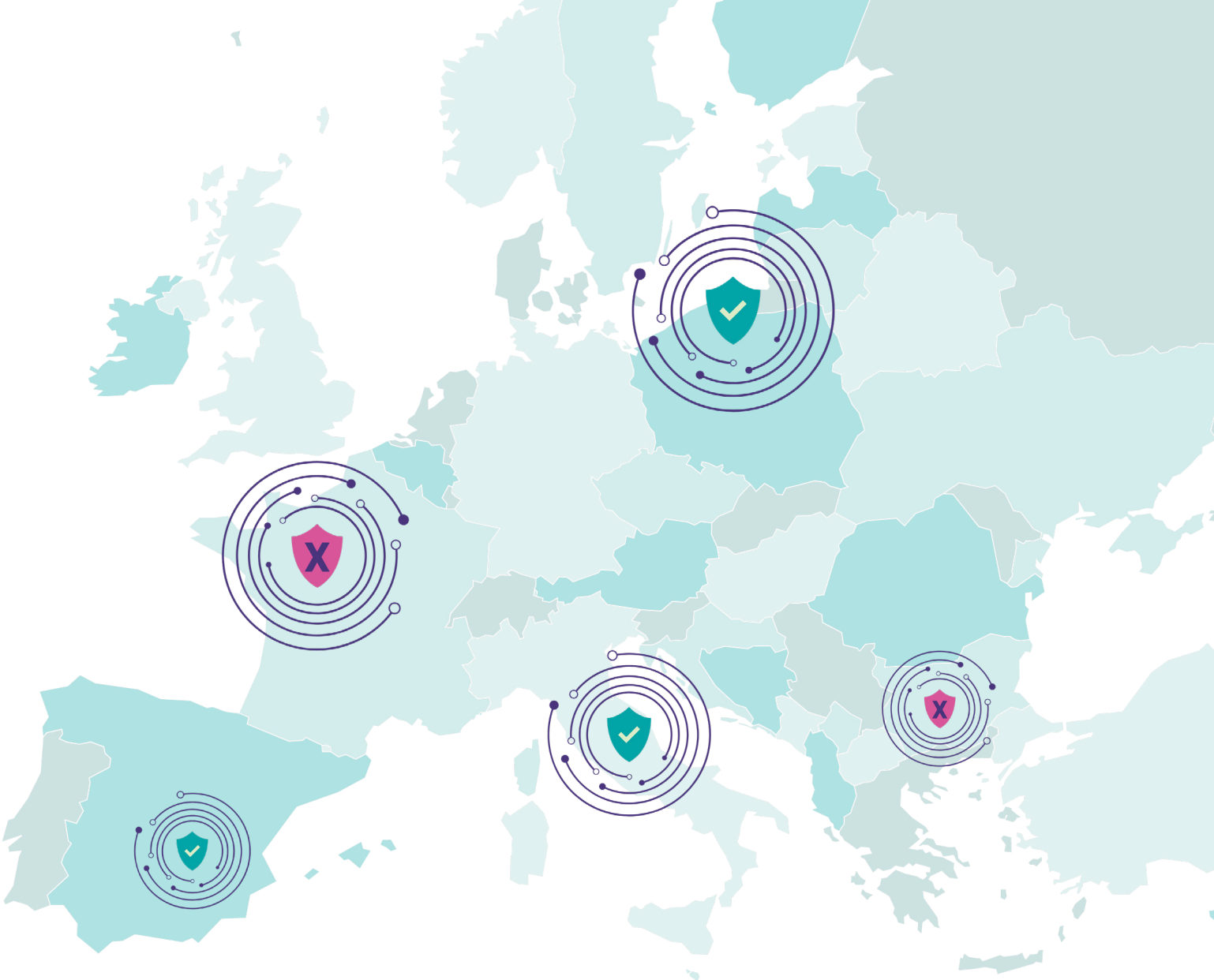


Software Security

Report in *Europe*

kiuwan
An Idera, Inc. Company

INDEX

Overview:

The European cybersecurity market is predicted to grow from $8.56 billion in 2020 to $22.67 billion by 2027, exhibiting an impressive 14.93% CAGR in that period. Of course, this growth is in large part a reaction to (and reflection of) the growth in cybercrime and cyber attacks in the region — so much so that the European Union is financing equipment and infrastructure growth in the high-priority application security (AppSec) sector.

