Top 10 Cyber Incidents 2021

This report has been produced by:

Isaac Guasch

Cyber Security Specialist

Tokio Marine HCC

Top 10
Cyber Incidents 2021

2021 has been a year of quick growth for the cyber security industry. Since the Covid-19 pandemic began, the proliferation and variety of cyber incidents have increased and so has the need to implement and heighten security.

In this report and based on our internal estimation, our in-house Cyber Security Specialist, Isaac Guasch, presents a list of 2021's most significant cyber incidents, ranging from attacks leveraging current popular trends to threats targeting governments or the travel sector. Also, read on for a "Bonus Track" on two cyber attacks that underline the need to be cyber-ready.

1 Kaseya

Worldwide IT provider

SOURCE

Impact

Systemic risk or incalculable due to Kaseya's clients' and 3rd parties' widespread use of VSA.

Description

Kaseya is a Managed Service Provider (MSP) that provides IT solutions to more than 40,000 companies worldwide. They use and provide VSA software, a unified remote monitoring and patch management tool for handling networks and endpoints.

On 2nd July 2021, Kaseya's incident response team reported a potential security incident involving this software which would potentially affect both on-premises and SaaS clients. Attackers were able to exploit a vulnerability and bypass authentication to then run an arbitrary command execution. Essentially, the attackers leveraged the standard VSA product functionality so as to deploy a ransomware known as REvil.

According to MITRE, REvil is a highly configurable ransomware family linked to the GOLD SOUTHFIELD group that has operated as ransomware-as-a-service (RaaS) since April 2019 or earlier. Main techniques used in these attacks include data encryption, data exfiltration and data destruction.

2 Microsoft Exchange

Worldwide IT provider

SOURCE

Impact

Systemic risk or incalculable due to Microsoft's clients' and 3rd parties' widespread use of Microsoft Exchange products. On 12th March, Microsoft and RiskIQ said at least 82,000 servers remained unpatched.

Description

On 2nd March 2021, Microsoft released out-of-band security updates to address vulnerabilities affecting Microsoft Exchange Server products.

On 3rd March 2021, Cybersecurity and Infrastructure Security (CISA) partners observed active exploitation of vulnerabilities in Microsoft Exchange Server products, and issued an emergency directive and an alert. Successful exploitation of these vulnerabilities allows an unauthenticated attacker to execute arbitrary code on vulnerable exchange servers, enabling the attacker to gain persistent system access, access files and mailboxes on the server and credentials stored on that system. Successful exploitation may additionally enable the attacker to compromise trust and identity in a vulnerable network.

SITA

3

Worldwide IT provider

SOURCE

Impact

This supply chain attack affected multiple Airlines, including Star Alliance members (formed by Air Canada, SWISS, Lufthansa, Turkish Airlines, Singapore Airlines, among others), KrisFlyer and hundreds of thousands of passengers.

Description

1 billion passengers per year use boarding SITA services. SITA, provides IT and telecoms services to around 2500+ customers, 1000+ airports and claims to serve around 90% of all international destinations.

On 4th March, SITA confirmed "it was the victim of a cyber attack, leading to a data security incident involving certain passenger data that was stored on SITA Passenger Service System (US) Inc. servers. Passenger Service System (US) Inc. ("SITA PSS") operates passenger processing systems for airlines. After confirmation of the seriousness of the data security incident on February 24, 2021, SITA took immediate action to contact affected SITA PSS customers and all related organisations. SITA acted swiftly and initiated targeted containment measures. The matter remains under continued investigation by SITA's Security Incident Response Team with the support of leading external experts in cyber-security."

At the moment, SITA has not confirmed the volumetry of the data leak, the airlines affected, nor is there any official confirmation from the airline's side.

Colonial

4

US top pipeline

SOURCE

Impact

Significant: In the days following the attack, the average price of a gallon of gas in the US increased to more than $3 for the first time in seven years as drivers rushed to the pumps.

Description

On 7th May 2021, America's largest "refined products" pipeline went offline after a hacking group called Darkside infiltrated it with ransomware. Colonial Pipeline covers over 5,500 miles and transports more than 100 million gallons of fuel daily. As a consequence, the attack led to shortages across the East Coast.

Attackers gained access to Colonial's network through a compromised Virtual Private Network account because of leaked passwords on the dark web. This entry point allowed hackers to deploy the ransomware attack that finally disrupted Colonial's systems.

The pipeline operator said it paid the hackers $4.4 million in cryptocurrency. On 7th June 2021, the DOJ announced it had recovered part of the ransom. US law enforcement officials were able to track the payment and take back $2.3 million using a private key for a cryptocurrency wallet.

Pichincha

5

Ecuador's largest bank

SOURCE

Impact

Business interruption of Ecuador's largest bank and partial operation for more than a week.

