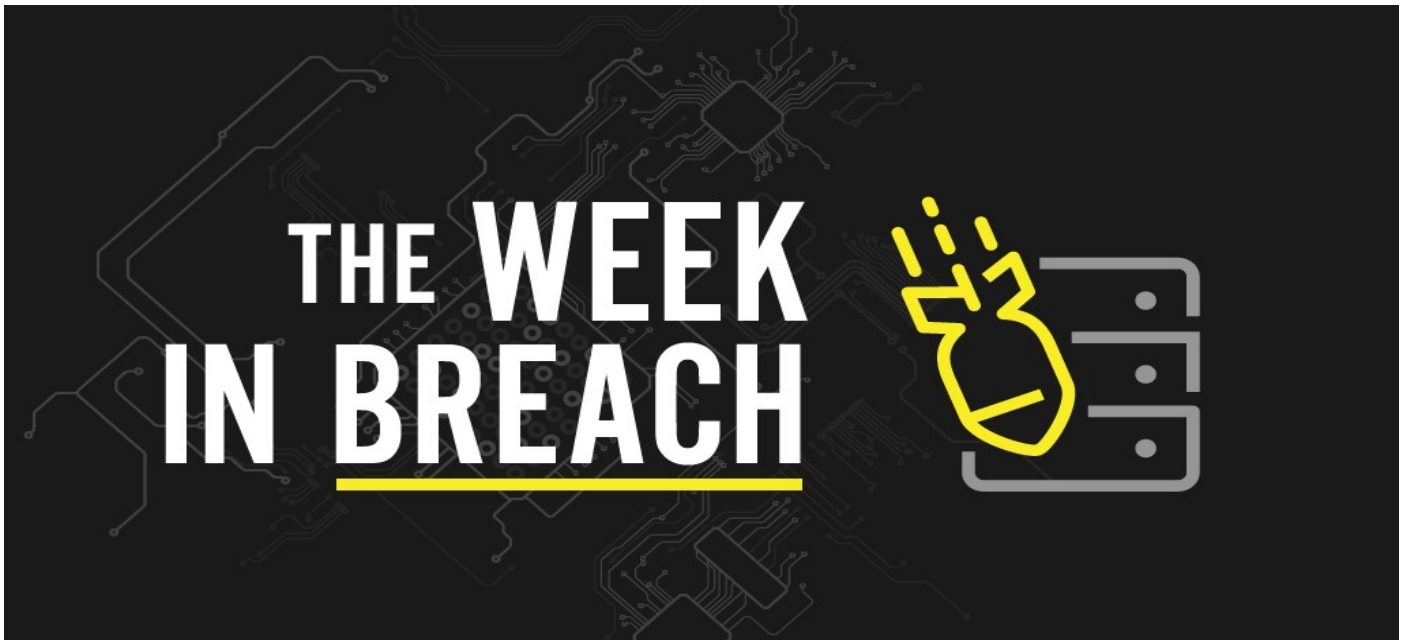
THE WEEK IN BREACH NEWS: 05/12/21—5/18/21

DenBe Computer Consulting
Connecting Business

May 19, 2021 by Dennis Jock

In a Week in Breach first, it's the All Ransomware Edition. Cybercrime gangs have been busy at Toshiba, Ireland's health service, the US Veterans Administration and other organizations around the globe. Plus, we'll explore the state of email security, the most likely delivery system for ransomware!



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***

United States – Three Affiliated Tribes

https://nativenewsonline.net/currents/three-affiliated-tribes-hit-by-ransomware-attack-holding-tribal-information-hostag

Exploit: Ransomware

Risk to Business: **1.607= Severe**

The Three Affiliated Tribes (the Mandan, Hidatsa & Arikara Nations) announced to its staff and employees that its server was infected with ransomware. Since the server was hacked, the tribe has been unable to access files, email and critical information. Employees were also asked to refrain from using their work computers, Investigation and recovery is ongoing.

Individual Impact: No sensitive personal or financial information was confirmed as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How It Could Affect Your Business: Protection from ransomware needs to be a top priority for every organization. These days a new attack is launched every 40 seconds putting every business in the line of fire.