*...European cybersecurity market is predicted to grow from **$8.56 billion** in 2020 to **$22.67 billion** by 2027...*

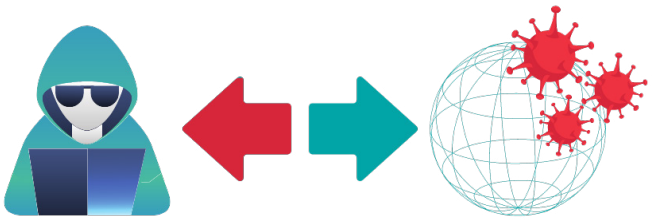
The EU's relatively new Cybersecurity Strategy unveiled in 2020 had always been meant to improve cyber resilience in the region, but a few trends since then have presented a shifting landscape to consider. Foremost among them are the changes brought on by measures against the COVID-19 pandemic and the increasing role of misinformation and disinformation in cyberattacks and campaigns.

Aside from developments that directly came about thanks to the radically dynamic impact of COVID-19, there are also key changes in the usual areas of cybersecurity, both old and new. Malware is becoming more sophisticated and harder to analyze, distributed denial of service (DDoS) attacks are finding new ground in mobile networks and the Internet of Things (IoT), and cryptocurrency becomes a mainstay of cybercrime.

In the shifting appsec landscape, this report aims to provide an overview of software security in Europe. This Europe AppSec report discusses the top ten trends in appsec and cybersecurity in the region, briefly touching on each and highlighting some key information. It will also explore some of the more recent breaches brought to light in recent years.

COVID-19 Sparks a Cybercrime Deluge

As the pandemic quickly grew to overwhelming proportions, so too did expectations of a spike in a variety of cybercrime and attacks. Indeed, COVID-19 definitely increased the ways threat actors approached their modus operandi. COVID-19 multiplied opportunities for cybercriminals as it served to become the dominant lure for phishing attacks. Threat actors actively shifted their focus to pandemic-related information, most recently in an effort to leverage vaccine information in the context of threats to data.



COVID-19 affected and disrupted practically every aspect of daily work and life. The general public's interest, curiosity, and concern during the pandemic opened up new and more intensive avenues for phishing and social engineering. Teleworking saw an increase in demand for third-party providers for companies supporting their remote employees, creating vulnerabilities in what would otherwise be business as usual appsec measures. Network appliances and remote access services that supported teleworking were heavily targeted during the height of the pandemic, most notable of which were ***increased attacks on VPN, Citrix, and RDP services***.

Cyber espionage tasking also shot up due to COVID-19 with the healthcare and pharmaceutical sectors in particular seeing increases in attacks. Targeted ransomware attacks grew as the pandemic over-burdened and disrupted the private and public healthcare sectors. Ransomware families like **Maze**, **Conti**, and **Netwalker** were observed to increasingly target small to medium-sized healthcare businesses.

AI-Enabled *Misinformation and Disinformation* Increased the Breadth and Depth of Threat Actor Capabilities

Misinformation is defined as an unintentional attack where incorrect or inaccurate information is inadvertently shared, whereas disinformation is the intentional creation of fake information. Often, these simply set the stage for later attacks through exposing vulnerabilities created by eroding trust or misleading actions. Unsurprisingly, social media is the most prominent vector for misinformation and disinformation. On platforms like ***Twitter, around 5% to 15% of users are bots responsible*** for the spread of fake information to facilitate manipulation or set up phishing campaigns.

