SOCRadar®
Your Eyes Beyond

GERMANY THREAT LANDSCAPE REPORT 2023

A Threat Intelligence Analysis of Germany in the context of emerging Dark web threats

socradar.io

Table of Contents

Executive Summary

Germany is the world's fourth-largest economy, following the United States, China, and Japan, and holds the distinction of being the largest economy in Europe. It is also the world's third-largest exporter. Though the country is renowned for its heavy industry and manufacturing, the service sector contributes the most to its GDP(Gross Domestic Product) , making up 70%. Additionally, Germany plays a significant role in European politics and has been the target of various forms of attacks, including cyber espionage, from multiple threat actors. Organizations in both the public and private sectors, particularly those involved in geopolitically significant projects, remain key targets for such attacks.

Tensions like the Russia-Ukraine crisis have led to an increase in cyber-attacks on countries that are opposed to Russia. According to a cyber threat analysis report published by Thales in March 2023, the percentage of cyber-attacks targeting European Union (EU) countries rose from 9.8% to 46.5% in the six months following the onset of the Russia-Ukraine crisis. This increase is directly related to the conflict; 61% of recorded global attacks over the course of a year originated from Russia, primarily targeting countries that support Kyiv.

These threats also present significant risks to German organizations. Germany's technological advancement, economic power, and pivotal role in European and global politics make it an attractive target for state-sponsored cyber actors, known as Advanced Persistent Threats (APTs), as well as financially motivated threat actors from countries like Russia, China, and Iran.

A cyber threat actor can be an individual or group that poses a threat to cybersecurity. These actors can be state-sponsored or act as professional entities, commonly referred to as APTs. They typically operate in anonymity, frequenting hidden corners of the internet known as the "dark web" which search engines do not index. In these dark web environments, often called the "underground" they communicate through forums and channels, exchanging and selling a range of technical tools, malware, and information acquired from data breaches. This highlights the importance of cyber threat intelligence. Knowing who owns your data can influence your responsive actions. Even more crucial is identifying software vulnerabilities that are exploited by these actors. Gaining insights about the threat actors' preparation phase, their profiles, and their tactics, techniques, and procedures (TTPs) are essential security measures.

SOCRadar combines open-source and dark web intelligence to provide reliable and actionable information. It alerts you to potential cyber incidents that could escalate and offers solutions. Security analysts at SOCRadar analyzed intelligence data from September 2022 to September 2023, which was gathered by monitoring underground forums and channels used by threat actors 24/7. The findings are presented in the Germany Threat Landscape Report 2023. The report aims to assist decision-making processes for organizations in both the public and private sectors, providing insights on how to manage and reduce cybersecurity risks and improve your security posture.

KEY FINDINGS

SOCRadar security analysts detected and analyzed over 330 dark web incidents (excluding ransomware) associated with organizations based in Germany between September 1, 2022, and September 1, 2023. They reached the following key conclusions:

- Based on the data analyzed over one year, the industries most affected by these threats are Finance, Insurance, Commercial Banking, E-commerce (specifically Electronic Shopping and Mail-Order Houses), Information Services, Telecommunications, Retail Trade, and other sectors.

- The prominent industries included in the "Other sectors" category that are affected by cyber incidents are Accommodation, Food Manufacturing, Transportation and Warehousing, and Commodity Contracts Intermediation (including the Cryptocurrency & NFT Market).

- More than 30 industries and sub-sectors have been targeted by these cyber threats. This is significant evidence that the attack surface of internet services is expanding, vulnerabilities are increasing, and malicious actors are capitalizing on this by adopting a strategy of sectoral expansion.

- Within a one-year timeframe, 152 ransomware attacks were carried out by 26 different ransomware groups targeting organizations in Germany. According to the number of victims, the most successful ransomware actors were LockBit 3.0 (with 32 victims), BlackBasta (29), Cl0p (18), Play (12), Royal (12), and AlphVM Blackcat (11).

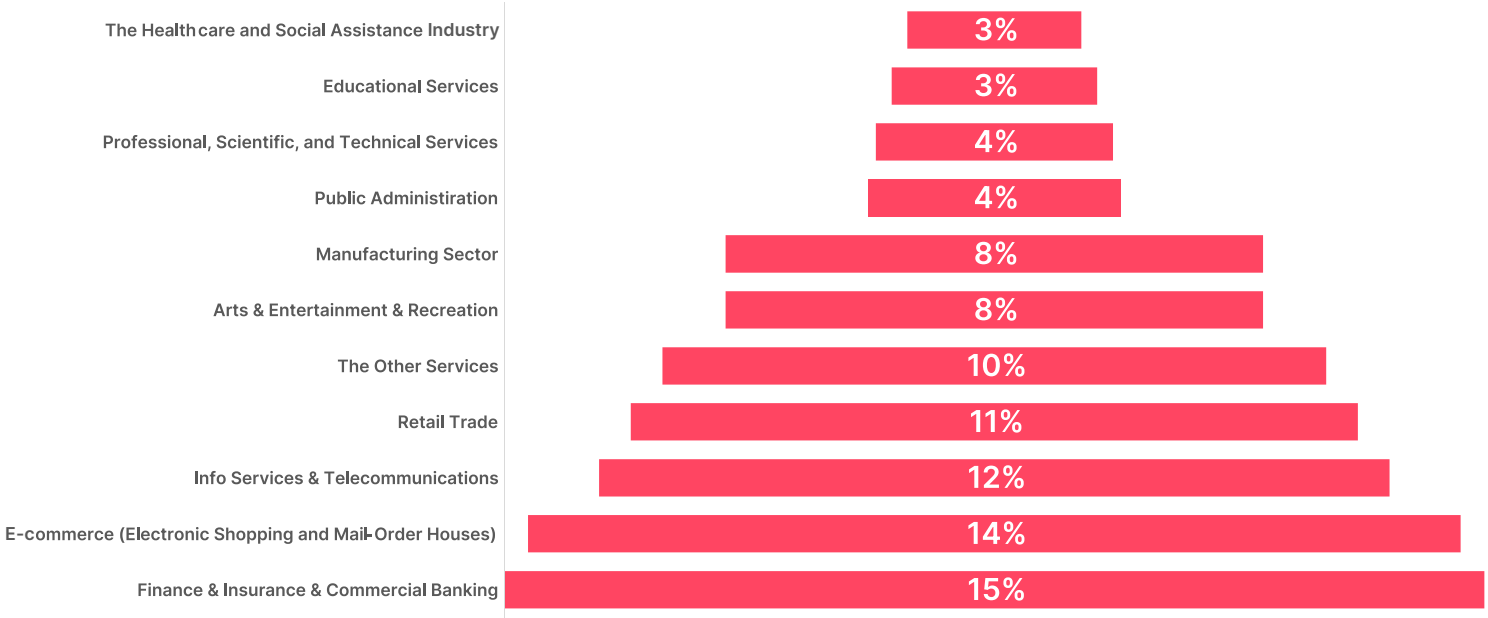
- The main industries most vulnerable to ransomware attacks, based on the number of incidents, are Manufacturing (with 46 incidents), Professional, Scientific, and Technical Services (18), Information Service (13), and Retail Trade (13).

- According to SOCRadar's observations, the Advanced Persistent Threat (APT) groups targeting organizations in Germany include Ice Fog, Turla Group, TA866, and Charming Kitten (also known as APT35) and Killnet is notorious for its DDoS attacks targeting NATO countries.

Spotlight on: Dark Web Threats Targeting Industries in Germany

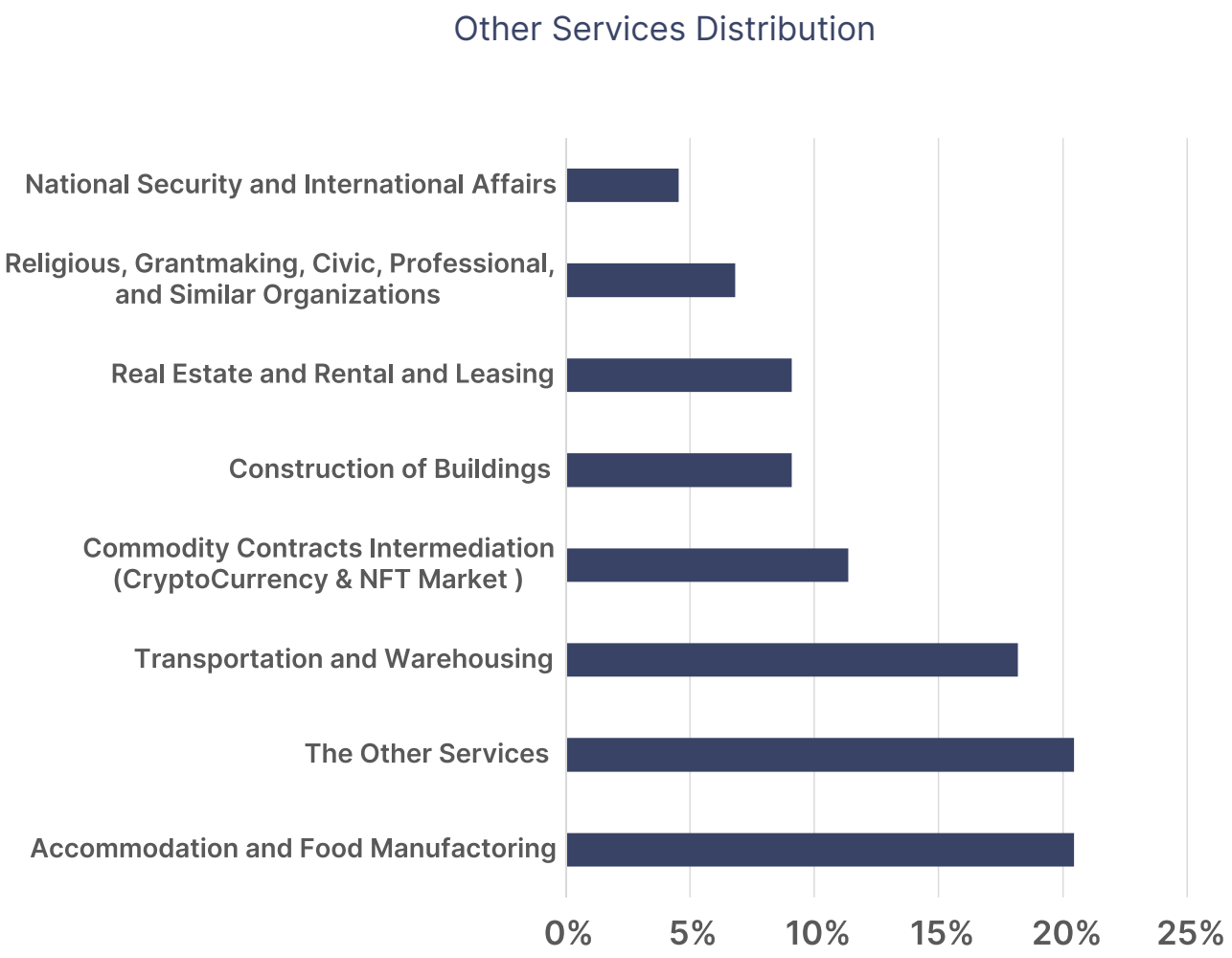
Within the last one-year period, more than 330 cyber incidents, mostly data breaches, targeting organizations both private and public sectors in Germany were detected and the distribution of these incidents by industries is given below. More than 30 sectors and sub-sectors were affected by these cyber incidents. This points to the expansion of attack surfaces and the diffusion policies of threat actors, thus clearly showing that the number of victims is increasing.

