AmericanAg™
Reinsuring your world

Article

Major Cyber Incidents of 2020

This past year has left its mark in many ways. Major data breaches were among the many events and trends impacting business in 2020. According to a study conducted by the University of Maryland, hacking attacks occurred on average 2,244 times per day, which is every 39 seconds.[1] Organized crime groups were responsible for 55% of breaches,[2] and large breaches involving the cloud are becoming more and more commonplace.

Let's take a look at some of the key incidents of cybercrime that made the headlines in 2020.

Travelex Attack

Target: Travelex

In January, the foreign exchange company Travelex, which owns kiosks all over the globe, announced that they had been attacked by the REvil ransomware group, which demanded a $6 million ransom. This attack impacted 17,000 customers[3], and the company's reputation took a hit. The damage also affected banks such as Barclays, Royal Bank of Scotland, and HSBC, as they were unable to fulfill foreign currency orders for their customers. The hackers told the media that they had downloaded five gigabytes of sensitive customer data.[4]

Microsoft Data Breach

Target: Microsoft

In January, Microsoft disclosed a data breach occurring from a change made to the network security group that allowed misconfigured security rules to expose data. This breach affected 250 million records containing information such as email addresses, IP addresses, and support case details.[5] Microsoft later reported that their investigation found no malicious use, and most customers did not have personally identifiable information that was exposed.[6]

[1] Cukier, Michel, "Study: Hackers Attack Every 39 Seconds," A. James Clark School of Engineering, University of Maryland, accessed December 2020, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.
[2] "Summary of Findings: Verizon Data Breach Investigations Report," Verizon, accessed December 2020, https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/.
[3] Tsang, Amie, "Hackers Cripple Airport Currency Exchanges, Seeking $6 Million Ransom," The New York Times, January 9, 2020, https://www.nytimes.com/2020/01/09/business/travelex-hack-ransomware.html.
[4] Tidy, Joe, "Travelex: Banks halt currency service after cyber-attack," BBC News, January 8, 2020, https://www.bbc.com/news/business-51034731.
[5] MSRC Team, "Access Misconfiguration for Customer Support Database," Microsoft Security Response Center, January 22, 2020, https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/
[6] MSRC Team, "Access Misconfiguration for Customer Support Database."

Marriott Data Breach

Target: Marriott International

At the end of February, the login information of two Marriott employees was obtained by hackers. Guest information such as names, addresses, birthdates, telephone numbers, loyalty account information, personal details, partnerships, and affiliations was obtained and leaked in early 2020, impacting 5.2 million people.[7] Just two years prior in 2018, the hotel chain had announced another data breach affecting 500 million guests.[8]

DarkHotel WHO Phishing

Target: World Health Organization (WHO)

In February, advanced attackers and dedicated criminal gangs created a website that mimicked the WHO's email service and attempted to steal user passwords. It is suspected that hackers intended to later pose as the United Nations specialized agency to steal money and sensitive information. Public fear and vulnerability during the coronavirus pandemic likely served as motivation for the criminals.

Twitter Bitcoin Hack

Target: Twitter/Bitcoin Community

In July, bad actors gained access to accounts maintained by Twitter employees and scraped their passwords. After gaining improper access to the passwords, the bad actors were able to utilize Twitter accounts to disseminate false information and add credibility to a Bitcoin scam. Key takeaways: the human element is a key area of risk and anything a business might have could be valuable to attackers.[9]

Garmin Ransomware Attack

Target: Garmin Ltd.

This leading GPS company was attacked in August, likely by the group Evil Corp., which installed WastedLocker ransomware on Garmin systems through email, unpatched vulnerabilities, and remote desktop protocol. This led to an outage affecting internal systems and product usability. It is suspected (but not confirmed) that Garmin paid the requested $10M ransom.[10] This serves as yet another example of how ransomware continues to target businesses and exploit any opening.

[7] "Marriott Data Breach 2020: 5.2 Million Guest Records were Stolen," Security Boulevard, April 13, 2020, https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/.
[8] "Marriott Announces Starwood Guest Reservation Database Security Incident," Marriott International News Center, November 30, 2018, https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/.
[9] "2020 Breaches in Review," webinar from Arctic Wolf Networks, Eden Prairie, MN, December 16, 2020.
[10] "2020 Breaches in Review," webinar from Arctic Wolf Networks.

SANS Institute Consent Phishing

Target: SANS Institute

SANS Institutes is a leading cybersecurity training company, with over 165,000 trained security professions. In August, nearly 30,000 records of personally identifiable information (PII) were exfiltrated from the company's systems through a malicious Office 365 add-on installed by a legitimate user. With this attack on cybersecurity company, it's evident that everyone can be breached and organizations should invest in adequate detection and response.[11]

Las Vegas Schools Ransomware Attack

Target: Clark County School District (CCSD)

CCSD – the 5th largest school district in the US, with over 300K students[12] – was attacked by the "Maze" ransomware gang on the first day of school. Through email, unpatched vulnerabilities, and remote desktop protocol, the ransomware attacks severely disrupted operations as students were returning to class. Student data was later found available and unsecured on the dark web. This case demonstrates that when cybercriminals threaten to publicly release sensitive data, organizations should assume that they can and will follow through with their threat.

FBI Healthcare Warning

Target: US Healthcare Industry

In October, the FBI and the Cybersecurity & Infrastructure Security Agency (CISA) issued a joint warning about major expected attacks on US healthcare organizations. Specifically, the warning identified the TrickBot malware as the attack vector, and Ryuk and Conti as the ransomware payload to be used. The US healthcare industry is a $3.3 trillion industry with over one million doctors and thousands of hospitals, practices, facilities, and labs.[13] This plot shows us that ransomware will continue to target all different types of businesses. Advanced attackers will exploit any opening, and the cost to impacted businesses could include anything a company could physically pay to survive.