Misinformation and disinformation are increasingly becoming central to cybercrime, and AI-enabled technologies are bolstering phishing attacks. The increased use of online and social media use proved to be green pastures for misinformation and disinformation campaigns, and the surge of new active users owing to pandemic-related lockdowns worldwide only added fuel to the fire.

One of the most common ways people were directly attacked using misinformation or disinformation was through targeted campaigns of fake news relating to the pandemic. They are then made more susceptible to fraud and phishing attempts related to COVID-19 information, such as through the sale of fake cures for instance. One specific example is a campaign including advertisements guaranteeing early vaccine access after the victim makes a deposit.

Overall, misinformation and disinformation campaigns have proven themselves formidable in hybrid attacks that reduce public trust — a significant factor in cybersecurity.

Cryptocurrency Becomes a Mainstay in Cybercrime

Cryptocurrency has become a staple way threat actors get paid through acts like ransomware attacks. In addition, ***cryptojacking has also become such a widespread phenomenon*** that browser add-ons or extensions have been developed to automatically counter it, similar in concept to automated ad blocking counteracting widespread advertising use.

Cryptojacking, which is essentially hidden cryptomining, is the act of making use of a victim's computing power to mine crypto-currency. Victims typically unknowingly install programs or scripts that allow cybercriminals to hijack their internet connected devices to run "coin miners" and generate cryptocurrency without their consent.

While the dominant type of cryptojacking — drive-by cryptomining — had been in decline since 2019, threat actors have been exploring other avenues. Cisco reports, for instance, ***that in 2020, 69% of its customers were affected by cryptomining malware***. They noted that out of any other malicious activities observed, cryptomining generated the most DNS traffic.

Cryptojacking infections **reached record highs in 2021**, particularly in the first quarter of the year when cryptomining malware increased by 117%. Some reports indicate that this surge was linked to the increase in 64-bit mining applications.

In terms of market share, cryptomining malware saw the following players lead the board:

- XMRig (35%)
- JSECoin (27%)
- Lucifer (7%),
- WannaMine (6%)
- RubyMiner (5%)
- Others miners (20%)

Cryptocurrencies may be in a state of flux as of late, but so long as there is financial gain to be attained with these attacks, they are only expected to continue in the long run.

Cyberattacks Are Becoming *Increasingly Motivated* by Money

Financial gain is becoming the largest motivator behind cybercrime, with even state-sponsored actors engaging in revenue-generating activities.

The North Korean group **Lazarus**, for instance, appeared to have conducted ransomware intrusions specifically for monetary gain. In the U.S., individuals linked to the group **APT41/WICKED PANDA** had been indicted by the Department of Justice for cyber espionage activities and cybercrime attacks on the video game industry. A common theme was for the group to hack games to obtain in-game currency and then sell for profit. Another threat group, **PIONEER KITTEN**, had been observed peddling corporate network access on underground forums. Again, cryptocurrency is heavily involved in cybercrime, with groups like **Labyrinth Chollima** and **Stardust Chollima** targeting exchanges and stealing wallet credentials among other activities.

As the COVID-19 phishing and fraud campaigns mentioned above show, cybercriminal activities large and small are all leaning towards financial gain, and one of the trends ***seen in Europe recently has been the increase in ransomware***. Triple extortion ransomware schemes increased in 2021, and, more alarmingly, the ransomware-as-a-service business model is on the rise, complicating the attribution of individual threat actors. Additionally, phishing-as-a-service unfortunately is also growing. Both unethical business models are arming ransomware and phishing with structure and organization, corroborating the observation that financial gain is increasingly becoming front and center for cyberattacks.

The *Most Common Vectors* for Ransomware Remain

Amidst all the growth in various areas of cybercrime, there are staples that remain the same, such as the most common vectors for ransomware — namely, compromise through phishing emails and RDP brute-forcing. Not coincidentally, these two methods are the cheapest and most profitable for cybercriminals.