Cyber Incidents by Industries



Spotlight on: Dark Web Threats Targeting Industries in Germany

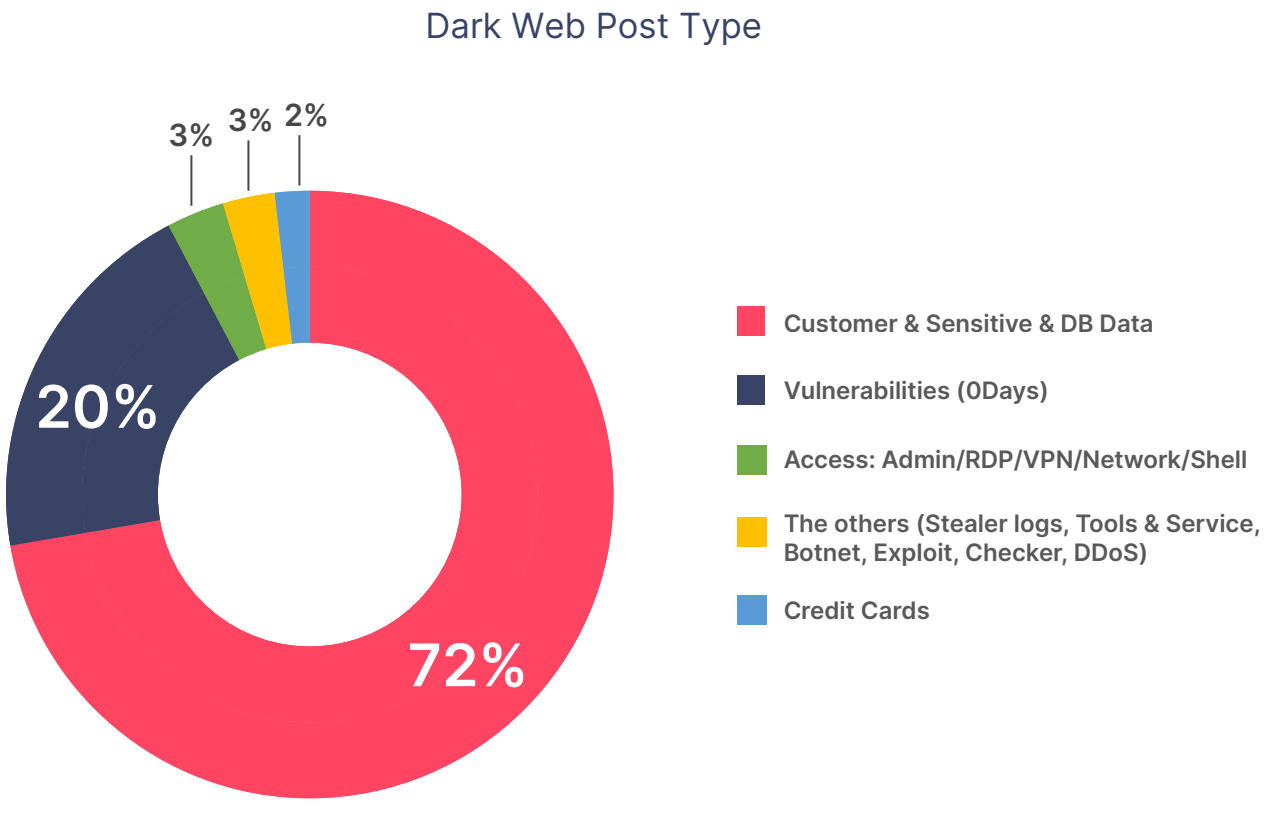
The breakdown by sector and sub-sector in the "Other services" category, which covers 10% of the 5th place among the sectors targeted by threat actors, is also shown below. As stated in the Verizon Data Breach Investigation Report, the importance of these exposed data becomes apparent when we consider that confirmed data breaches account for approximately 10 percent of the actual percentage. Without monitoring hacker forums and channels, where the measures taken against cyber threats detected only on the clear web are not sufficient, it is not possible to determine exactly which kind of data at risk from each organization.



Spotlight on: Dark Web Threats Targeting Industries in Germany

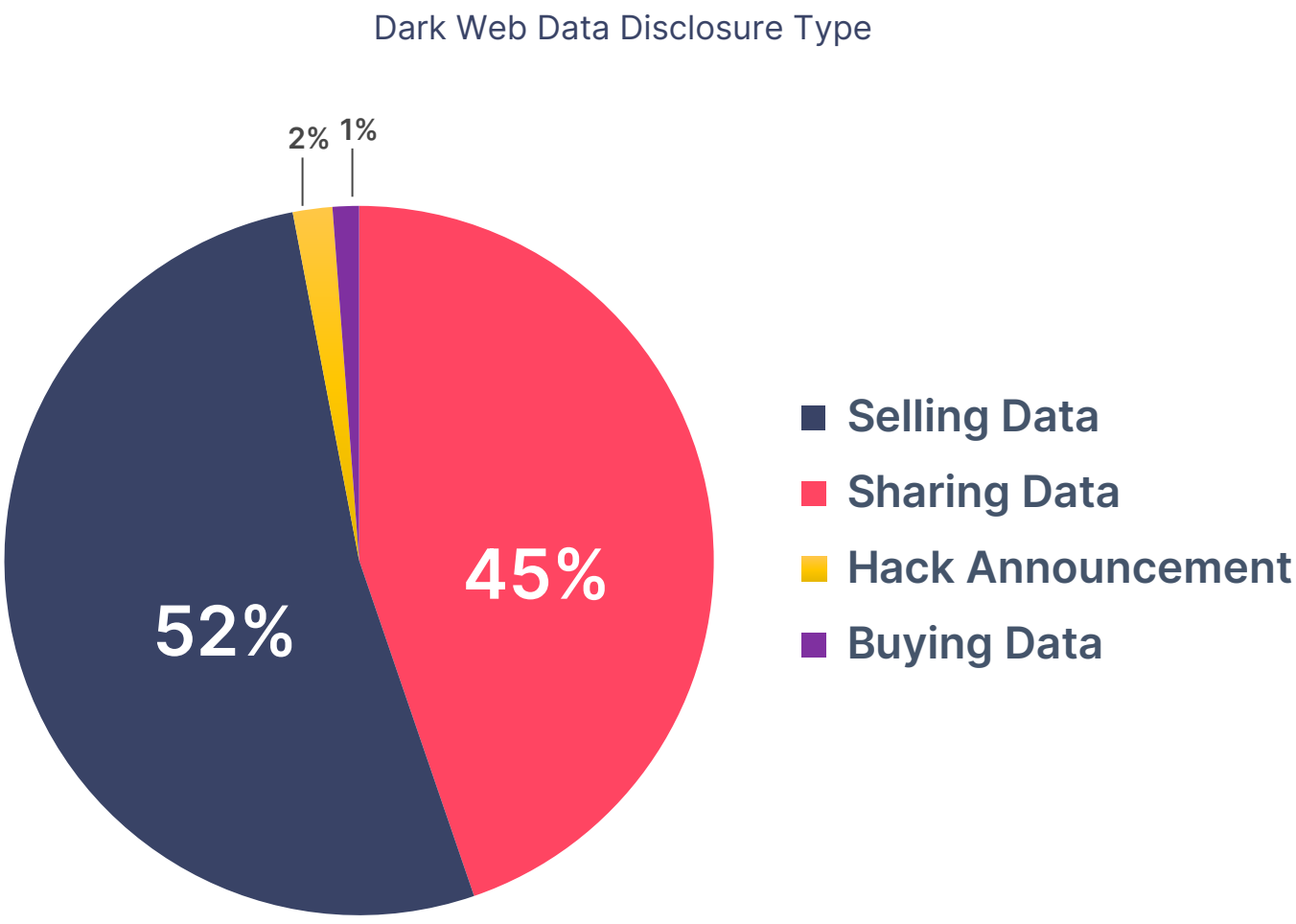
Unauthorized and illegal access to both personal and corporate data has unfortunately become an accepted risk, with a high likelihood of data leakage. According to SOCRadar's analysis, 72% of the breached data includes sensitive information like customer details. Information related to Admin, RDP, VPN, Network, and Shell access, which is crucial for initial cyber-attack stages, comprises 20% of the breached data. According to insights from SOCRadar research analysts, there has been a significant increase in the sale of these access credentials. This emphasizes that dark web activities include not just compromised data, but also critical information sold for potential future cyber-attacks.

