Top 10 Cyber Incidents 2022

This report has been produced by:

Isaac Guasch

Cyber Security Leader

Tokio Marine HCC International

TOKIO MARINE
HCC

Top 10 Cyber Incidents 2022

2022 has been a year of global inflation, massive hikes in energy costs, and war. So, it should come as no surprise that the cost of a data breach has reached an all-time high. In this report, our Cyber Security Leader, Isaac Guasch, uncovers the key cybersecurity attacks of 2022 in terms of financial impact and reputational damage. These attacks highlight the malicious intent of not just common criminals, but also world leaders, and show how just one attack can affect millions of consumers (with a special mention of one of the current biggest fashion-retailers). Also, read on for a "Bonus Track" where Isaac showcases just how far we have come in AI technology.

Russia's invasion of Ukraine 1

(Nation State attack)

SOURCE

Impact

Global catastrophe.

On 24th February, Russia invaded Ukraine under the pretext of a "special military operation", as announced by its head of state, Vladimir Putin. In addition to the physical conflict, as another vector of warfare, cyber attacks were carried out to target critical infrastructure, public administration and many private companies.

Several attacks had been documented even before the invasion. On 15th February, most of the Ukrainian government websites, banks and radio stations suffered massive DDoS (Distributed Denial of Service) attacks which disabled them for several hours. This was followed by the disruption of satellite network facilities, malware attacks (using IsaacWiper and HermeticWizard, a new destructive worm that wipes data from infected machines), spoofing (hacking a TV station to report fake information, phishing, etc.) and an endless list of other attacks.

This shows how cyber criminals can be put to use by nation states to complement traditional warfare and maximise damage across different sectors of society.

ProxyNOTShell 2

(Supply chain attack, Worldwide IT provider)

SOURCE 1

SOURCE 2

Impact

Systemic risk or incalculable due to Microsoft clients' and 3rd parties' widespread use of Microsoft Exchange.

In late September, two new Microsoft Exchange vulnerabilities were disclosed publicly. The vulnerabilities, CVE-2022-41040 and CVE-2022-41082, allow an attacker to compromise the exchange server (41040) and to remotely execute code (41082).

These vulnerabilities are very similar to the Exchange vulnerabilities announced in 2021 and pose systemic risk of incalculable consequences to a wide range of enterprises. Microsoft Exchange – the email system – is a core foundational enterprise system and one of the main sources of sensitive and attack-enabling information.

Costa Rica

3

(Nation State attack)

SOURCE 1

SOURCE 2

Impact

State of National Emergency; $10M ransom demanded, estimated daily losses of $30M; systemic risk for the country.

On 17th April, a ransomware attack was launched against nearly 30 institutions belonging to the Costa Rica government. The attack forced the country to shut down its major operations on taxes, imports and exports for several days.

The president of Costa Rica, Mr. Alvarado, stated on 21st April that it had been "a criminal cyber attack on the State". Two weeks later, on 8th May, Costa Rica decreed a state of national emergency due to cyber attacks. The perpetrators were a Russian group of hackers wanting to show their might against a country with relatively poor cyber defences.

This shows how a group of criminals can paralyse a whole country. Costa Rican authorities have recognised their lack of prevention and ability to respond to cyber attacks and have vowed to pour more resources into improving the country's cyber security.

Revolut

4

(Financial institution)

SOURCE

Impact

Data breach: 50k customer data; Reputational damage.

On 11th September, Revolut discovered a malicious access to their IT systems, potentially impacting their clients' personal data. In compliance with the General Data Protection Regulation (GDPR) and due to the nature of the incident, Revolut reported the data breach to the State Data Protection Inspectorate of Lithuania (VDAI), who confirmed the notification on its official website.

The official statement issued by the VDAI also announced the initial information and actions taken: "According to preliminary data, access to the Revolut database was obtained through the use of social engineering methods. [...] Upon noticing the security incident, Revolut's security team took prompt action to eliminate the attacker's access to the company's customer data and stop the incident."

According to the same statement, the personal data (such as names, addresses, emails and account data) of 50,150 customers around the world, 20,687 of which were in the European Economic Area, may have been affected during the incident. Any stolen payment card numbers had been masked, said the company.

The emerging high-growth FinTech companies that hold credit card data are an extremely attractive target for hackers. Attacks on these natively digital systems can potentially – and financially – affect millions, as well as ruin an up-an-coming platform's reputation for good.

The Finnish Parliament

5

(Nation State attack)

SOURCE 1

SOURCE 2

Impact

Business interruption of the legislative branch of a Nation State.