Cybercriminals have been observed to match COVID-19 lure themes to the different stages of the pandemic, and phishing campaigns are imbuing attacks with authoritative and highly emotionaly charged triggers. For example, there has been a marked increase in phishing lures related to new COVID-19 variants, vaccine information-related lures, and even passing mention of the pandemic with previously used lure content like invoices and deliveries.

RDP compromise as a vector of attack has been in decline since 2020, but it remains a heavily used method to gain an initial foothold for threat actors. Cybercriminals brute force RDP by taking advantage of weak credentials, lack of two-factor authentication, and other vulnerabilities. They go on to leverage legitimate access (through genuine credentials) to stay undetected within the network. Many small to medium-sized enterprises do not actively monitor such activity and are thus more likely to fall prey to this method.

Business Email Compromise (BEC) Increased, Gaining in Sophistication and More Refined

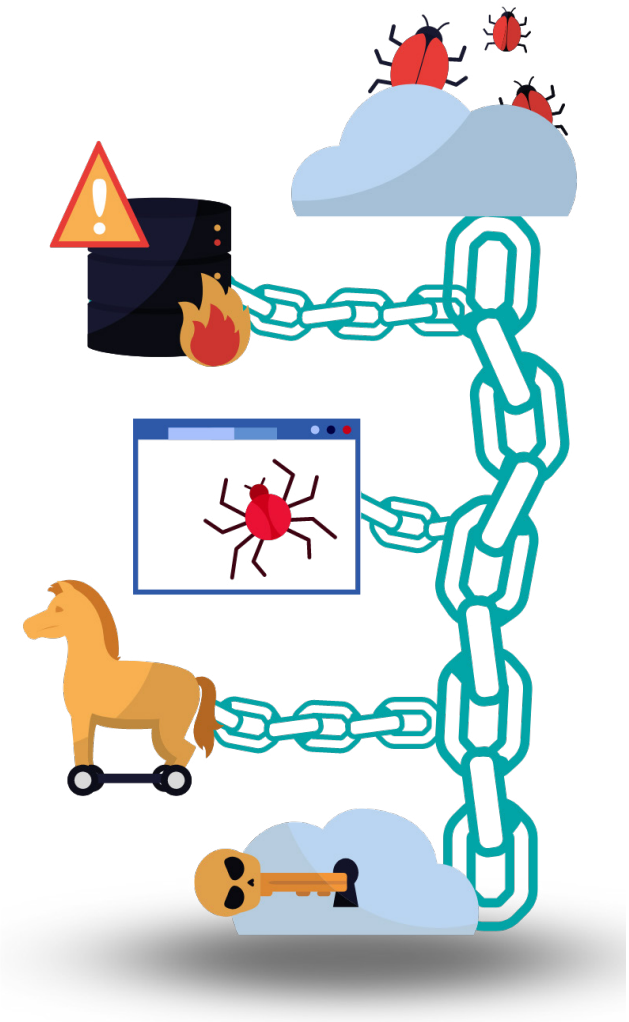
BEC was cited as the costliest type of cybercrime in 2020 when organizations reported related **losses of more than $1.8 billion**. BEC schemes have also become more sophisticated, making use of complicated credential phishing and converting money into cryptocurrency. **Office 365 accounts were reported to be heavily targeted by BEC scams in the EU in recent years**, implying that cybercriminals conducted other attacks such as password spraying and credential phishing against the victims. BEC attacks have also been observed to focus more on small to medium-sized enterprises.

In one BEC attack in March 2021, senior employees in retail, insurance, and finance were lured by what appeared to be Office 365 updates to phishing pages that captured their login credentials. Once their account credentials were accessed, the attackers were able to gain information that they then used to send fraudulent messages requesting bank transfers.

These types of attacks are likely to interest more sophisticated groups in the future. The group Cosmic Lynx, for example, appears to already have been drawn by the highly lucrative potential of BEC scams.