In fifth place, accounting for 2% of the incidents is the sale and sharing of vulnerabilities commonly exploited by threat actors, such as zero-day and SQL injection flaws. As evidenced by the MOVEit incident, which has been a topic of concern for months, zero-day vulnerabilities can pose a threat to a broad range of companies when found in widely used software. As of September 2023, over 1,100 victim organizations and more than 50 million people have been affected by the exploitation of MOVEit vulnerabilities by the Cl0p ransomware group, also known as TA505. Currently, 37 German organizations have been affected by the MOVEit breach.



Spotlight on: Dark Web Threats Targeting Industries in Germany

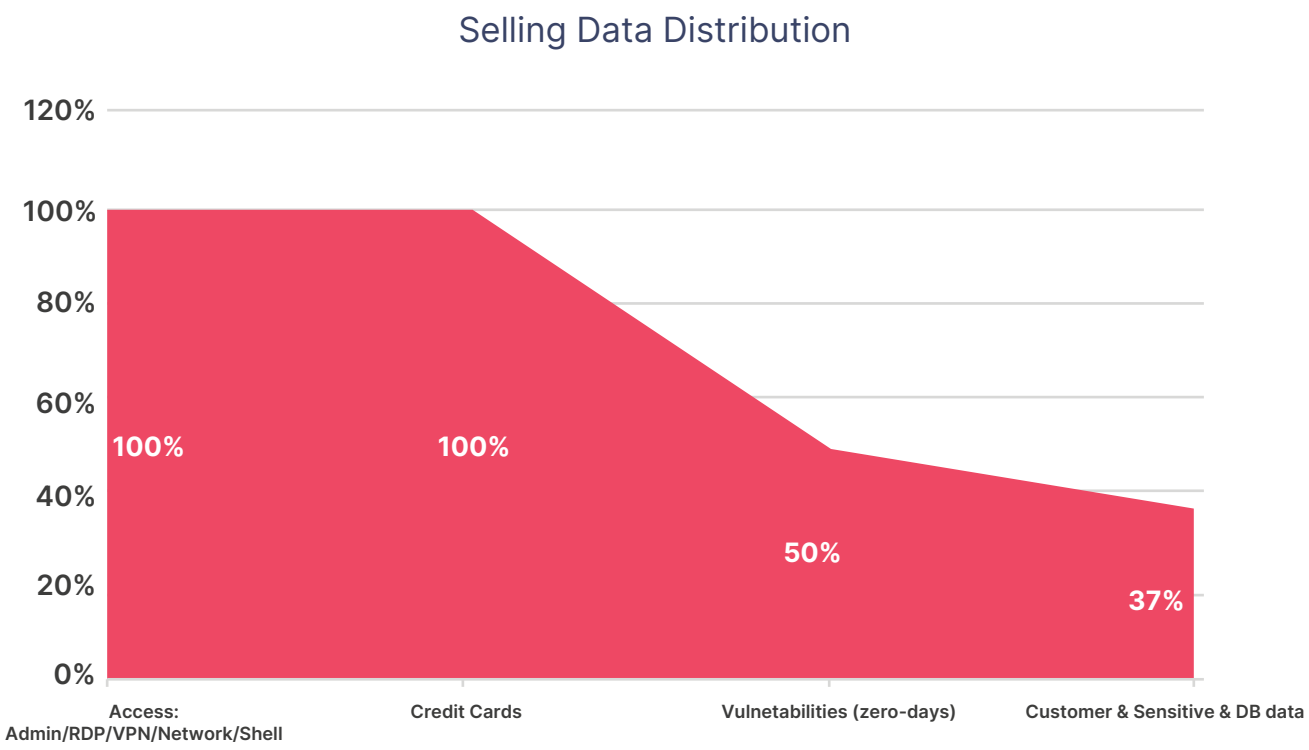
The distribution of data in dark web posts according to types of disclosure is presented below. The fact that more than half of the posts (52%) involve the sale of data indicates a trend among threat actors to not only share data but also to monetize it quickly.



Spotlight on: Dark Web Threats Targeting Industries in Germany

Additionally, the majority of the shared data comprises personal, commercial, and sensitive information resulting from data breaches. This includes data from organizations that have not paid ransoms, a tactic known as the double extortion method, which ransomware groups have increasingly used recently.

The proportional distribution of data types offered for sale is also detailed below. It was observed that all access and credit card information (100%), half of the vulnerabilities, such as zero-days (50%), and 37% of the data containing personal and sensitive information were put up for sale.



Recent Dark Web Activities Targeting Entities in Germany

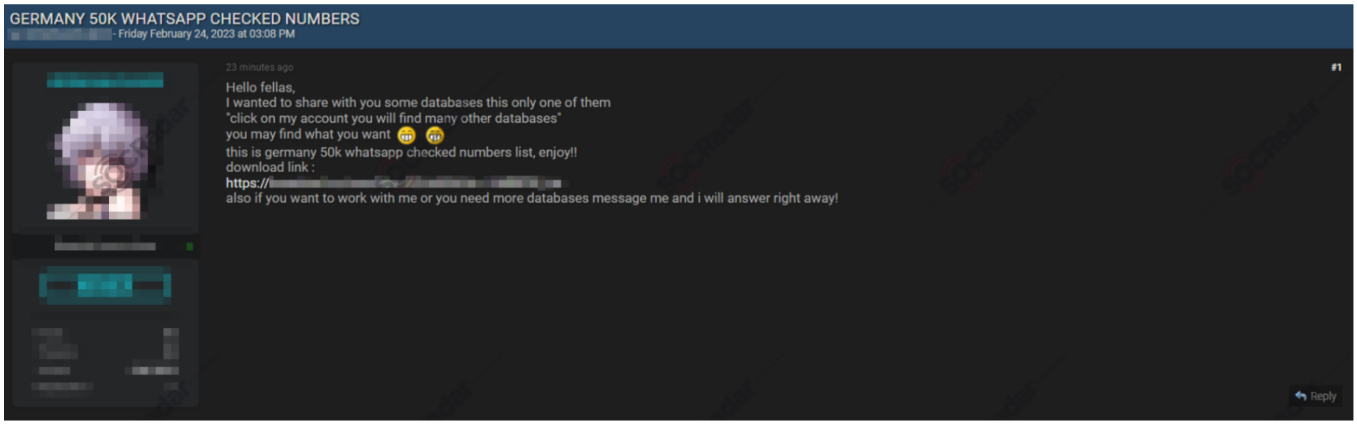
In 2023, SOCRadar's Dark Web team detected and identified some of the most prominent dark web cybercrime activities targeting German entities. These incidents are described in chronological order, based on the type of postings found on underground forums.

Customer & Sensitive & DB data

On January 19, 2023, a new alleged database leak was detected for the German Institute for Global and Area Studies (www.giga-hamburg.de) in a hacker forum monitored by SOCRadar. GIGA is a German research institute that analyzes political, economic, and social developments in Africa, Asia, Latin America, and the Middle East. It also conducts comparative research on international relations, development, globalization, violence, and security.

GIGA database sale in a hacker forum

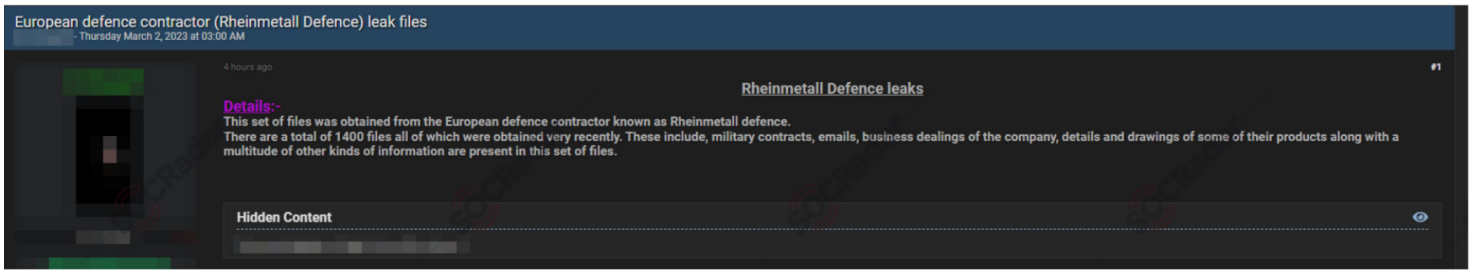
On February 24, 2023, a new alleged database leak affecting German WhatsApp users was detected. The leaked data contains a list of 50,000 verified WhatsApp numbers.