On 9th August at around 2.30pm, a DDoS (Distributed Denial of Service) attack was directed against the Finnish Parliament's external websites. The Parliament announced steps to limit the attack together with service providers and the national Cyber Security Centre. It was not until the next day at 10pm that the Parliament's official Twitter account confirmed the situation had been normalised.

According to the Finnish national broadcaster YLE, a Russian hacker group called NoName057 claimed responsibility for the attack. The group had published a post on their Telegram channel confirming they were responsible for the attack and their motive: "We decided to make a "friendly" visit to neighbouring Finland, whose authorities are so eager to join NATO".

Political positions taken by countries can make them a target of cyber criminals with opposing political ideas.

6 Okta

(Worldwide IT provider)

SOURCE

Impact

Data breach, reputational damage and intellectual property theft.

In early December, GitHub – the world's largest source code repository – alerted Okta about a possible suspicious access to their code repositories. Upon investigation, Okta concluded that their code repositories had indeed been accessed and copied.

According to Okta's investigation, despite intellectual property theft by means of code copying, there was no unauthorised access to the Okta service, or to any customer data.

As an exercise in transparency, the company quickly made a statement explaining the incident, scope and their response to remediate any consequences: "We have since reviewed all recent access to Okta software repositories hosted by GitHub to understand the scope of the exposure, reviewed all recent commits to Okta software repositories hosted with GitHub to validate the integrity of our code, and rotated GitHub credentials. We have also notified law enforcement."

Apart from reputational damage, there is a potential risk that the attackers will study Okta's codes and use this information to launch future attacks on their products.

7 TSB

(Financial institution)

SOURCE

Impact

Financial loss: £48,65M fine for operational resilience failings.

On 20th December, the UK Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) imposed a £48,65M fine on TSB Bank. The fine corresponds to an incident that occurred in April 2018, when TSB updated its IT systems and migrated its corporate and customer services data onto a new IT platform. While the data itself migrated successfully, the platform immediately experienced technical failures. This resulted in significant disruption to the continuity of TSB's banking services, including branch, telephone, online and mobile banking.

As acknowledged by the FCA, the migration programme was highly complex and carried a high level of operational risk, and its success was critical to providing continuity and safety of core functions. The regulators concluded that "TSB failed to organise and control the IT migration programme adequately, and it failed to manage the operational risks arising from its IT outsourcing arrangements with its critical third-party supplier."

This is a clear demonstration of how far the costs of an IT incident can go.

8 SHEIN

(Fashion e-commerce retailer)

SOURCE

Impact

Reputational damage and financial loss: 39M clients' accounts stolen and $1.9M fine.

On 12th October, the New York Attorney General secured $1.9 million from e-commerce retailer, Zoetop Business Company, Ltd. (Zoetop), owner of the brands SHEIN and ROMWE, for failing to properly handle a data breach that compromised the personal information of tens of millions of consumers worldwide, and for lying about the scope of the breach to consumers.

A data breach incident had also occurred back in June 2018, when attackers stole personal and credit card information and hashed customer account passwords from SHEIN. The initial public statement made by Zoetop stated that only 6.42 million consumers had been impacted by the breach and that the company was in the process of notifying all affected customers. However, two years later, Zoetop discovered login credentials for ROMWE customer accounts available on the dark web.

A forensics investigation finally concluded that 39 million SHEIN and 7 million ROMWE accounts had been compromised, and that the company had failed to take adequate steps to protect many of the impacted accounts after the breach, as well as downplaying the extent of the cyberattack to consumers. Transparency in reporting cyber incidents to authorities and customers should not be taken lightly as financial and reputational consequences for failing to do so can be harsh.

Binance

9

(Fintech)

SOURCE 1

SOURCE 2

Impact

Financial loss: 2M BNB (Binance's cryptocurrency), worth $566 million.

On 7th October, Binance – a cryptocurrency exchange – officially confirmed on Twitter that they had suffered a security incident: "An exploit on a cross-chain bridge, BSC Token Hub, resulted in extra BNB. We have asked all validators to temporarily suspend BSC. The issue is contained now. Your funds are safe. We apologize for the inconvenience and will provide further updates accordingly."

Binance is the largest cryptocurrency exchange and, as many others, they have their own coin (BNB), tokens and related products like BNB SmartChain (BSC), to empower users to build their decentralised apps and digital assets on one blockchain and take advantage of the fast trading to exchange on the other.

