Top 10 Cyber Incidents 2020

This report has been produced by:

Isaac Guasch

Cyber Security Specialist

Tokio Marine HCC

TOKIO MARINE HCC

Top 10 Cyber Incidents 2020

2020 has been an unprecedented year, and as such has given rise to a number of serious cyber incidents of all types; indiscriminate of geography and industry sector.

In this report and based on our internal estimation, Isaac Guasch, our in-house Cyber Security Specialist, has compiled a list of the worst and most significant cyber incidents from 2020 in terms of financial impact and reputational damage. They outline just how active cyber criminals are, how devastating attacks can be and how important it is to know how to manage and prepare for this increasingly prolific risk and its various disguises. Also, read on for a "Bonus Track" listing of top actors and activity.

1 SolarWinds

(FireEye, Microsoft, Nvidia, Cisco, US Government, …)

SOURCE

Impact

Unpredictable. Known victims include: the US Government and Military, Consultancy, Accountancy, Technology, Telecoms firms, as well as the Education sector. The attack has a global reach, affecting North America, Europe, Asia and the Middle East.

Description

Leading provider of IT infrastructure management software SolarWinds have announced that vulnerabilities within their Orion products (versions 2019.4 through to 2020.2.1 HF1) are currently being exploited by malicious actors. Nicknamed the "Sunburst attack", initial compromise is estimated to have begun as early as Spring 2020 and is ongoing today.

2 COVID-19 Scams

SOURCE

Impact

Unpredictable. Several groups working to fight the coronavirus pandemic, including the WHO, NIH, the US Centers for Disease Control and Prevention (CDC), and the Gates Foundation.

Description

Email phishing attacks have spiked over 600% since the end of February 2020 due to Coronavirus pandemic. Additionally, as the race to obtain the Covid vaccine progressed, numerous attacks on various companies in the supply chain have been detected. According to an IBM report, "this calculated operation started in September 2020. The COVID-19 phishing campaign spanned across six countries and targeted organizations likely associated with Gavi, The Vaccine Alliance's Cold Chain Equipment Optimization Platform (CCEOP) program […]. While firm attribution could not be established for this campaign, the precision targeting of executives and key global organizations hold the potential hallmarks of nation-state tradecraft."

3 Cognizant Technology Solutions Corp

SOURCE

Impact

Disruption of client services, revenue and impact on margins.
The company paid $50-70 M for ransom.

Description

On April 18, 2020, Cognizant Technology Solutions (CTS), was hit by Maze ransomware cyber-attack, which resulted in service disruption of company's clients.

The tech giant confirmed the breach on its website. It took steps to contain the cybersecurity incident and notified its clients about the breach and measures to take to further secure their systems. During a ransomware data breach attack, attackers generally infect the company's systems with the virus, steal the data, and demand payment from the company to restore the data. But, in case of Cognizant Maze ransomware, attackers threatened the company to pay the ransom or they would publish the breached information online.

4 Energias de Portugal (EDP)

SOURCE

Impact

10 TB data stolen, and $10.9 M demanded.

Description

The Portuguese multinational energy company, Energias de Portugal (EDP) faced one of the most threatening cybersecurity incident in April 2020.

A ransomware attack, named RagnarLocker successfully targeted EDP. The cyber-attackers demanded a ransom of $10.9 million to unlock its files. The files contained critical data, including contracts, billing details, transactions, client's and partner's personal details like names, passwords, etc. In a ransom note on the site, the hackers claimed that they will publish the information on public blogs or websites if the ransom goes unpaid.
The energy firm, however, has not disclosed if they paid the ransom, or steps that it took to investigate the attack.

5 MGM Hotel

SOURCE

Impact

Details of over 10.6 million users revealed.

Description

In February 2020, the personal details of more than 10.6 million guests who stayed at MGM Resorts hotels were leaked on a hacking forum. The information leaked included names, phone numbers, addresses, birth dates, and email addresses of users ranging from tourists, CEOs, celebrities, and government employees. However, the details of the credit cards were not breached. This cybersecurity incident started in the mid of 2019. Then, the MGM employees discovered unauthorized access to a server. From that day, the stolen information was being shared in several hacking forums. After the cybersecurity incident got revealed, immediately MGM notified the impacted individuals. In February, once again there was a data breach and as a result, information of MGM hotel users was published openly, on an accessible forum.