German WhatsApp users leak in the hacker forum

Recent Dark Web Activities Targeting Entities in Germany

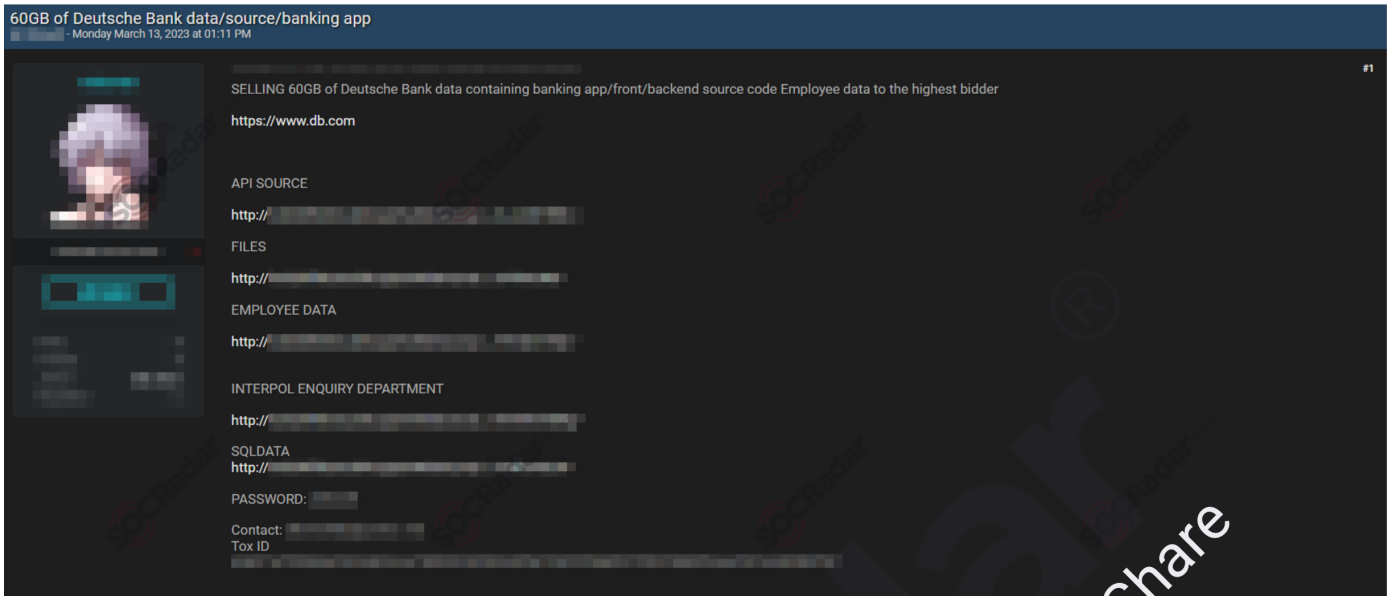
On March 2, 2023, a new alleged leak of sensitive documents was discovered for Rheinmetall AG, a German automotive and arms manufacturer headquartered in Düsseldorf. The leak reportedly contains 1,400 files, including military contracts, e-mails, business dealings, and detailed product information.



Rheinmetall AG sensitive information leak in hacker forum

Furthermore, Rheinmetall AG was announced as a new ransomware victim **on May 20, 2023,** according to the Black Basta ransomware group's website, also monitored by SOCRadar. Given that this ransomware attack occurred after the database leak, it is concluded that most companies have been hacked more than once.

On March 13, 2023, another alleged sensitive data leak was detected for Deutsche Bank. The data, offered for sale to the highest bidder, contains 60GB of information, including banking application source code, employee data, Interpol Enquiry Department details, SQL data, and passwords.



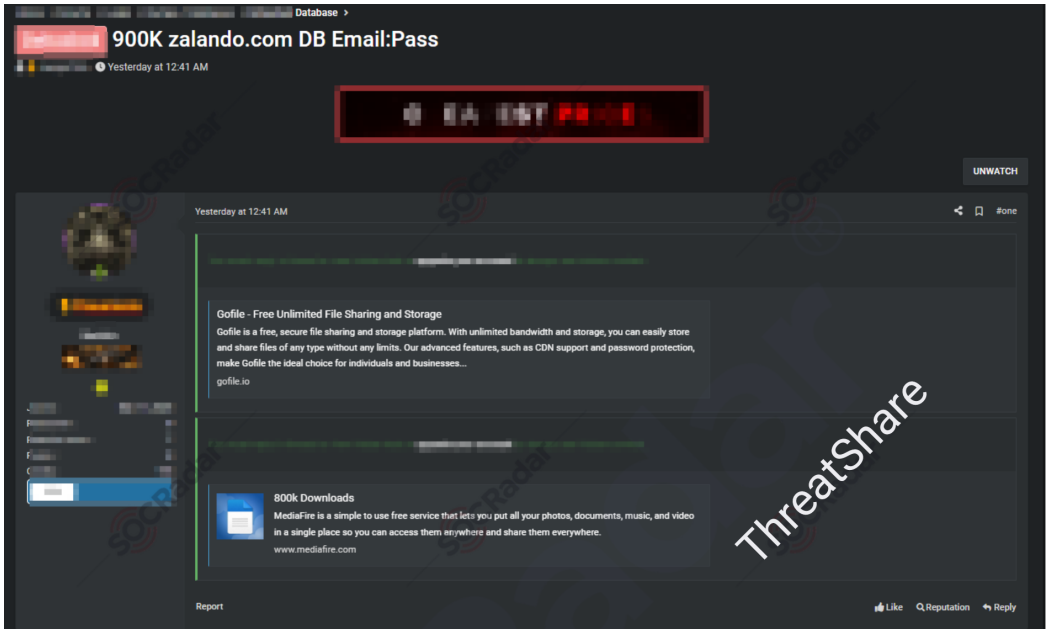
Deutsche Bank sensitive information leak in the hacker forum

Recent Dark Web Activities Targeting Entities in Germany

On March 18, 2023, in a hacker forum monitored by SOCRadar, a new alleged customer database sale was detected for Deutsche Telekom. The data leak is from November 2022. Details of Deutsche Telekom's 27.3 million German customers in the data including name, last name, home address, and phone number. Deutsche Telekom AG is a German telecommunications company headquartered in Bonn and is the largest telecommunications provider in Europe by revenue.

Deutsche Telekom database sale in the hacker forum

On March 22, 2023, in a hacker forum monitored by SOCRadar, a new alleged database leak was detected for Zalando. Zalando SE is a publicly traded German online retailer of shoes, fashion and beauty active across Europe that has more than 51 million active users in 25 European markets.

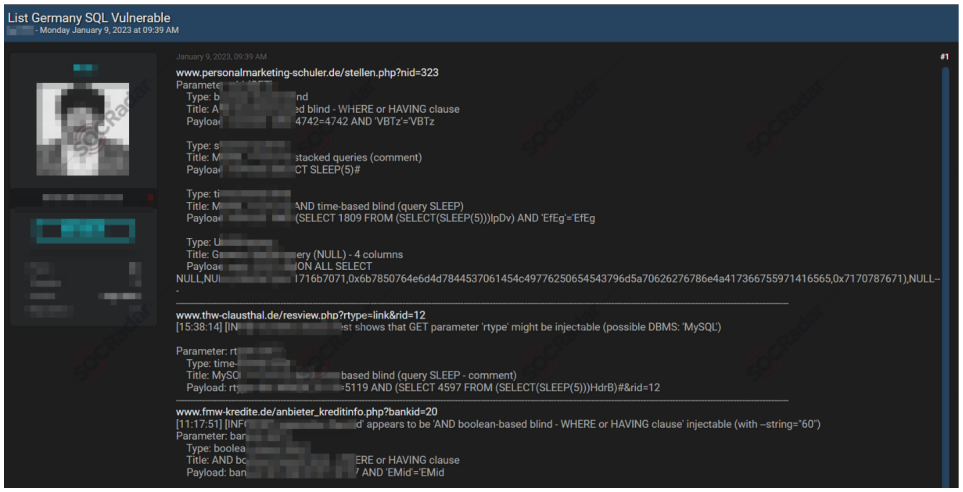


Zalando database sale in the hacker forum

Recent Dark Web Activities Targeting Entities in Germany

Software Vulnerabilities (Zero-Days, SQL Injection vulnerabilities and, etc.)

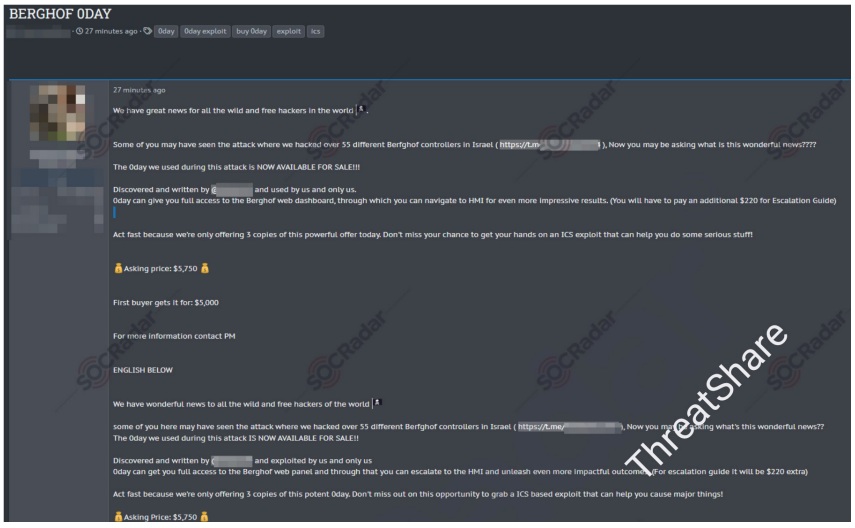
On January 9, 2023, in a hacker forum monitored by SOCRadar, a new alleged SQL Injection vulnerability was detected for many German websites. A SQL injection attack consists of "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database and modify database data.