Sophisticated Supply Chain Compromises Target MSPs

According to the European Union Agency for Cybersecurity (ENISA), the threat to supply chains opens up the possibility of catastrophic cascading effects. The organization has indicated that these supply chain compromises are critical even among other major appsec threats. Cybercriminals are targeting managed service providers (MSPs) to create opportunities, according to ENISA's analysis of supply chain attacks discovered from January 2020 to July 2021. According to their data, in 2021, there were four times more supply chain attacks than the previous year.



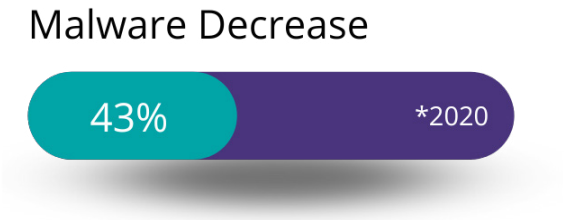
In a report dedicated to this threat, ENISA reported that cybercriminals first attack suppliers to gain access to the assets of their customers or those of another supplier. Cyberattacks are only categorized to be supply chain attacks if both supplier and customer are targets. In the report, ENISA analyzed 24 supply chain attacks and found that 58% of them wanted access to data (customer personal data or intellectual property), and another 16% wanted access to people.

The organization found that in 62% of the attacks, the cybercriminals leveraged the customers' trust in their supplier, and in fact, 66% of the attacks were focused on supplier code. Additionally, malware was used in 62% of all cases analyzed.

ENISA recommended that organizations incorporate their suppliers into their processes and standards for data protection and security verification.

Malware Reporting Continues to Decline, *but...*

Since the start of 2020, malware has been undergoing a gradual decline: in North America and Europe, for example, malware attacks decreased by around 43% from 2019 to 2020.



However, the global teleworking practices forced by pandemic lockdowns may be limiting malware visibility as throngs of people started using personal devices to perform their work. These same devices typically do not match the level of malware detection and protection of in-office business networks.

Additionally, though ENISA expects numbers related to malware to continue to dip, there are some concerning upwards trending figures that point to malware becoming more about the quality of the attacks rather than the quantity. For example, malicious Office files have exceeded the number of malicious PDF files by 150% in 2020. Furthermore, malware that targets Windows container environments is becoming widespread.

In November 2020, malicious container images that found and exploited vulnerabilities in a user's **Kubernetes environment** were first identified. One month later, researchers also discovered an infection that would not be detected by common static scanners: file-less malware that was executed from memory. By March 2021, researchers discovered Siloscape: the first known malware that specifically targets Windows containers and compromises cloud environments.

In an effort to bypass detection, malware developers have gone back to one of the oldest tricks in the book: resorting to new or uncommon programming languages. Some programming languages that were used to create malware in ***2020 to 2021 included Go, DLang, Rust, and Nim***. New strains of malware are harder to reverse engineer and dynamically analyze.

DDoS Actors Find New Ground

Ransom Denial of Service (RDoS) has been gaining in popularity starting from August 2020. Groups such as Lazarus Group, Fancy Bear, and Armada Collective actively engage in this activity, which usually targets e-commerce, travel, and finance. RDoS does not require as many resources as a traditional DDoS, and it's often used to blackmail organizations with vulnerable systems in one of two ways:

- **Attack-first RDoS** where an attack begins and ransom is demanded for it to stop
- **Extortion-first RDoS** where an extortion letter and a small-scale DDoS is conducted to prove the threat

Additionally, traditional DDoS is going mobile. A new wave of DDoS attacks is stemming from the widespread deployment of 5G networks and the continued adoption of IoT. 5G can make IoT more vulnerable, while IoT itself makes for an excellent threat vector for DDoS.

Devices and sensors connected to IoT make for ideal DDoS targets as these often do not have sufficient resources for proper security. They are simple to corrupt and often come with weak protections and misconfigurations by default. Cybercriminals also leverage the fact that users are operating complex mobile systems while lacking security skills.