Description

In early October 2021, Ecuador's largest private bank, Banco Pichincha, confirmed they suffered a cyber attack that disrupted operations and took its ATM and online banking portal offline. They were partially operative while ensuring the ATMs were functioning again by 11th October. Although Banco Pichincha has not publicly disclosed the nature of the attack, a cybersecurity analyst said that it is a ransomware attack with threat actors installing a Cobalt Strike beacon on the network.

Cobalt Strike is a very common red team tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". However, this tool is also commonly used by ransomware gangs and other threat actors to gain persistence and access other systems on a network.

In February, Banco Pichincha suffered another cyber attack by cybercriminals known as Hotarus Corp who claimed to have stolen files from the bank's network.

Belarusian

6

SOURCE

Impact

Massive data leak of Belarusian citizens, from cross-border controls, emergency calls history and police database.

Description

On 8th November 2021, in light of the international tension against Belarus's authoritarian regime, the hacking group Belarusian Cyber-Partisans claimed to access the full database of those crossing the country's borders. This would include the alleged movements of KGB officers and president Alexander Lukashenko himself. The data leaked concerned not only Belarus citizens but also other nationals crossing the Belarusian border either by air, rail, road or foot. The group's previous leaks have proved instrumental in helping justify international sanctions against the regime.

The hacked data included the entire police database, comprising of CCTV footage and the employment history of officers, as well as the tapped phone calls of regime supporters and opponents. Also included were the personal details of every Belarusian citizen, their passport photos, home addresses, and workplaces, plus the last 10 years of emergency call history, including those made by people reporting their co-workers for opposing the regime.

Poly Network

Cryptocurrency

7

SOURCE

Impact

$610 million in cryptocurrencies. This was the largest security incident in DeFi (Decentralized finance) history in terms of the value stolen.

Description

Poly Network facilitates exchange between several blockchains as users trade one cryptocurrency for another, such as trading Bitcoin for Ether. More specifically, Poly Network is an interoperability protocol for heterogeneous blockchains, which lets users swap tokens from one digital ledger to another.

On 10th August 2021, Poly Network suffered an anonymous attack in which over $610 million in cryptocurrencies was stolen.

Tokens are swapped between blockchains using a smart contract which contains instructions on when to release the assets to the counterparties. According to an analysis of the transactions, the hackers appeared to override the contract instructions for each of the three blockchains and diverted the funds to three wallet addresses, which are digital locations for storing tokens. The attacker(s) stole funds in more than 12 different cryptocurrencies, including Ether and a type of bitcoin, according to blockchain forensics company, Chainalysis.

Eventually, all assets were returned to Poly Network on 19th August, according to its official Twitter profile, putting some uncertainty on the real intentions of the attacker.

RENAPER

Argentinian ID database

8

SOURCE

Impact:

Records of potentially 45 million Argentinian citizens stolen.

Description

RENAPER is Argentina's National Registry of Persons and the official system used for issuing national ID cards to all citizens. It is also referenced by other national agencies for personal information queries.

On 9th October 2021, a hacker tweeted that they had breached the government's IT network and stolen the entire population's ID card details; data that is now being sold in private circles. In an official press release, the Ministry of Interior confirmed that the attacker published 44 pictures of individuals including celebrities and public employees. According to the official version and after the initial analysis, authorities claimed that "the database did not suffer any data breach or leak".

However, the same attacker published a probe of the data and claimed to have all the records of the 45M estimated population, threatening to publish all the information and continue selling the data to interested buyers.

Apache Log4j 9

Software component

SOURCE

Impact

Systemic risk or incalculable due to the widespread use of Log4j library in millions of products or app components.

Description

On 9th December 2021, a zero-day vulnerability known as Log4j or Log4Shell was released.

The vulnerability affects a popular open-source library (Apache Log4j2 2.14.1 and its prior versions) to log user inputs across multiple use cases. This Log4j library is used in configuration, log messages and parameters, and uses the Java Naming and Directory Interface (JNDI) to look for data and resources in a directory service. This feature could allow an attacker controlling log messages to execute arbitrary code and could also allow an unauthorised user to gain elevated privileges on a remote computer.

Log4j is present in a huge amount of in-house and market software solutions and widely used in countless app components. The vulnerable code also affects some of the prominent IT service companies and tech vendors such as Amazon Web Services, Oracle, Cisco, IBM, Fortinet or VMware (to name some), making it extremely critical from a risk concentration point of view, which can result in a Single Point of Failure (SPoF) for many sectors.

Volkswagen USA 10

SOURCE

Impact

Data breach impacting over 3.3 million customers from United States and Canada. This included information gathered for sales and marketing purposes from 2014 to 2019.