SQL injection vulnerabilities found on many German websites in the hacker forum

On May 27, 2023, in a hacker forum monitored by SOCRadar, the sale of a new zero-day exploit was detected for Berghof Automation. Berghof Automation GmbH manufactures factory automation equipment. The Company offers automated production systems for chemical, logistics, heavy duty product, and mechanical engineering industries that serve customers worldwide.

The threat actor cited an attack in Israel where they hacked more than 55 different Berghof controllers and offered the 0-day vulnerability for sale at $5,750. For an additional $220, buyers could gain full access to the Berghof web control panel for access to the Escalation Guide.



Berghof Automation GmbH zero-day vulnerability in the hacker forum

Recent Dark Web Activities Targeting Entities in Germany

Access: Admin/RDP/VPN/Network/Shell

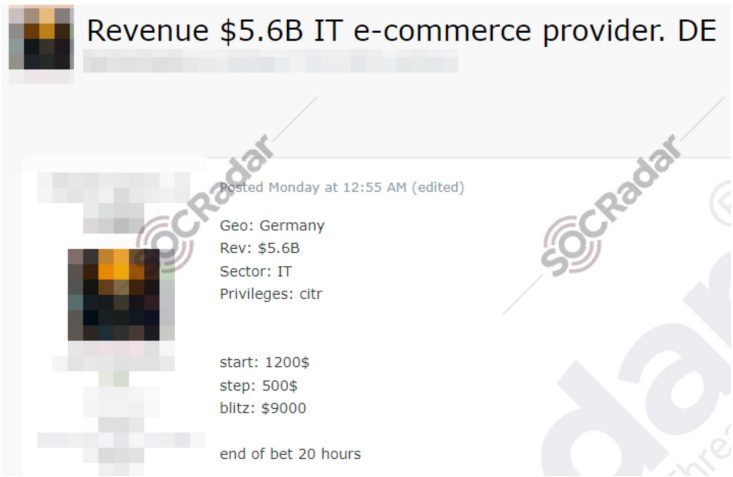
On February 20, 2023, in a hacker forum monitored by SOCRadar, an unauthorized VPN access was offered for sale, allegedly belonging to a German manufacturing company. The company, operating in the Industrial Electronics Manufacturing sector with 20,000 employees and a claimed revenue of $5.5 billion, had its VPN entry point user rights auctioned starting at $1,500.

Unauthorized VPN access found at German Manufacturing company in the hacker forum

On April 30, 2023, in a hacker forum monitored by SOCRadar, an unauthorized admin access sale was detected that allegedly belongs to an electric company that operates in Germany. It is claimed that the VPN + local admin authorizations of the company, which provides commercial services in Germany for electrical installation and steel companies, concrete construction manufacturers, are being auctioned starting from 499 dollars.

Unauthorized Admin access found at German Electric company in the hacker forum

On June 26, 2023, in a hacker forum monitored by SOCRadar, an unauthorized network access sale was detected that allegedly belongs to an e-commerce company that operates in Germany. It is understood that the company, whose domain admin privileges is also auctioned for sale at a price starting from $1,200, is an e-commerce giant operating in the IT sector with a revenue of $5.6 billion.

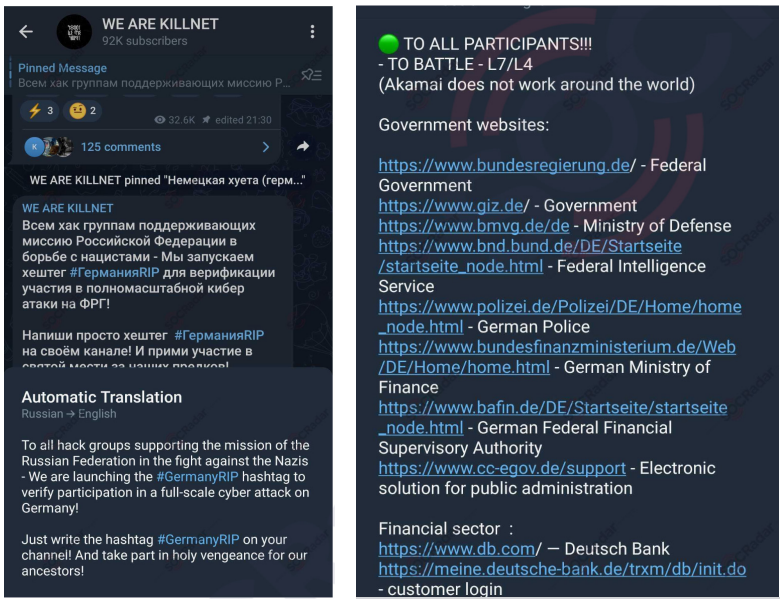


Unauthorized Network access found at German E-commerce company in the hacker forum

Recent Dark Web Activities Targeting Entities in Germany

The others (Stealer logs, Tools & Services, Botnets, Exploits, DDoS Attacks)

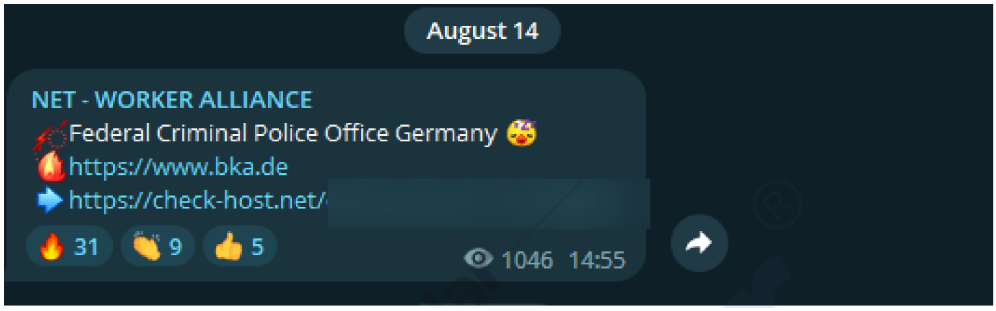
On January 26, 2023, the pro-Russian hacking group KillNet targeted government websites, banks, and airports with a coordinated Distributed Denial of Service (DDoS) campaign. They announced the launch of hashtag #GermanyRIP with the aim of encouraging the participation of hacking groups supporting the Russian Federation's alleged mission "to combat Nazis" through a potential full-scale cyber-attack on Germany.



Killnet announcement targeting German public and private institutions

On August 14, 2023, SOCRadar's Dark Web team uncovered an alarming announcement on the Telegram channel of the threat actor group NET-WORKER ALLIANCE. The announcement claimed that they had successfully launched a DDoS attack on the website of the Federal Criminal Police Office of Germany. NET-WORKER ALLIANCE is no newcomer to making such announcements; with a pro-Russian stance, this group has previously taken credit for targeting major European institutions like Europol and CYBERPOL.

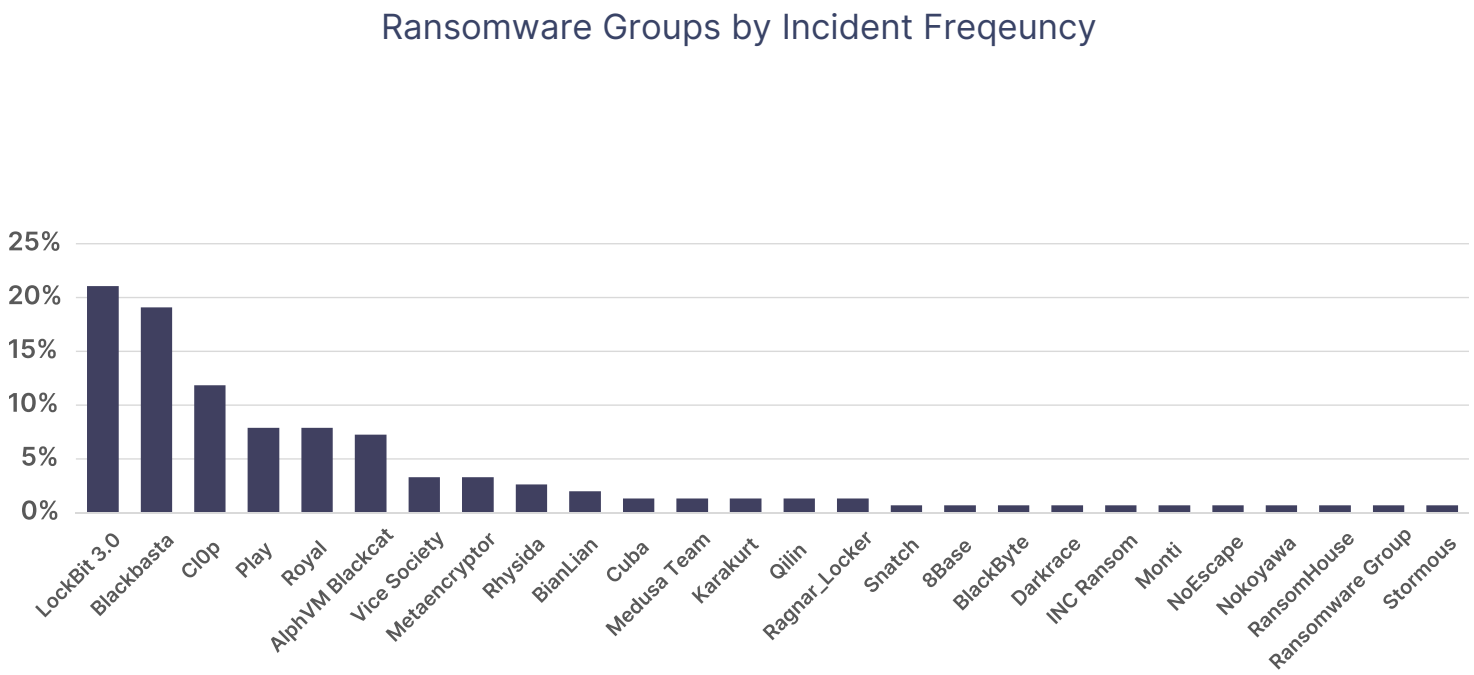
The collective formed an alliance on July 29, emerging as a consolidation of several threat actors: BLOODNET, Phoenix, BlueNet, CyberCat, unkn0wn, and Contagio. Their reasoning appears clear: to combine efforts, bring more pro-Russian cyber actors into the fold, and expand their offensive capabilities—particularly in the areas of DDoS, defacement, and penetration.