Initial estimates for funds taken off BSC are between $100M - $110M. However, the company stated that thanks to the community and their internal and external security partners, an estimated $7M had already been frozen when the statement was released.

In a further update on Binance.com, the company transparently shared the conclusions from their internal assessment and confirmed that "a total of 2 million BNB was withdrawn". Binance is the largest crypto marketplace, and the value of the loss was extremely high, which is why this is undoubtedly considered a Top-10 attack.

Twitter

10

(Social media)

SOURCE 1

SOURCE 2

Impact

Data breach: 5.4M user data leaked and 400M users scraped.

On 5th August, Twitter announced an incident impacting some accounts and private information on its social network.

As a result of a bug bounty program, the company was aware of a new system vulnerability that could reveal some personal information during the log-in flow. Although the bug was fixed, the official communication mentioned that "Twitter learned through a press report that someone had potentially leveraged this and was offering to sell the information they had compiled. After reviewing a sample of the available data for sale, we confirmed that a bad actor had taken advantage of the issue before it was addressed."

A few months later, in November 2022, the company gave an update about the incident, informing that some user data had allegedly leaked online, and their Incident Response Team determined that the exposed data was the same as in the incident announced in August.

It is estimated that the amount of data leaked is of 5.4 million accounts.

In addition to that, in December 2022, a threat actor claimed to be selling public and private data of 400 million Twitter users scraped in 2021 using the same vulnerability. The hacker threatened the owner of Twitter, Elon Musk, about a potential massive GDPR fine if the data were to be published, and asked $200,000 for an exclusive sale to avoid this.

Bonus Track

Looking forward and to raise awareness of current hot topics on the cyber arena, here a peak into the potential risks and benefits of a relatively emerging technology that is now available to any user – Artificial Intelligence.

The risks of Artificial Intelligence

Artificial intelligence (AI) is a rapidly developing technology that has the potential to revolutionise many industries, but it also poses significant cyber risks.

One of the main risks associated with AI is the possibility of hackers gaining access to the systems and data used to train and operate the technology. This could allow them to manipulate the AI algorithms and potentially disrupt or exploit the system. For example, if an AI system is used in a self-driving car, a hacker could potentially alter the algorithms to cause the car to crash.

Another risk is the potential for AI to be used to automate cyber attacks. For example, an AI system could be trained to scan the internet for vulnerabilities in a company's network and then launch a coordinated attack on those vulnerabilities. This could be done at a much faster pace than a human attacker could manage, making it much more difficult to defend against.

AI also poses a risk to data privacy. As AI systems become more prevalent, there is a risk that personal data will be collected and used without proper consent or oversight. This could lead to sensitive information being mishandled or misused.

Finally, AI systems can also be vulnerable to bias and discrimination. If the data used to train an AI system is biased, the resulting algorithms could perpetuate and even amplify those biases. This could have serious consequences, particularly if AI is used in decision-making processes that affect people's lives, such as hiring or loan approval.

Overall, it is important for organisations to be aware of the potential cyber risks associated with AI and to take steps to mitigate them. This may include implementing strong security measures, carefully managing the data used to train AI systems, and being mindful of any potential biases in the algorithms. By taking these precautions, organisations can help to ensure that AI is used safely and ethically.

Conclusions

It has become clear that artificial intelligence is an important risk to closely monitor in the coming years. Actually, it is already being widely used for different purposes – the text you have just read was written precisely by an artificial intelligence engine* and has not been edited by any humans.

While the potential for positive impacts through the use of AI in all kinds of fields is huge, we wanted to briefly introduce the new risks that AI can and will bring along.

It is incredible to see that, nowadays, algorithms not only solve mathematical problems, but can explain calculation steps in human language, answer complex questions on any topic, write articles, theses or dialogues between invented people, provide pieces of code in almost all programming languages, and much much more.

This universal access to knowledge will undoubtedly suppose a change in the rules of the game.

However, AI technology will also carry many risks, as touched upon in the above text. The issue of determining the authenticity of the information, in addition to the speed of creating new applications and process automation, make it hard to quantify these new risks.

To give a tangible example, let's focus on the use of AI to generate code snippets. This possibility opens a big door for programmers as well as attackers. Imagine a disgruntled employee asking the AI engine to write an email supposedly written by a third party, in English, using business language, with no more than 200 words, etc. This employee can also request a piece of software on how to send fake emails.

Creating new ways to attack could be as simple as connecting these two outputs. Our team has been studying the AI engine since its release. The sophistication of the model is such that when it was asked to write a Javascript code to send emails, the tool corrected us, saying that this was not possible, as Javascript is a client-side programming language, and suggested to use server-side languages such as PHP, while also providing a code example to send emails.