6 Zoom App

SOURCE

Impact

Reputation and brand image damaged.

Description

In April 2020, Zoom, a famous video conferencing app, suffered an attack called Zoombombing.

A vulnerability in Zoom allow people with bad intentions to join the private meetings, read conversations, and screen share images of whatever they wanted, mainly sort of offensive, like adult or shock videos. The company later updated its iOS app to stop sending user data to Facebook. Zoom later improved the security of their Zoom meetings as well.

7 Marriott

SOURCE

Impact

Approximately 5.2 million hotel guests data. Marriott is one of the largest hotel brands with 7,300 hotel and resort properties in 134 countries.

Description

In its second significant data breach within two years, Marriott revealed that personal details of approximately 5.2 million hotel guests were fraudulently accessed in 2020. The personally identifiable information taken included names, addresses, phone numbers, birth-dates and airline loyalty information. Hackers often target hotel chains both to sell personal information of guests and to track the travel of government officials with security clearances and business leaders. The company said the guest information was hacked in mid-January via login credentials of employees at a franchised property and it was alerted to the incident at the end of February. Marriott disabled those logins and is supporting authorities in the investigation. According to a statement from Marriott, they do not believe the data breach affected their Marriott Bonvoy account passwords or PINs, payment card information, address, emails, passport information, or driver's license numbers.

8 Experian

SOURCE

Impact:

Records of 24 million people and 793,749 businesses' data stolen.

Description

Experian, a consumer credit reporting agency, suffered a major breach, impacting nearly 24 million South African consumers and about 793,749 business entities in August 2020.

The agency further revealed that an individual fraudulently claiming to be one of its clients requested services from the company, prompting the release of the information. Soon, after the breach, the company reported the incident to the local authorities. Eventually, the misappropriated data was secured and deleted. Experian said that the data was not used for fraudulent purposes before being deleted. Also, it further said the cybersecurity incident did not compromise its own infrastructure, systems, and customer database.

9 Twitter

SOURCE

Impact

Reputation and brand image damaged.

Description

Some of the most recognized and highly regarded global Twitter handles were compromised and used to fraudulently tweet about Bitcoin. The accounts requested Bitcoin from their followers, promising double in return. Even though the tweets were only live for a short time, they generated Bitcoin worth more than US $100,000. Those duped into sending Bitcoin received nothing in return. Perpetrators used a phone spear phishing attack to obtain the credentials of Twitter employees who had access to internal support tools, and they targeted 130 Twitter accounts, successfully tweeting from 45, accessing the direct messages inbox of 36 and downloading the Twitter data of seven. Twitter issued a statement saying "We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools. We have locked accounts that were compromised and will restore access to the original account owner only when we are certain we can do so securely."

10 Garmin

SOURCE

Impact

Service disruption and economic extortion.

Description

Garmin announced it was the victim of a cyberattack that encrypted some of its systems. As a result, many of its online services were interrupted, including website functions, customer support, customer-facing applications, and company communications.

The company publicly said that they had no indication that any customer data, including payment information from Garmin Pay™, was accessed, lost or stolen. However, Garmin's press release confirmed that the ability to access online services was affected. Even though they started restoring the affected systems after the cyberattack, they expected to return to normal operation over the next few days.

Globally, cybercrime damages are expected to reach US $6 trillion in 2021.

Bonus Track

Using our Cyber Threat Intelligence tools, here is a listing of top actors and activity showing the types of existing cyber-criminal groups that are currently active and their motivations. Being aware of activity, groups, motivations and incidents not only highlights the need for prioritising Cyber Security as an essential part of any company's risk management strategy, but also helps outline considerations for resilience testing and a well-planned defence.

1 FIN 7

FIN 7 is a financially motivated intrusion set that selectively targets victims and uses spear phishing to distribute its malware. It has been observed that this group attempts to compromise diverse organizations for malicious operations involving the deployment of point-of-sale (POS) malware.

