, a VPN provides employees with access to the company’s internal resources. Unauthorized access would provide an entry point to the corporate’s internal network and the ability to compromise it further for malicious purposes.

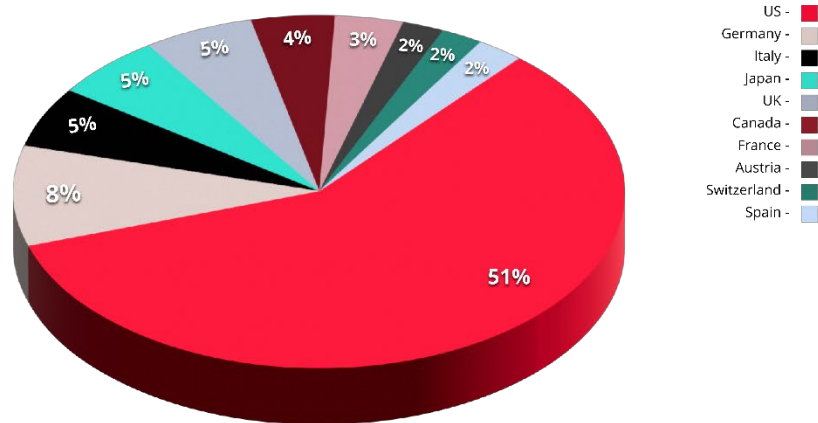
Ransomware Incidents

One of the possible outcomes of leaked credentials, compromised accounts, or other data exposed in cybercrime sources is a ransomware attack. KELA observed at least **179 ransomware attacks** targeting German companies from January 1, 2021 to April 30, 2022. This number derives from the chatter in ransomware gangs' blogs and negotiation portals, suggesting that the actual number of attacks can be higher. However, it is a sufficient number of victims to enable the identification of patterns in targeted companies and industries in Germany, which mostly follow the same patterns of the [top targeted industries by ransomware in 2021](#). Looking at all sectors, Germany is only fifth among the top targeted countries after the US, the UK, Canada, and France. But when looking closer at the automotive sector, Germany comes second after the US in the most targeted countries.



German ransomware victims by sector from January 2021 to April 2022

Top 10 targeted countries in the Automotive sector



In the research period, several German automotive manufacturers fell victim to ransomware attacks. For example, Edag, a service provider for the automotive industry, [confirmed](#) that it was a victim of a ransomware attack that occurred on March 13, 2021. A few days after their statement, on March 18, 2021, Clop operators took responsibility for the attack, claiming to have compromised Edag. Additionally, the operators published screenshots of "proof-of-breach" documents that included employees' contracts and passports.

On October 24, 2021, Eberspächer Group, a German car supplier, confirmed it was hit by a cyber-attack, which [affected](#) the company's IT infrastructure. As a result, the company was forced [to send part of its workforce home](#) on paid leave for the repair period. On November 16, 2021, the operators of Conti ransomware took responsibility for the attack. On November 29, 2022, Eberspächer Group [posted](#) that the website was back online, over a month after the attack. KELA observed that the Conti gang did not leak the data on their blog, but it is not clear if the company paid the ransom or not.

APTs targeting German companies

The cybercrime landscape includes different types of threat actors, not only financial-driven but also having different motivations, from ideological to political goals. For example, APTs — Advanced Persistent Threats — refer to a nation-state or a sophisticated, professional criminal organization that aims to launch cyber espionage, mainly against government agencies, and extract sensitive information over time.

Germany was targeted by different APT groups in 2021, with the country's automotive sector specifically being attacked in 2019 by APT32, also known as Ocean Lotus. The group is associated with the Vietnamese government and has been active since 2014. In 2019, it [was reported](#) that the group carried out a cyber-attack against BMW using a penetration testing tool named Cobalt Strike as a backdoor into the compromised network.

Conclusion

The German automotive sector is one of the leading sectors in Germany. It is constantly adopting digital and automation technologies, and therefore becoming a valuable target for various cyber criminals, from ransomware gangs to nation-state actors. Automotive manufacturers must ensure their supply chain is protected by monitoring and tracking their TIER1 and TIER2 third-party vendors. In the coming years, we expect more and more smart-connected vehicle manufacturing, making it a valuable target for cybercriminals. It is, therefore, crucial to follow high standards of cybersecurity, not only to prevent cyber threats but also to save human lives.

[**ACCESS KELA'S PLATFORM FREE TO AUTOMATICALLY EXPOSE RISKS TO YOUR ORGANIZATION**](#)