This is just a sample of what can be done and a warning that this technology is potentially a game-changer.

**ChatGPT, a chatbot launched by OpenAI in November 2022, built on top of OpenAI's GPT-3.5 family of large language models, and fine-tuned with both supervised and reinforcement learning techniques.*
Source: https://chat.openai.com/

Cyber at Tokio Marine HCC

We know… Cyber

Tokio Marine HCC has been innovating in Cyber Liability Insurance worldwide, for over 20 years. Our dedicated global team is made up of cyber insurance and in-house claims experts with deep industry knowledge and a wealth of cyber security experience. We promote active knowledge exchange, making us a global leader when it comes to cyber risk, while keeping you at the forefront of emerging threats on the ever-evolving Cyber landscape.

From offices in the U.S., our cyber team insures US-domiciled businesses, with a focus on the small- to mid-sized segment, as well as individuals concerned with protecting their family, home and privacy from cyber threats. From Europe and the U.K., our team concentrates on mid- to large-sized businesses domiciled anywhere outside of the U.S. In addition, we leverage our in-house Cyber expertise to enhance other Tokio Marine HCC insurance coverages, letting you take on risk with confidence.

Learn more about Cyber at Tokio Marine HCC by visiting tmhcc.com
Follow us on LinkedIn: #TMHCC_Cyber

Find out more about our Cyber Security Insurance at TMHCC International:

TMHCC Cyber Insurance

Email our Cyber Security Team

TOKIO MARINE
HCC

This report has been produced by:

Isaac Guasch Garcia

iguasch@tmhcc.com

Isaac Guasch
Cyber Security Leader
Tokio Marine HCC International

Contact Us

Barcelona
Tokio Marine Europe - Spanish Branch
Torre Diagonal Mar
Josep Pla 2, Planta 10
08019 Barcelona, Spain
Tel: +34 93 530 7300

London
HCC International
Fitzwilliam House, 10 St. Mary Axe
London EC3A 8BF, United Kingdom
Tel: +44 (0)20 7648 1300
Lloyd’s Box 252, Second Floor

Munich
Tokio Marine Europe - German Branch
Rindermarkt 16
80331 Munich, Germany
Tel: +49 89 3803 4640

#TMHCC_Cyber

A member of the Tokio Marine HCC group of companies

Tokio Marine HCC is a trading name of HCC International Insurance Company plc (HCCII), Tokio Marine Europe S.A. (TME) and HCC Underwriting Agency Ltd (HCCUA), members of the Tokio Marine HCC Group of Companies.

HCCII is authorised by the UK Prudential Regulation Authority and regulated by the UK Financial Conduct Authority and Prudential Regulation Authority (No. 202655). Registered with Companies House of England and Wales No. 01575839. Registered office at 1 Aldgate, London EC3N 1 RE, UK. TME is authorised by the Luxembourg Minister of Finance and regulated by the Commissariat aux Assurances (CAA); registered with the Registre de commerce et des sociétés, Luxembourg No. B221975 at 26, Avenue de la Liberté, L-1930, Luxembourg; Operating through its Spanish Branch, domiciled at Torre Diagonal Mar, Josep Pla 2, planta 10, 08019 Barcelona, Spain, registered with the Registro de Entidades Aseguradoras de la Dirección General de Seguros y Fondos de Pensiones under the code E0236, VAT number in Spain (“N.I.F”) W0186736-E, registered with the Registro Mercantil de Barcelona, at volume 46.667, page 30, sheet number B-527127, registration entry 1; and through its German Branch, domiciled at Berliner Allee 26, 40212 Düsseldorf, Germany, registered with the Handelsregister beim Amtsgericht Düsseldorf under the number HRB 84822, authorised by the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) under the number 5217. VAT ID No: DE320932530. We have authority to enter into contracts of insurance on behalf of the Lloyd’s underwriting members of Lloyd’s Syndicate 4141 which is managed by HCCUA.

The policyholder will always be informed of which insurer in our group will underwrite the policy according to jurisdiction.

Not all coverages or products may be available in all jurisdictions. The description of coverage in these pages is for information purposes only. Actual coverages will vary based on local law requirements and the terms and conditions of the policy issued. The information described herein does not amend, or otherwise affect, the terms and conditions of any insurance policy issued by Tokio Marine HCC Group of Companies. In the event that a policy is inconsistent with the information described herein, the language of the policy will take precedence.