Furthermore, virtualized environments that share resources have been found to amplify DDoS attacks. Cybercriminals have been observed to adjust their DDoS attacks by monitoring their targets' counter-measures through publicly available information as well. DDoS attacks are truly becoming more targeted, persistent, and multivector.

Threat Actors Are *Increasingly Consolidating* and *Collaborating*

One of the most worrying trends that can only be expected to continue is the increasing collaboration and professionalization of cybercriminals and groups. The global cybercrime ecosystem thrives on a cybercrime-as-a-service model that lowers the barriers for threat actors while also lengthening the reach of attacks. According to ENISA, the cybercrime ecosystem can broadly be categorized into:

- **Main services** — Typically, the primary services revolve around access brokers, credit/debit card testing services, phishing kits, malware packing services, ransomware, hosting and infrastructure, DDoS attack tools, anonymity and encryption, antivirus service counters, and general crime-as-a-service as well as recruiting for criminal groups.

- **Distribution services** — Heavily revolving around distribution, common service types include social networks, instant messaging, email spam, and the purchase of traffic or traffic distribution systems (TDS).
- **Monetization services** — This aspect covers services like money mules, collection and sale of payment card information, ransom payments, reshipping fraud networks, dump shops, and wire fraud cryptocurrency services.

This ecosystem and the actors within it function much in the same way as crime syndicates in terms of brokering information and access, creating affiliate programs to further accelerate the sales of malware, and partnering in cartels that enhance collaboration and resource sharing.

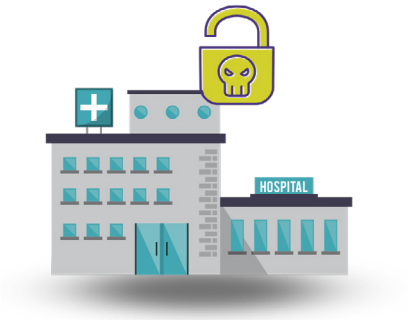
5 Recent *Security Breaches* Highlight the Cost of Insufficient AppSec

Major data breaches regularly make news rounds when they happen. More recently, for example, leaked phone numbers of over 500 million Facebook users had resurfaced after being leaked on hacking forums, and potentially hundreds of millions of LinkedIn users had their scraped data leaked as well. Furthermore, cybercrime that piggybacks on current events such as the Ukraine war can easily take the spotlight. Just this March 2022, for instance, Google uncovered a phishing campaign that targeted Ukrainian news providers while ESET Research pointed out some threat actors are creating fake donation pages masquerading as humanitarian aid for Ukraine.

Here are five recent security breaches that impacted European organizations to illustrate the threat and cost of insufficient appsec.

1. Private Data of 1.4 Million Patients *Stolen* From Parisian Hospital System

In an example of healthcare systems being targeted during the pandemic, reports surfaced towards the latter half of 2021 of the Paris public hospital system being attacked by hackers who accessed the information of around 1.4 million patients. The compromised data included information such as names, contact details, and security numbers of people who tested for COVID-19 in 2020. The hackers also got their results as well as the names and contact details of the healthcare professionals who treated them.

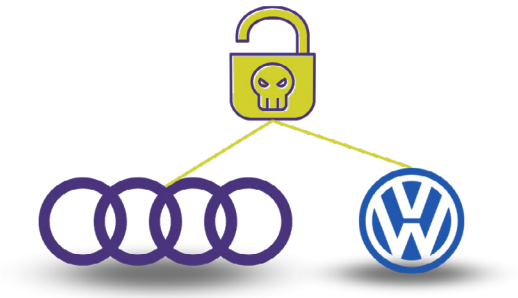


2. Supply Chain *Ransomware Attack* on IT Solutions Developer Compromises up to 1,500 SMEs

Kaseya, a provider of IT solutions for MSPs and enterprise clients, was targeted by a ransomware attack in mid-2021. In a textbook example of a supply chain attack, cybercriminals took advantage of Kaseya's Virtual System Administrator software vulnerabilities to gain access to several MSPs and their customers. Although less than 0.1% of Dublin- and Florida-based Kaseya's customers were involved in the breach, it is estimated that 800 to 1,500 SMEs may have been compromised because of the attack.