[11] Barth, Bradley, "SANS Institute breach proves anyone can fall victim to a 'consent phishing' scam," SC Media, August 13, 2020, https://www.scmagazine.com/home/security-news/data-breach/sans-institute-breach-proves-anyone-can-fall-victim-to-a-consent-phishing-scam/

[12] Arctic Wolf, "2020 Data Breaches in Review," accessed December 2020. https://arcticwolf.com/resources/analyst-reports/2020-data-breaches-in-review.

[13] "2020 Breaches in Review," webinar from Arctic Wolf Networks.

COVID Vaccine Attacks

Target: The Vaccine Research Industry

Vaccine research was a $46.88 billion industry in 2019,[14] and in 2020 it was a large target for cybercrime, as hackers attempted to compromise the COVID-19 vaccine development efforts. Threats came from both advanced attackers and Advanced Persistent Threat (APT) hackers – usually state-sponsored groups that gain unauthorized access to a computer network but remain undetected for an extended period of time. In December, US drugmaker Pfizer and partner BioNTech announced that documents related to the development of their COVID-19 vaccine had been "unlawfully accessed" in an attack, although they also specified that they did not believe any personal data of trial participants had been compromised.[15] The key lessons learned from these attacks include the need to address existing vulnerabilities and prioritize detection.

SolarWinds Attack

Target: Numerous US Government Agencies

Suspected Russian-linked hackers were able to get 18,000 government and private organizations, including 250 federal agencies and departments,[16] to download tainted software to allow them to infiltrate the government systems. Among the affected were the departments of Commerce, Homeland Security, and Agriculture. The complexity of the attack will likely have officials continuing to investigate for months to come.

Key Takeaways

The volume and sophistication of the 2020 cyber incidents provide some valuable insights. It is increasingly clear that all businesses are at risk from a cyber-attack, regardless of size, location, or type of operation. Ransomware will continue to evolve – criminals are sophisticated, and plots are getting increasingly intricate as time goes on. Additionally, remote work and the increased reliance on the cloud present a growing exposure. Cyber crime is far from going away, and targeted attacks are only expected to evolve in both frequency and severity throughout 2021.

With that, cyber insurance can play an important role. A solid cyber insurance policy not only provides coverage for multiple events and situations but also ensures peace of mind. At AmericanAg™, we understand the cyber exposures your customers face with their business and farming operations. Cyber Coverage from AmericanAg™ can help you protect them from the impact – so that they can focus on running their business or farming operation.

If you would like more information, please contact Sarah Kuhn, Research & Product Development Analyst, at skuhn@aaic.com or (847) 969-1009.

---

[14] "2020 Breaches in Review," webinar from Arctic Wolf Networks.
[15] Stubbs, Jack, "Hackers steal Pfizer/BioNTech COVID-19 vaccine data in Europe, companies say," Reuters, December 9, 2020, https://www.reuters.com/article/us-ema-cyber/hackers-steal-pfizer-biontech-covid-19-vaccine-data-in-europe-companies-say-idUSKBN28J2Q7.
[16] Schneier, Bruce, "The SolarWinds hack is stunning. Here's what should be done," CNN, January 5, 2021, https://www.cnn.com/2021/01/05/opinions/solarwinds-hack-what-should-be-done-schneier/index.html.

References

"2020 Breaches in Review." Webinar from Arctic Wolf Networks. Eden Prairie, MN, December 16, 2020.

Arctic Wolf. "2020 Data Breaches in Review," accessed December 2020. https://arcticwolf.com/resources/analyst-reports/2020-data-breaches-in-review.

Barth, Bradley. "SANS Institute breach proves anyone can fall victim to a 'consent phishing' scam," SC Media, August 13, 2020. https://www.scmagazine.com/home/security-news/data-breach/sans-institute-breach-proves-anyone-can-fall-victim-to-a-consent-phishing-scam/.

Cukier, Michel. "Study: Hackers Attack Every 39 Seconds." A. James Clark School of Engineering, University of Maryland, accessed December 2020. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

"Marriott Announces Starwood Guest Reservation Database Security Incident." Marriott International News Center, November 30, 2018. https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/.

"Marriott Data Breach 2020: 5.2 Million Guest Records were Stolen," Security Boulevard, April 13, 2020, https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/.

MSRC Team. "Access Misconfiguration for Customer Support Database." Microsoft Security Response Center, January 22, 2020. https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/.

Schneier, Bruce. "The SolarWinds hack is stunning. Here's what should be done," CNN, January 5, 2021. https://www.cnn.com/2021/01/05/opinions/solarwinds-hack-what-should-be-done-schneier/index.html.

Stubbs, Jack. "Hackers steal Pfizer/BioNTech COVID-19 vaccine data in Europe, companies say." Reuters, December 9, 2020. https://www.reuters.com/article/us-ema-cyber/hackers-steal-pfizer-biontech-covid-19-vaccine-data-in-europe-companies-say-idUSKBN28J2Q7.

"Summary of Findings: Verizon Data Breach Investigations Report." Verizon, accessed December 2020. https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/.

Tidy, Joe. "Travelex: Banks halt currency service after cyber-attack." BBC News, January 8, 2020. https://www.bbc.com/news/business-51034731.

Tsang, Amie. "Hackers Cripple Airport Currency Exchanges, Seeking $6 Million Ransom." The New York Times, January 9, 2020. https://www.nytimes.com/2020/01/09/business/travelex-hack-ransomware.html.