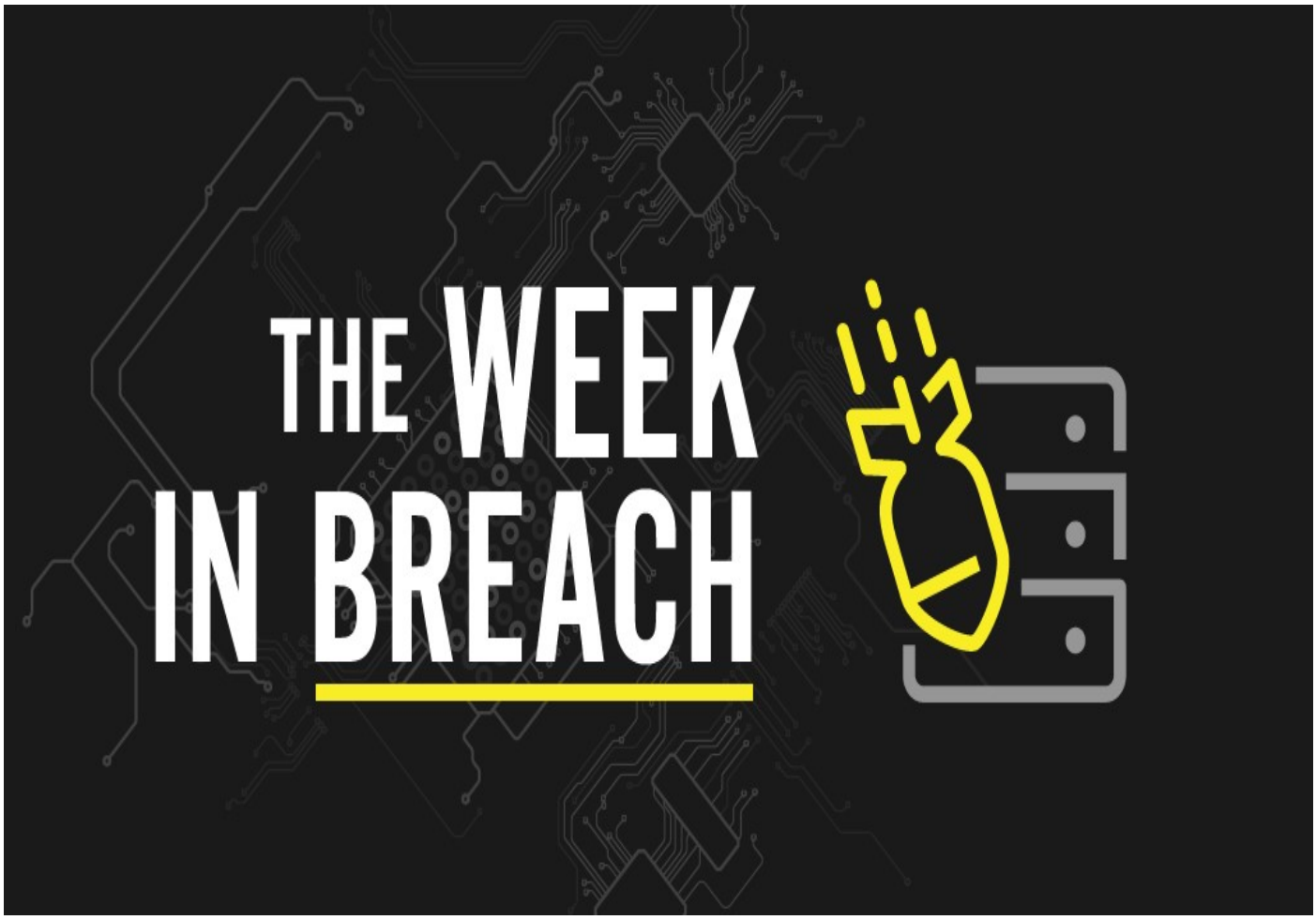
THE WEEK IN BREACH NEWS: 12/01/21— 12/07/21

DenBe Computer Consulting
Connecting Business

December 9, 2021 by Dennis Jock



Cybercriminals snatched millions from three cryptocurrency platforms, PII and PHI were exposed in major medical clinic snafus and the impact of ransomware on their clients according to MSPs, plus what they expect to see in the ransomware space in 2022.

