THE WEEK IN BREACH NEWS: 12/09/20 – 12/15/20

DenBe Computer Consulting
Connecting Business

December 16, 2020 by Dennis Jock

This Week in Breach News: This week's certainly been one for the books! Nation-state hackers mount a huge campaign against cybersecurity companies and several US federal agencies, the EU's drug regulator takes a hit, new insight into cyberattack response plan essentials, and fake Zoom invite pitfalls abound.

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** ID Theft Forum
- **Top Compromise Type:** Domain
- **Top Industry:** Education & Research
- **Top Employee Count:** 11-50

If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

SolarWinds

https://www.newsweek.com/solarwinds-hack-customer-list-suspected-russian-cyberattack-1554467

Exploit: Hacking (Nation-State)

SolarWinds: Cybersecurity Software Developer

Risk to Business: **1.122 = Extreme**

An incursion by suspected Russian nation-state hackers at this major cybersecurity solutions provider was the suspected starting point of a massive hacking incident impacting a number of federal agencies and defense assets. The hackers were able to obtain authentic credentials that enabled them to inject code into a routine software patch, opening backdoors into client files and systems.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: 3,000

How it Could Affect Your Customers' Business: Nation-state hacking is a growing problem that can lead to damaging, nightmarish consequences. One tool that was used in this hack was that old favorite – phishing.

FireEye

https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html

Exploit: Hacking (Nation-State)

FireEye: Cybersecurity Solutions Development and Testing

Risk to Business: 1.411 = Extreme

FireEye was also impacted in this week's suspected Russian hacking operation. Hackers were able to penetrate FireEye's systems security to obtain several of their vaunted Red Team tools. FireEye immediately detected the hack and released a statement exposing it. That was the first domino in the cybersecurity disaster cascade.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Even the biggest kids on the block can be taken down by determined hackers. Reviewing and updating cybersecurity and incident response plans has to be a top priority in 2020.

Netgain

https://www.bleepingcomputer.com/news/security/ransomware-forces-hosting-provider-netgain-to-take-down-data-centers/

Exploit: Ransomware

Netgain: Data Hosting Provider

Risk to Business: 2.127 = Severe

A ransomware incident led to shutdowns and slowdowns across Netgain's data hosting environment. The company was forced to completely shut down all systems on 12/4 for containment and remediation. Service has been restored to customers but they may still experience performance issues.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Ransomware can have damaging consequences for businesses that go beyond the initial hit causing huge operational headaches and long recovery operations.

Dental Care Alliance

https://www.infosecurity-magazine.com/news/1m-us-dental-patients-impacted-by/

Exploit: Hacking

Dental Care Alliance: Dental Practice Support Organization

Risk to Business: 2.336 = Severe

Dental Care Alliance, a professional support organization that includes more than 320 dentists in 20 states, has discovered that it experienced a data breach. The incident began on 09/18/20 and was ameliorated on 10/13/20. No cause has yet been specified and the incident is still under investigation.

Individual Risk: 2.114 = Severe

The stolen information included patient names, addresses, dental diagnosis and treatment information, patient account numbers, billing information, bank account numbers, the name of the patient's dentist, and health insurance information. potentially 10% of patients also had bank account information exposed. Impacted patients are being notified by mail and should be wary of spear phishing attempts using this information.

Customers Impacted: 1 million patients

How it Could Affect Your Customers' Business: When protecting sensitive information like medical data, it's essential to maintain strong access point protection to avoid expensive breaches and expensive fines.