8 Alarming Cyber Attacks That Made Corporates Go Bonkers In The Last Ten Years: A Decade In Review!

Posted on February 4, 2020

“If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.”
Former American Govt. Official Richard A. Clarke

This statement might evoke sarcasm, but is apt in the contemporary vulnerable cyberspace that’s full of hackers with malicious purposes. The tech-driven economy has made it mandatory for big corporates, as well as small businesses, to leverage digital solutions, but breaches and cybercrimes have become a sheer nightmare for them.

Little difficult to gulp this down, right? But as per the Clark School study by the University of Maryland, on an average, there is at least 1 hacking attempt executed on systems with internet connectivity every 39 seconds! Now, that’s simply shocking.

Moreover, 2019 has been worse in terms of breach activities as published in a report from Risk Based Security, which states that approximately 3,813 breaches were documented through June 30, putting more than 4.1 billion files at stake. But what was even more frightening is that the number of reported breaches was up 54% in comparison to the midyear of 2018.

Was that an accidental increase? No, the rise in the amount of cybercrimes has been gradually increasing & is believed to only grow further in the coming years. To understand the present situation, first let’s get a little idea on the history of cybercrimes.

Want To Know The Story Behind Cyber Crimes? Let’s Get Rolling Then!

According to The History Of Hacking, in 1878 the victim of hacking attempts weren’t computers but telephones and the criminals were some odd teenage boys who tried misdirecting or disconnecting calls while running the switchboards and were termed as practical jokers and not even hackers.

However, as per Tripwire the very first attempt to something that’s close to hacking was spotted in

the 1970s, when computerized phones became the target of the criminals who injected malicious series of codes to find a way to pay for long-distance calls.

The 1990s can be called as the decade when some of the very first cyber criminals like Robert Morris, Kevin Mitnick, Vladimir Levin, and Kevin Poulsen were arrested, as well, convicted for stealing proprietary software from giant organizations and introducing the first computer worm.

Hacking saw a new surge in the 2000s as cybercriminals targeted government bodies and big brands like Microsoft and Amazon with the help of more sophisticated attacks. But in comparison to all the previous decades, the last has been the master of all. In fact, from 2006 to 2019 itself, data breaches increased by 160%, with an average data breach costing 3.92 million in 2019!

On that note, we have compiled a list of the top data breaches that occurred in the past decade taking into account not only the number of records compromised, but also, on the damage or impact the attack had on the organization, its employees, stakeholders, partners, and of course its users.

8 Biggest Breaches of the Decade!

1. Yahoo: The Worst Of All

Yahoo has been one of the biggest victims of data breaches in the last decade. The giant reported 500 million user accounts have been compromised in 2014 and above 1 billion in 2013, according to The New York Times. Yahoo later confirmed in October 2017, that all 3 billion of its user accounts were impacted!

This data breach was considered as one of the biggest in the history of cybercrime. Also, these attacks brought along a fundamental shift in the business partnership of Yahoo with Verizon, where the latter paid for the losses incurred due to these breaches and removed roughly $400

million from the buying price.

2. eBay: One Of The Most Mysterious Cyber Crimes Ever

In May 2014, the E-commerce brand became a victim of hacking and the impact was that 145 million users got compromised. As per Washington Post hackers gained illegal access to eBay employees' login details for 229 days and then grabbed the credentials of millions of users.

As per SC Media, eBay made 84% of its users to reset their login credentials because of this instance. Although, the company has never revealed the exact details of the attacks but they have somehow managed to sustain their commerce volume.

3. Marriott International: The Breach That Caused A Massive Six Point Drop In The Giant's Market Shares

The hotel and hospitality brand had been a constant victim of hacking from 2014-18, exposing 500 million customers data. Starwood hotel chain was the first victim of the cyber attacks that retained in the systems after Marriott acquired the former in 2016 and got spotted two years later in 2018.

As per CSO Online, hackers were able to fetch the personal information of customers such as the contact details, travel info, guest numbers of the Starwood Hotels, passport numbers, etc.

However, Marriott claimed that the credit card details like the expiry date and card numbers of 100 million customers also got stolen in the breach. The New York Times published that these attacks were planned by the Chinese hackers functioning under one of their intelligence-gathering missions.

4. Equifax: The Carelessness Of An Employee Exposed The Sensitive Data Of Millions Of Customers

The US credit brand found out in 2017 that approx. 147 million customers' credentials have been compromised by hackers. These details include their names, addresses, driver's license numbers, credit card credentials, passport numbers, etc.