Planned Parenthood

https://www.washingtonpost.com/nation/2021/12/01/los-angeles-planned-parenthood-hack/

Exploit: Ransomware

Risk to Business: 1.616= Severe

Bad actors gained access to the personal information of an estimated 400,000 patients of Planned Parenthood in Los Angeles this past October in a probable ransomware attack. A spokesperson said that someone gained access to Planned Parenthood Los Angeles' network between October 9 and 17, deployed and exfiltrated an undisclosed number of files. The breach is limited to the Los Angeles affiliate and an investigation is underway.

Risk to Business: 1.703= Severe

PPLA told clients that PII and PHI had been exposed including the patient's name, address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescriptions.

Customers Impacted: 400,000

How It Could Affect Your Business: *Medical information is valuable, especially sensitive information like this that can be used for both cybercrime and blackmail, and patients expect that healthcare providers will protect it.*

Gale Healthcare Solutions

https://www.zdnet.com/article/sensitive-information-of-30k-florida-healthcare-workers-exposed-in-unprotected-database/

Exploit: Misconfiguration

Risk to Business: 1.611=Severe

More than 30,000 US healthcare workers' personal information was recently exposed due to a non-password-protected database owned by Gale Healthcare Solutions, a Florida-based healthcare staffing provider. Files containing the PII of healthcare workers that the company placed were hosted on an unsecured AWS cloud server that was uncovered by security researchers in September. Gale Health Solutions says that the environment has been deactivated and secured. The company also says that there is no evidence there was any further unauthorized access beyond the researcher or that any

Individual Risk: 1.813=Severe

Researchers reported that the files they saw contained a healthcare worker's face image or ID badge, full name and a number consistent with an SSN. Other personal data about the impacted workers may also have been exposed.

Customers Impacted: 300,000

How It Could Affect Your Business *This mistake will be expensive and coveted healthcare workers may be inclined to choose a different staffing agency because of this carelessness.*

MonoX

https://www.hackread.com/hackers-steal-badger-defi-monox/

Exploit: Hacking

MonoX: Cryptocurrency Finance

Risk to Business: 1.318=Extreme

The MonoX DEX platform has experienced a breach that did damage to the tune of $31 million. The breach took place after hackers exploited a vulnerability in smart contract software, then exploited the vulnerability to increase the price of MONO through smart contracts and bought assets with MONO tokens. DeFi platform Badger was also reportedly hit by hackers for $120 million last week after they gained access
by targeting a protocol on the Ethereum network.

Individual Impact: No consumer PII or financial data loss was disclosed in this breach as of press time.

Customers Impacted: Unknown

How It Could Affect Your Business *In an ultra-competitive sector like crypto, customers will be watching every move a company makes, especially if it could potentially cost them money.*

DNA Diagnostics Center

https://www.zdnet.com/article/dna-testing-center-admits-to-breach-affecting-ssns-banking-info-of-more-than-2-million-people/

Exploit: Ransomware

Risk to Business: 1.819= Severe

DNA Diagnostics Center said that on August 6, the company discovered that there had been unauthorized access to its network that enabled someone to access and exfiltrate an archived database that contained patient PII collected between 2004 and 2012. The Ohio-based company says that 2,102,436 people had their information exposed. Victims may have been ordered to undergo genetic testing as part of a legal matter.

Individual Risk 1.617= Severe

The company is sending letters to impacted individuals warning them that they may have had their PII and sensitive data such as Social Security number or payment information exposed. Anyone whose personal information was accessed is being offered Experian credit monitoring.

Customers Impacted: 2,102,436

How it Could Affect Your Business *Companies that store two kinds of valuable data like this are at high risk for an expensive and damaging ransomware incident that will have lasting financial results.*