NET-WORKER ALLIANCE post about DDoS attack targeting the Federal Criminal Police Office

Top Ransomware Groups Targeting German Companies

During a 12-month period, the SOCRadar XTI platform registered 152 ransomware incidents targeting organizations in Germany. This platform is continually fed with data from hacker forums and Telegram channels, monitored and tracked by the SOCRadar Dark Web team. In that same period, 26 different ransomware groups were identified as having carried out these cyber-attacks.



Below is the top 5 list of ransomware groups targeting organizations in Germany, based on data from the past 12 months:

- LockBit 3.0
- Blackbasta
- Cl0p
- Play & Royal Ransomware
- AlphVM Blackcat

Top Ransomware Groups Targeting German Companies

The sector distribution targeted by ransomware attacks over the last year is illustrated in the graph below. It's evident that more than 20 industries and sub-industries have fallen victim to successful ransomware attacks. Virtually no industries remains untouched by ransomware threats, leading to the conclusion that applications accessible via the internet are potentially targeted by cyber-attackers, regardless of the industry.

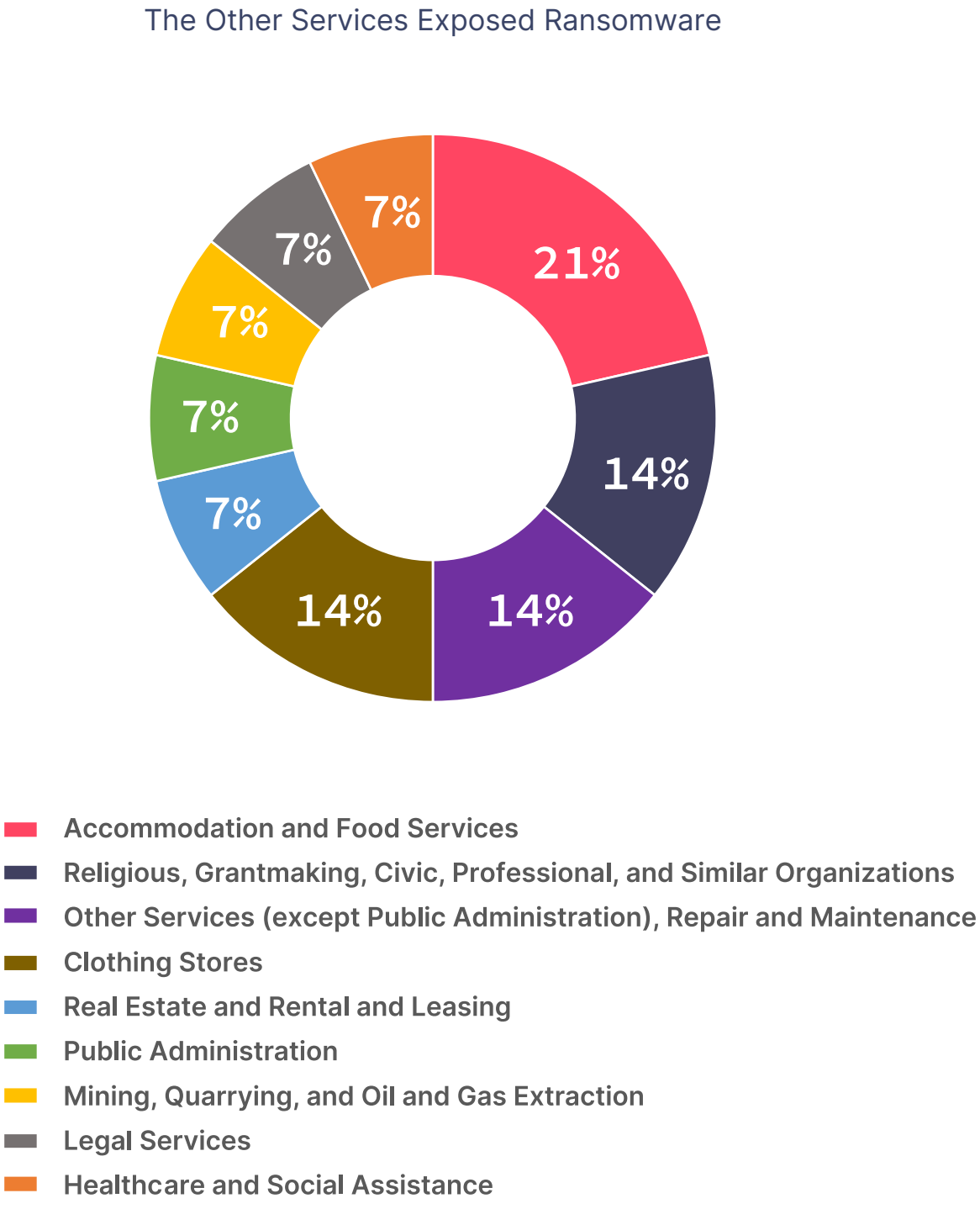
The top 5 most targeted industries, along with the number of attacks for each, are also provided below.

1. **Manufacturing (46)**
2. **Professional, Scientific, and Technical Services (18)**
3. **Other Services (except Public Administration) (14)**
4. **Information Service (13)**
5. **Retail Trade (13)**

Ransomware Distribution by Industries

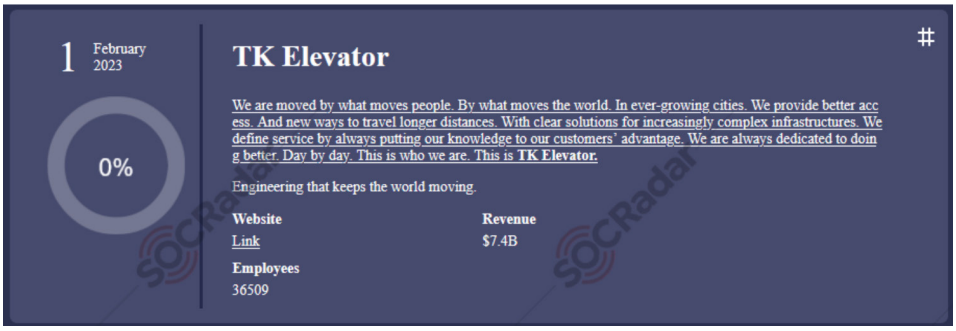
Top Ransomware Groups Targeting German Companies

The chart below provides a breakdown and distribution of sectors in the "Others" category, which ranked as the 3rd most attacked.



Prominent Ransomware Attacks in 2023

On February 1, 2023, the Royal ransomware group's website allegedly announced a new victim: TK Elevator. TK Elevator GmbH, also known as ThyssenKrupp Elevator, is a company that produces elevators, escalators, moving walkways, and accessibility solutions. It is currently the fourth-largest elevator manufacturer in the world, serving customers in over 100 countries.



Royal Ransomware victim: TK Elevator

On March 5, 2023, SOCRadar monitored the Vice Society ransomware group's website and detected new data leaks that allegedly belonged to HAW Hamburg. HAW Hamburg is currently the second-largest higher education institution in Hamburg and one of the largest universities of applied sciences in Germany. The university offers practical courses in subjects like IT, life sciences, design, media, business, and social sciences, with professors hailing from various relevant industries.

Vice Society Ransomware victim: HAW HAMBURG

On May 23, 2023, the Play ransomware group's website, also monitored by SOCRadar, allegedly announced a new ransomware victim: Black Cat Networks. The company has been providing managed support for on-premises computer network infrastructure since 2007. The threat actor announced that they have confidential data, including customer and employee documents, financial records, and tax information, and threatened to disclose them within 3 days if the ransom is not paid.

