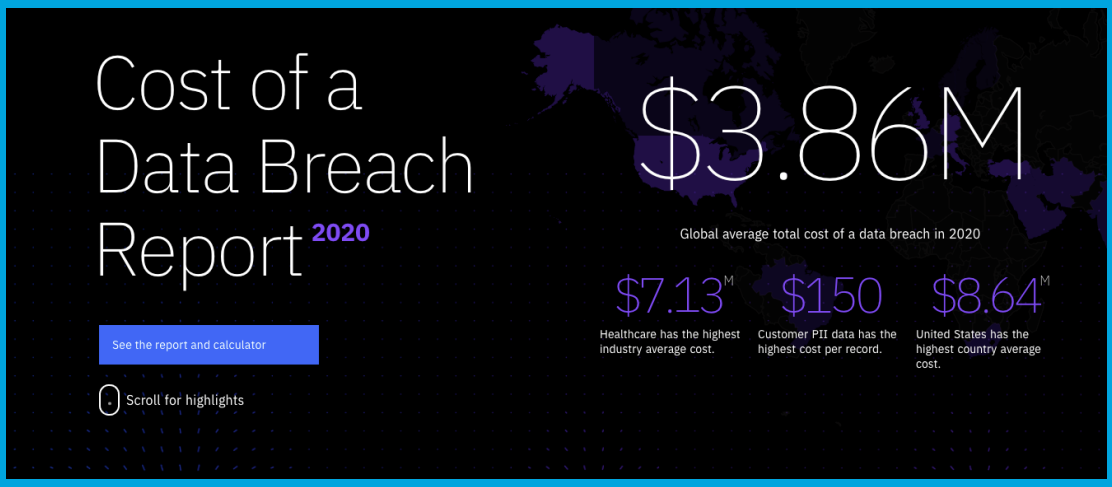
Security Newsletter

7 December 2020

Subscribe to this newsletter

The biggest hacks, data breaches of 2020



Cybersecurity may be far from many of our minds this year, and in light of a pandemic and catastrophic economic disruption, remembering to maintain our own personal privacy and security online isn't necessarily a priority. However, cyberattackers certainly haven't given anyone a break this year. Data breaches, network infiltrations, bulk data theft and sale, identity theft, and ransomware outbreaks have all occurred over 2020 and the underground market shows no signs of stopping.

Many companies and organizations, too, have yet to practice reasonable security hygiene, and vulnerabilities pose a constant threat to corporate networks. As a result, we've seen a variety of cyberattacks this year, the worst of which we have documented below.

Remote work became a major security consideration of study participants due to the spread of the COVID-19 pandemic. The average time to identify and contain a data breach, or the "breach lifecycle," was 280 days in 2020. Speed of containment can significantly impact breach costs, which can linger for years after the incident. The share of breaches caused by malicious attacks has steadily increased. Compromised credentials was the most expensive initial cause of malicious breaches in the study, while the type of threat actor also had a major impact on cost. Security automation solutions — including AI, analytics and orchestration — and incident response (IR) preparedness, including formation of IR teams and testing IR plans, showed the greatest reduction in data breach costs.

Read More on ZDNet

Cost of Data Breach Report 2020

Multiple Botnets Exploiting Critical Oracle WebLogic Bug — Patch Now!

Multiple botnets are targeting thousands of publicly exposed and still unpatched Oracle WebLogic servers to deploy crypto miners and steal sensitive information from infected systems. The attacks are taking aim at a recently patched WebLogic Server vulnerability, which was released by Oracle as part of its October 2020 Critical Patch Update and subsequently again in November (CVE-2020-14750) in the form of an out-of-band security patch.

Although the issue has been addressed, the release of proof-of-concept exploit code has made vulnerable Oracle WebLogic instances a lucrative target for threat actors to recruit these servers into a botnet that pilfers critical data and deploy second stage malware payloads. According to Juniper Threat Labs, operators of the DarkIRC botnet are exploiting this RCE vulnerability to spread laterally across the network, download files, record keystrokes, steal credentials, and execute arbitrary commands on compromised machines.

It's recommended that users apply the October 2020 Critical Patch Update and the updates associated with CVE-2020-14750 as soon as possible to mitigate risks stemming from this flaw. Oracle has also provided instructions to harden the servers by preventing external access to internal applications accessible on the Administration port.

Read More on TheHackerNews

More #News

- Malicious npm packages caught installing remote access trojans
- Microsoft removes 18 malicious Edge extensions for injecting ads into web pages
- Theoretical Attack on Synthetic DNA Orders Highlights Need for Better Cyber-Biosecurity
- Credit card skimmer fills fake PayPal forms with stolen order info
- Four years after the Dyn DDoS attack, critical DNS dependencies have only gone up
- Hackers Targeting Companies Involved in Covid-19 Vaccine Distribution

- Hackers-For-Hire Group Develops New 'PowerPepper' In-Memory Malware
- Nintendo Hacker's Sentence: 3 Years in Prison
- Impressive iPhone Exploit
- Google Chrome will soon warn you when using weak passwords
- Russian hacking group uses Dropbox to store malware-stolen data

#Breach Log

- Healthcare provider AspenPointe data breach affects 295K patients
- MasterChef, Big Brother producer hit by DoppelPaymer ransomware
- BlackShadow hackers extort Israeli insurance company for $1 million
- Metro Vancouver's transit system hit by Egregor ransomware
- Ransomware gang says they stole 2 million credit cards from E-Land
- K12 online schooling giant pays Ryuk ransomware to stop data leak

#Patch Time!

- Drupal issues emergency fix for critical bug with known exploits
- VMware fixes zero-day vulnerability reported by the NSA
- Microsoft Office November 2020 updates fix Outlook, Skype issues

#Tech and #Tools

- Tool Release – Carnivore: Microsoft External Assessment Tool
- Introducing CRLite: All of the Web PKI's revocations, compressed
- Kernel privilege escalation: how Kubernetes container isolation impacts privilege escalation attacks
- WriteHat, a reporting tool written by pentesters, for pentesters.
- XSSworm.dev ~ Self-replication contest [write-up]
- AliExpress Captcha Reuse
- Improving OAuth App-to-App Security
- Foundations of a Multi-Cloud Security Strategy
- Maintained list of 0day "In the Wild"
- Trickbot now offers 'trickboot': persist, brick, profit
- CIS Community Defense Model
- Open Source Does Not Equal Secure
- Open Source Tool Helps Secure Siemens PCS 7 Control Systems
- Techniques for writing least privilege IAM policies

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us