The ex-CEO of Equifax, Richard Smith confessed that these breaches happened due to the carelessness of one of their employees who failed to process an important update that resulted in an application vulnerability on one of their websites. Watch the video to know more!

5. Adobe: Another Corporate Giant Came Under The Radar Of Cyber Criminals In 2013

Adobe's IT infrastructure got hacked big time and the giant announced the same officially in October 2013, quoting that it compromised 3 million user accounts but later revised the number to 38 million. To make matters worse, a file containing 7.5 million usernames and hashed passwords appeared online.

According to The Verge the criminals targeted many things but primarily they managed to hack:

- Various invalid Adobe IDs
- Test account data
- Adobe IDs that were inactive
- Adobe IDs with invalid encrypted passwords

Besides this, the source code for Photoshop was stolen, along with, user credentials such as the names, logins, credit card details, etc. in this hack.

6. Target Stores: The Worst Thanksgiving Gift The Organization Could Ever Have Gotten!

In 2013, just before Thanksgiving, hackers began to target the company but it came to their attention only in January 2014. As per Forbes, the breaches impacted 70 million people, wherein the cyber attackers leveraged a third-party HVAC vendor and gained illicit access to Target's point-of-sale payment card readers across all 1,800 U.S. stores.

Hackers stole the Personally Identifiable Information (PII) of the users that included their names, emails, contact numbers, and physical addresses. The breaches came at the cost of the company's CIO and CEO's resignation. However, as per CSO Online, a settlement in 2017 was announced that promised the tightening of Target's security infrastructure within 180 days.

7. Friend Finder Network: A Breach That Impacted 412.2 Million User Accounts

2016 proved to be the worst year for this casual hookup and friend finding platform as cybercriminals hacked 412.2 million user accounts by penetrating 6 databases of the Friend Finder Networks including AdultFriendFinder.com, Cams.com, Penthouse.com, Stripshow.com, iCams.com & an unknown domain and grabbed user information like names, email addresses, and passwords.

As per ZDNet, the hackers primarily managed to gain access to the pseudonyms, IP addresses, birth details, postal codes, and the sexual orientations of the users. Also, many deleted accounts were spotted in the breach that exhibited the company's poor security practices and outdated IT infrastructure.

One shocking thing about this particular breach was that the hacked account details got exploded

on the dark web in the form of spreadsheets that spilled secrets like if the user was gay or straight and whether they're involved in extramarital affair.

Public circulation of private information created anxiety amongst the site's users and many of them even warned others to be cautious of blackmailing attempts. According to a report from Channel 4 News a couple of the leaked email addresses were found to be owned by some government officials and armed services professionals.

8. Anthem Blue Cross: The Biggest Healthcare Cyber Crime Victim Of All Times

The last decade has proved to be even worse for the healthcare niche as there were a couple of breaches that left everyone shocked. One of them was when the medical insurance provider brand Anthem Blue Cross became a victim of cyber crime in 2015.

The company officially disclosed on January 29 that hackers had stolen 78.8 million patient records by accessing the database comprising personal details like names, addresses, contacts, etc. And a breach of this magnitude began simply when a user within one of Anthem's subsidiaries opened a phishing email!

As per AppKnox, the company was lucky as no credit card credentials or patients' medical information was leaked in the breach. Also, the company made settlements for the same in 2017, which costed $115 Million!

Conclusion

If we keep on analyzing cybercrime of the past decade then no article would ever get completed. These were just some of the major attacks executed in the last ten years & they clearly showcase the sophistication and intelligence with which contemporary hackers are blessed!

Having said that, we at WhoisXml API over the past decade have also been working hard to create product & solutions that can help security experts to not only investigate, but also to stay a step ahead of malicious entities & prevent them from causing any damage. That is why over the years we have become a trusted domain Whois, DNS, IP and cyber threat intelligence data provider for threat intelligence/ infosec companies, anti-malware/security vendors, cybercrime units, government agencies, brand protection agencies, banks, payment processors, investment funds, and many more. To meet all the data needs of such large organizations, we provide various comprehensive Enterprise Packages that can aid your security teams with all the Intel they need from a single source.

We are sure that you wouldn't want to be next in such a list and hence it's better to start taking cybersecurity seriously. To successfully fight against growing cyber attacks, it's crucial that organizations create strong policies & training for cyber security awareness amongst its employees and also include security best practices as a part of their culture.

To know how we can support you please send us an email at support@whoisxmlapi.com with your requirements & our team will be more than happy to help you.

Happy Digital Defending!