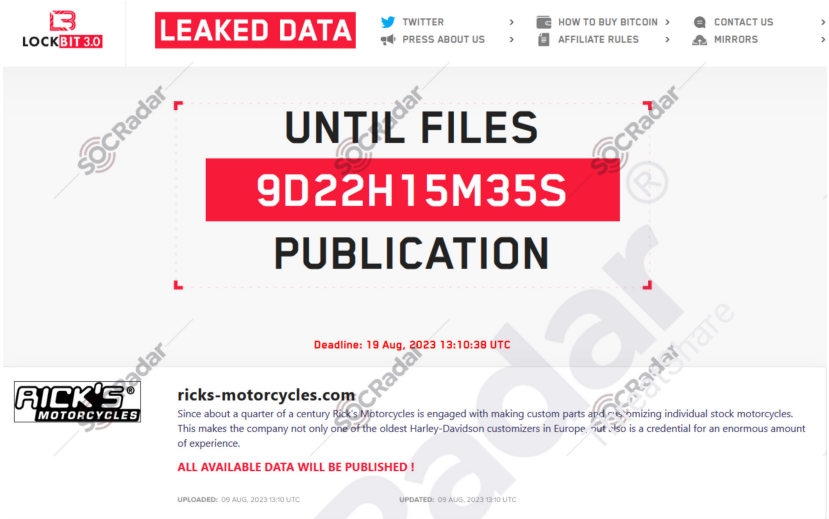
Play Ransomware victim: Black Cat Networks

Prominent Ransomware Attacks in 2023

On June 26, 2023, the Cl0p ransomware group's website, under SOCRadar's surveillance, allegedly announced a new ransomware victim: Siemens Energy. Siemens Energy AG is an energy company that was formed through the spin-off of the former Gas and Power division of Siemens AG. The group's product range mainly includes power transmission and distribution, generators, power plant technology, low-voltage switchgear, turbines (including wind, steam, and gas turbines), compressors, and electrolyzers.

Cl0p Ransomware victim: Siemens Energy

On August 9, 2023, the LockBit 3.0 ransomware group's website, also monitored by SOCRadar, allegedly announced a new victim: Rick's Motorcycles. For approximately a quarter of a century, Rick's Motorcycles has been engaged in manufacturing custom parts and customizing individual stock motorcycles. This experience makes the company not only one of the oldest Harley-Davidson customizers in Europe but also speaks to its extensive expertise in the field.



LockBit 3.0 Ransomware victim: Rick's Motorcycles

Top 5 Threat Actors Targeting German Organizations

According to research insights from SOCRadar, Germany has been targeted by sophisticated cyber-attacks in 2023, particularly from Advanced Persistent Threat (APT) groups. Here is some crucial information about five of the most prominent threat actors in highly dangerous category:

The China-based threat group Ice Frog has been conducting active cyber-espionage campaigns since at least 2011. It mainly targets government agencies, military contractors, maritime and shipbuilding organizations, telecom operators, satellite operators, industrial and high-tech companies, as well as media outlets in South Korea and Japan. Additionally, the group targets organizations in Western countries like the United States, Germany, and other parts of Europe.

The Russia-based threat group Turla, also known as Snake, is a highly sophisticated APT group focused on espionage and intelligence gathering. Active since the late 1990s, Turla is considered one of the earliest examples of cyber-espionage. The group primarily targets government departments, military organizations, and embassies.

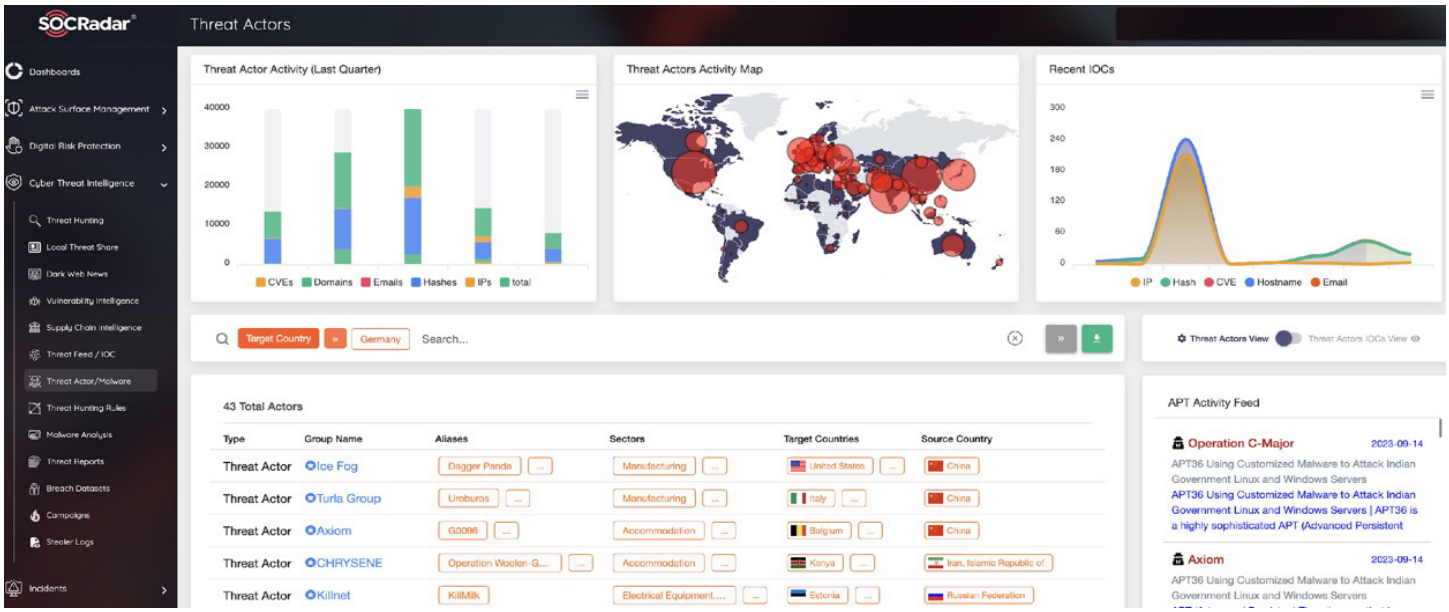
A financially motivated new threat actor, TA866, has been operating since October 2022. It targets organizations in both the U.S. and Germany. The attack chain typically starts with a malicious e-mail containing an attachment or URL, leading to the installation of malware like WasabiSeed and Screenshotter. TA866 is an organized actor capable of scaling attacks, relying on its proprietary tools and the ability to purchase tools and services from other vendors.

Top 5 Threat Actors Targeting German Organizations

Charming Kitten (also known as APT35) is an Iranian government-affiliated cyber warfare group. Identified by various companies and government officials as an advanced persistent threat, its primary targets include military, diplomatic, and government personnel in the U.S., Western Europe, and the Middle East. The group also targets the media, energy, defense, engineering, business services, and telecommunications sectors.

KillNet is a pro-Russian hacking group that gained notoriety during Russia's invasion of Ukraine in 2022. It remains active and is known for its Distributed Denial of Service (DDoS) attacks against government agencies and private companies, particularly in NATO countries.

Considering that threat actors often selectively target victims based on various criteria and tend to focus on specific sectors, contextual information enriched with dark web intelligence is crucial. Information about the changing tactics, techniques, and procedures (TTPs), as well as malware campaigns from SOCRadar's Threat Actors module, can be invaluable for proactive measures.

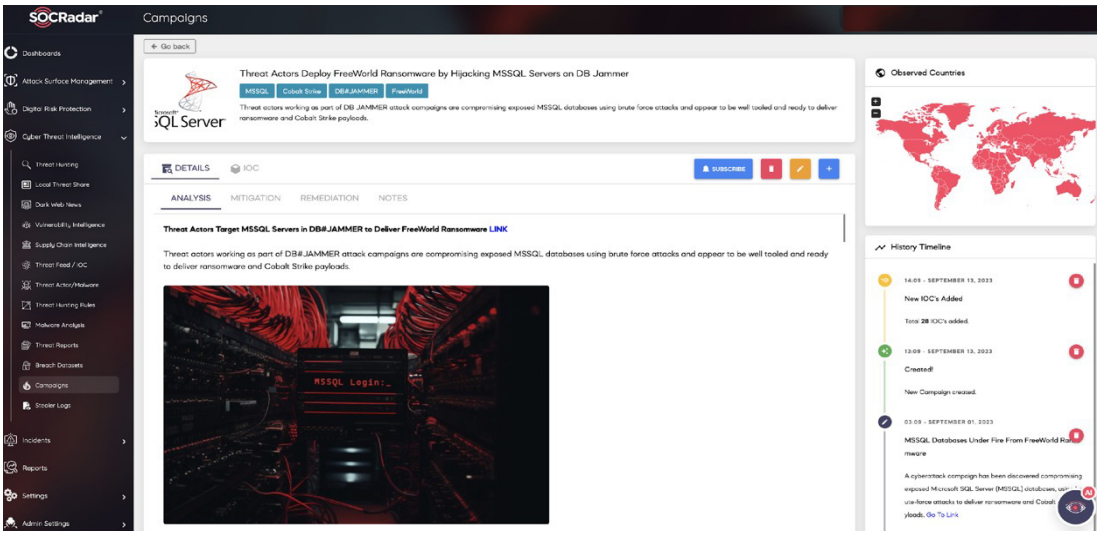


SOCRadar Threat Actors/ Malware Module

Top 5 Threat Actors Targeting German Organizations

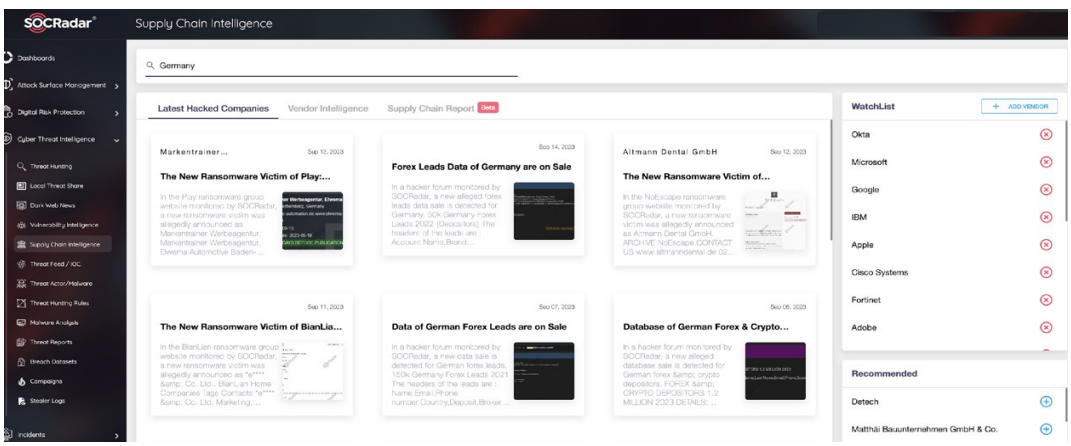
Additionally, the SOCRadar campaign page, which combines dark web and Open-Source Intelligence (OSINT), provides information on recent attack activities that have been specifically timed, successful against their targets, and continue to spread.