3. 3.3 Million Volkswagen and Audi Customers Affected by *Data Breach*

Many current or prospective buyers of auto manufacturer Audi had their data stolen in June 2021 after unsecured information relating to sales and marketing was exposed online. The data breach had been traced to an associate vendor. The leaked private customer information of 3.3 million people included names, mailing addresses, email and phone numbers, and the data pertaining to vehicles they purchased, leased, or about which they inquired.



4. Airlines IT Services Provider *Hacked*

SITA, an aviation industry IT supplier that works with 90% of the world's airlines, reported towards the end of the first quarter of 2021 that hackers had gained access to passenger information. The Switzerland-based company reported in a statement that it was the target of a "highly sophisticated attack" but did not immediately disclose what information was breached pending investigation. Estimates put the number of affected individuals in the hundreds of thousands.

4. Cryptocurrency Exchange Shuts Down Following *Cyberattack*

Russian cryptocurrency exchange Livecoin was hacked around Christmas 2020, and one month later it had to close down for good. The cyberattackers took control of the exchange's systems to tamper with exchange rate values, for instance, adjusting Bitcoin exchange rates at the time from $23,000 to $450,000. When Livecoin alerted users to stop all activity, the hackers cashed out their profits. Livecoin said the technical and financial damage of the attack led to the decision to permanently close its doors.

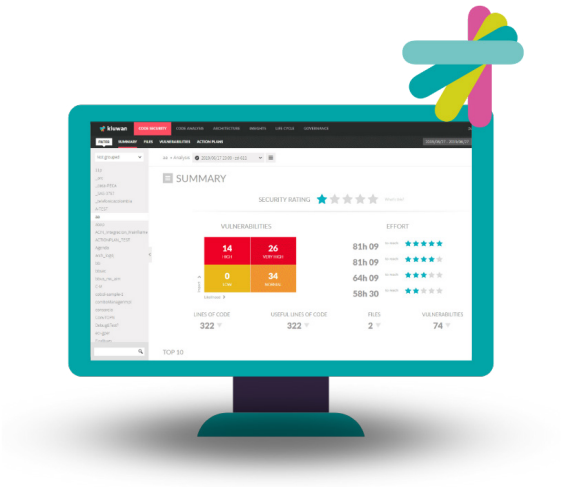
The cybersecurity landscape is a living digital arms race that shifts as both sides evolve to meet the others' challenges. With the trends examined in this report and the damage evident in some of the most recent security breaches that impacted European organizations, it's clear that top-of-the-line appsec is a worthwhile investment for any company that requires robust standards and protections for development, security, and operations (DevSecOps).

Kiuwan Helps Organizations Maximize AppSec Capabilities

In the face of these appsec trends in Europe, organizations running DevOps need a partner to constantly keep abreast of software supply chain code vulnerabilities and bolster their development security.

Kiuwan offers top-class solutions for application security and is uniquely positioned to protect Go language applications from being exposed to data breaches. The DevSecOps capabilities Kiuwan provides can identify code vulnerabilities and integrate with your DevOps pipeline to automate security processes.

Book a demo with Kiuwan today!



*YOU KNOW **CODE**, WE KNOW **SECURITY**!*

GET IN TOUCH:

Headquarters
2950 N Loop Freeway W, Ste 700
Houston, TX 77092, USA

United States **+1 732 895 9870**
Asia-Pacific, Europe, Middle East and Africa **+44 1628 684407**
contact@kiuwan.com
Partnerships: **partners@kiuwan.com**