Description

On 10th March 2021, Audi and Volkswagen were alerted to the fact that an unauthorized third party may have obtained certain customer information. Audi and Volkswagen immediately commenced an investigation to determine the nature and scope of this event.

The investigation confirmed that, in early May 2021, a third party obtained limited personal information received from or about customers and interested buyers from a vendor used by Audi, Volkswagen, and some authorised dealers in the United States and Canada.

While the investigation continues, Audi and Volkswagen believe that the majority of affected data includes some or all of the following contact information: first and last name, personal or business mailing address, email address, or phone number. In some instances, the data also included information about a vehicle purchased, leased, or enquired about.

> “2021 has taught us that resilience testing and a well-planned defence is paramount”
>
> - Isaac Guasch

Bonus Track

Last year we listed 10 of the top actors and activity showing cyber-criminal groups, using our Cyber Threat Intelligence tools. This year, we want to highlight two cases that caught our attention, and that emphasize the growing impact of cyber threat activity on enterprise risk across all industry segments.

1 Emotet is back

Emotet, "the world's most dangerous malware", was taken down by a major international police operation in 2021. However, it is allegedly now back in operation.

Emotet first appeared online as a banking trojan, and in 2016 became a malware loader designed to infect a victim and then download (or load) other malware. This change in its codebase meant that it was able to allow other malware gangs to rent access to infected computers.

One of the things that made Emotet so popular and dangerous was the fact that it was offered to other cyber-criminal groups to perpetrate their attacks, as a kind of "Attack as a Service" model. Different threat actors used Emotet malware as an entry door to their victims to later deploy other types of malware of their own.

In January 2021, EUROPOL confirmed that law enforcement and judicial authorities worldwide took down the Emotet botnet in an internationally coordinated action between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine lead by EUROPOL and EUROJUST.

The disruption of Emotet's operations was extremely complex as the botnet used a very sophisticated and resilient infrastructure based on a huge number of servers located worldwide that protected it against takedown attempts.

However, in late 2021, various researchers from cybersecurity companies discovered a re-incarnation of Emotet. More specifically, it was observed that another well-known malware botnet Trickbot, was being used to spread and install Emotet on infected Windows systems again. The same groups of researchers confirmed that specific Emotet DLL were detected in several systems and found to be circulating as email attachments in the form of Microsoft Excel spreadsheets, Microsoft Word documents, and password-protected zip files containing a Word document. Furthermore, this use of email has evolved beyond one-time phishing emails, instead using data from stolen email chains (presumably gathered from previously infected Windows hosts) to send a spoof reply to a current email chain.

In conclusion, and despite the extreme effort and advanced police operation, all evidence points towards Emotet threatening the cyber space once again in 2022.

Sources

- https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
- https://www.zdnet.com/article/emotet-once-the-worlds-most-dangerous-malware-is-back/

2 REvil disappearance

Another example of huge effort made by the authorities is the (forced) disappearance of REvil, thanks to a police operation carried out by the FBI.

As mentioned, and according to MITRE, REvil is a highly configurable ransomware family linked to the GOLD SOUTHFIELD group that has operated as ransomware-as-a-service (RaaS) since April 2019 or earlier. REvil is highly configurable and shares code similarities with the GandCrab RaaS.

To illustrate its harmful potential, some of the cyber incidents named previously in this report, like Colonial or Kaseya, have involved a REvil attack, with systemic consequences in the case of the latter. Furthermore, JBS USA, one of the biggest food producers and #1 global beef producer, also confirmed that they were hit by this ransomware and stated that they paid USD $11 million in ransom.

During this period, REvil activities were closely followed and investigated by the FBI and in October the group vanished. The U.S. Department of Justice arrested a Ukrainian citizen and a Russian national, seizing $6.1 million tied to ransomware payments. Both were charged with conspiracy to commit fraud and intentional damage to a protected computer.

According to three private sector cyber experts working with the United States and one former official, this operation was performed thanks to a multi-country operation that was able to hack the group itself and force them offline.

“The FBI, in conjunction with Cyber Command, the Secret Service and like-minded countries, have truly engaged in significant disruptive actions against these groups,” said Kellermann, an adviser to the U.S. Secret Service on cybercrime investigations.

In the days following the take-down, a leadership figure known as “0_neday,” who had helped restart the group’s operations after an earlier shutdown, said REvil’s servers had been hacked by an unnamed party.

Now only time will tell whether this will be the end of REvil.

Sources

https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9

Find out more about our Cyber Security Insurance:

TMHCC Cyber Insurance

Email our Cyber Security Team

This report has been produced by:

Isaac Guasch Garcia

iguasch@tmhcc.com

Isaac Guasch
Cyber Security Specialist
Tokio Marine HCC

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.