2 FIN 11

FIN 11 is a financially motivated threat group that has conducted some of the largest and longest running malware distribution campaigns observed amongst our FIN groups to date. The group has been active since at least 2016, but identified overlaps with TA505 activity suggests they may have been conducting operations as early as 2014. In addition to their high-volume spam campaigns, FIN11 is also notable due to their consistent evolvement of malware delivery tactics and techniques.

3 FIN 8

FIN 8 is a persistent, financially motivated set of network intrusion set whose operators have used relatively sophisticated network compromise tactics and have repeatedly deployed the PUNCHTRACK point-of-sale (POS) malware. The actors behind these intrusions are unknown, but close similarities across the intrusions that have been associated with FIN8 are strongly indicative of common operators.

4 UNC1878

UNC1878 is a financially motivated group that monetizes their intrusions by extorting their victims following the deployment of RYUK ransomware. UNC1878 has used various offensive security tools, most commonly Cobalt Strike BEACON, along with legitimate tools and built-in commands such as PSEXEC, WMI, and BITSadmin.

5 UNC2053

UNC2053 is a financially motivated cluster of activity that encompasses the use of various loader and backdoor combinations that are distinct but share a common networking protocol. Regularly, it has been observed these campaigns incorporating new delivery tactics and it is plausible that UNC2053 relies on multiple partners for distribution. There is a high confidence that common actors are behind the development of TrickBot and these families. UNC2053 appears to partner with multiple threat actors who leverage access obtained by UNC2053 to subsequently deploy ransomware.

6 APT41

APT41 is a Chinese state-sponsored espionage group that also conducts financially motivated activity for personal gain. The group has been active since at least 2012 and has conducted espionage operations against healthcare, high-tech, and telecommunications organizations. APT41 also carried out operations against the video game industry for financially motivated intrusions as well as to steal source code and digital certificates. The group executed multiple supply chain compromises, gaining access to software companies to inject malicious code into legitimate files before distributing updates.

7 FIN 6

FIN 6 is a financially motivated intrusion set that has operated since at least mid-2014. The intrusion set has compromised multiple point-of-sale (POS) environments through the use of TRINITY (aka "FrameworkPOS") POS malware and more recently SCRAPMINT to steal payment card data. Since early 2017, it has been observed an expansion of TTPs, indicating that the intrusion set is also targeting card-not-present (CNP) data in eCommerce environments. In numerous cases, data stolen through these intrusions has been monetized through the Joker's Stash card shop. As of mid-2018, at least one FIN6-affiliated actor began to deploy various ransomware payloads, including LockerGoga, Ryuk, MegaCortex, and Maze malware. In addition to the use of publicly available tools such as Metasploit and Cobalt Strike, FIN6 commonly leverages SQUIDSLEEP and SQUIDGATE malware sold by the actor "badbullzvenom."

8 TEMP.Overboard

TEMP.Overboard is a Chinese cyber espionage operation most likely based in Wuhan and best known for spear-phishing campaigns delivering TSCOOKIE and closely related malware payloads. The group typically leverages weaponized documents in spear-phishing emails that are tailored to targets of interest via social engineering tactics. Historic and recent activity demonstrates that the group remains a consistent threat to government-related functions and industries including telecoms and technology companies, especially in East Asia.

9 ATP34

ATP 34 is a cyber espionage group with a nexus to Iran that has been operational since at least 2014. It is believed APT34 conducts operations largely focused on phishing efforts to benefit Iranian nation-state interests. This threat group has conducted broad targeting across a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East, but has targeted North American and European organizations. It is assessed that APT34 works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.

10 UNC2452

UNC2452 is a sophisticated group that has targeted government and private sector entities worldwide. They have employed numerous unique capabilities, including gaining initial access through as software supply chain vulnerability. After gaining access to a victim network, UNC2452 has a light malware footprint, often leveraging legitimate credentials to access data and move laterally.

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

Tokio Marine HCC - Financial Lines

A member of the Tokio Marine HCC group of companies