Intelligence information on these campaigns can be crucial to your business. Campaigns can be defined as a series of unauthorized intrusion activities sharing common goals and objectives over time. These activities may or may not be directly linked to a specific threat actor. Therefore, you can follow these threat elements, which spread over a specific area, through the SOCRadar Campaign Page.



SOCRadar Campaign Page

Furthermore, supply chain attacks are emerging threats used to distribute malware by infecting trusted, legitimate applications. These attacks often exploit businesses with weak security postures. Therefore, SOCRadar's Supply Chain Intelligence module can alert you to companies already exposed to cyber-attacks, extract actionable intelligence from vendors' past incidents and data breaches, and provide you with a report enriched with threat intelligence insights.



SOCRadar Supply Chain Intelligence Module

Conclusion and Recommendations

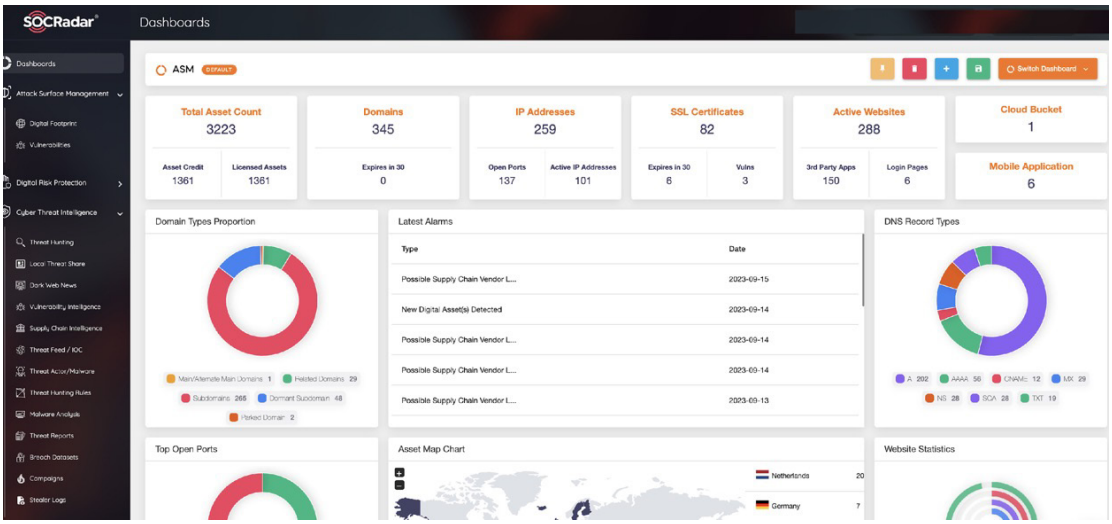
While Germany maintains its place among the economically developed countries, it has become one of the primary targets of cyber threat actors and has been significantly affected by cyber risks. The advent of Industry 4.0 and the commissioning of cyber-physical systems have particularly heightened security concerns in industries critical to economic development, such as manufacturing.

According to SOCRadar's research findings, half of the attacks targeting the manufacturing sector focus on automobile dealers, where Germany is the global leader. Additionally, the rise in ransomware attacks has severely impacted German organizations. Companies generating revenues in the billions of dollars have been hacked and victimized. Therefore, it's essential to bolster cybersecurity measures, particularly in emerging areas like Cyber Threat Intelligence (CTI), by adopting a cutting-edge security approach and setting a proactive security agenda for businesses.

Compared to data from 2022, older threat actors have been supplanted by new ones (such as the transition from LockBit 2.0 to LockBit 3.0), and there has been a rise in threat actors targeting Germany, particularly through ransomware attacks. While the volume of attacks targeting different sectors has remained relatively stable in quantitative terms, the number of sectors affected has increased by 33%. Additionally, there has been a notable escalation in the financial and reputational damage incurred by larger companies.

Based on these research results, the following recommendations are crucial for German organizations:

- Digital attack surfaces should be well-defined and managed through Attack Surface Management (ASM) services. These services discover your digital assets, assess and help mitigate your cybersecurity risk. ASM services are critical for understanding and making your expanding attack surface more visible by alerting you to relevant vulnerabilities.

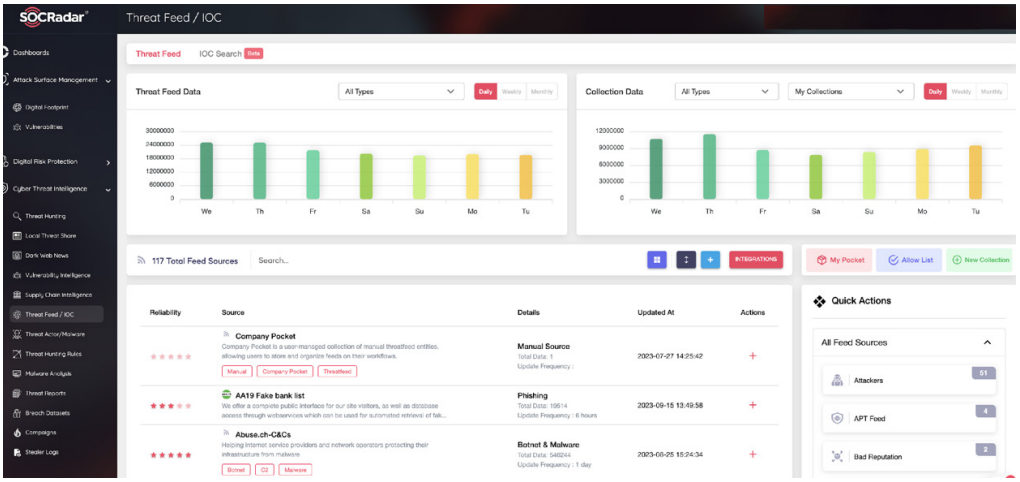


SOCRadar Attack Surface Management Module

Conclusion and Recommendations

- We find that organizations often discover cyber incidents like data breaches long after they have been compromised. To transform this reactive approach into a proactive strategy, organizations should utilize a Security Operations Center (SOC) infrastructure. This infrastructure should be fueled by Cyber Threat Intelligence (CTI) feeds that provide security analysts with actionable insights from dark web intelligence, ultimately converging cyber threat detection and response capabilities.

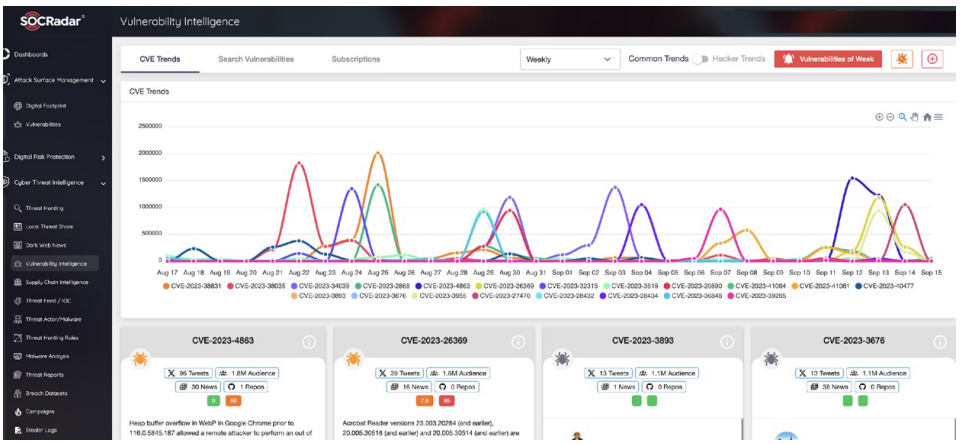
SOCRadar's Threat Feed and Indicator of Compromise (IoC) Management module assists cybersecurity teams by providing enriched data via easy-to-use dashboards. Cybersecurity professionals can customize these feeds to stay updated on the latest threats, search for indicators of Compromise (IoCs), and integrate them into company systems using the TAXII protocol.



SOCRadar Threat Feed/ IOC Management Module

- Given indications that threat actors, particularly ransomware groups, are exploiting an increasing number of vulnerabilities, it is crucial to prioritize patch management and deploy patches promptly. Moreover, as the frequency of known exploited vulnerabilities rises, databases like CISA's Known Exploited Vulnerabilities (KEV) catalog should be continually monitored, with actions taken as quickly as possible.

With SOCRadar's Vulnerability Intelligence Module, you can gain insights into which vulnerabilities are being exploited by threat actors and identify trends. Contextual and actionable intelligence about potentially vulnerable technologies can be used to expedite risk assessment and information validation processes.



SOCRadar Vulnerability Intelligence Module

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

12.000
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique dark web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and dark web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS 12 MONTHS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking dark web news, and new ransomware attacks

Download on the App Store

GET IT ON Google Play

Gartner Peer Insights™ 4.9/5