United States – US Veterans Administration (VA)

https://threatpost.com/veterans-medical-records-ransomware/166025/

Exploit: Ransomware

Veterans Administration: Federal Agency

Risk to Business: 1.722= Severe

The VA has found itself in the cybersecurity hot seat again after a data breach at a records contractor exposed more than 200,000 records for veterans. The contractor, United Valor Solutions, appears to have been the victim of a ransomware attack. Researchers found a trove of their data online, including this sensitive VA data. The VA has announced that its Veterans Benefits Administration (VBA) Privacy Office is currently working with Medical Disability Examination Officer (MDEO) and contractors to further handle the incident, with the VA Data Breach Response Service investigating independently.

Individual Risk: 1.722= Severe

The exposed records contain included patient names, birth dates, medical information, contact information and even doctor information and appointment times, unencrypted passwords and billing details for veterans and their families, all of which could be used in socially engineered spear phishing or fraud scams.

.

Customers Impacted: 200,000

How it Could Affect Your Customers' Business: Ransomware is the gift that keeps on giving for medical sector targets. Not only are those victims facing expensive investigation and recovery costs, but they can also expect a substantial HIPAA fine and possibly more regulatory scrutiny.

Ireland – Health Service Executive (HSE)

https://www.bbc.com/news/world-europe-57134916

Exploit: Ransomware

Health Service Executive (HSE): National Healthcare Provider

Risk to Business: **1.668 = Severe**

Ransomware rocked Ireland after the Conti gang perpetrated attacks on both the Department of Health and Ireland's national healthcare provider Health Service Executive (HSE). HSE was forced to take action including shutting down the majority of its systems including all national and local systems involved in all core services and all major hospitals. The ransom demand is reported to be $20 million. The National Cyber Security Centre (NCSC) has said the HSE became aware of a significant ransomware attack on some of its systems in the early hours of Friday morning and the NCSC was informed of the issue and immediately activated its crisis response plan. On Monday, May 18, officials announced that diagnostic services were still impacted as well as other patient care necessities. Officials alos said that it may take the Irish health service weeks to repair systems and restore all services, at a price that will reach

Individual Impact: No sensitive personal or financial information was confirmed as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is the preferred weapon of cybercriminals at every activity level. Increased security awareness training makes organizations up to 70% less likely to experience damaging cybersecurity incidents like this one. attacks.

Germany – Brenntag

https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/

Exploit: Ransomware

Brenntag: Chemical Distributor

Risk to Business: **1.523 = Severe**

Brenntag suffered a ransomware attack that targeted their North America division. As part of this attack, the DarkSide ransomware gang encrypted devices on the network and stole unencrypted files. This is the same gang that starred in last week's Colonial Pipeline incident. On their leak site, DarkSide claimed to have stolen 150GB of data during their attack. Reports say that Brenntag paid the threat actors more than $5 million for the decryption key. exposed credentials, experiment data and other proprietary information that were stored with no security.

Individual Impact: No sensitive personal or financial information was confirmed as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is the weapon of choice for top cybercrime gangs because they know that they'll find a few companies who are more than willing to pony up cash rather than undertake an expensive recovery or risk having proprietary data exposed.

Norway – Volue

https://www.smh.com.au/national/nsw/police-investigate-cyber-attack-on-nsw-labor-party-20210505-p57p4y.html

Exploit: Ransomware

Volue: Green Energy Solutions Provider

Risk to Business: 2.109 = Severe

Norwegian green energy solutions provider Volue has been the victim of a ransomware attack, using Ryuk ransomware. Volue offers industrial IoT, data and market analysis, power trading, construction software, optimization and trading software, water infrastructure documentation and management, and transition and distribution software solutions to more than 2,200 customers across 44 countries. Volue's investigation is ongoing, but so far it has found no evidence of data exfiltration, either personal or "energy-sensitive data." Operations are expected to be restored quickly.

Individual Impact: No sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is the modern cybercriminal's weapon of choice. Make sure your clients are taking every possible precaution because 61% of organizations worldwide experienced a damaging ransomware incident in 2020.

France – Acer Finance

https://securityaffairs.co/wordpress/117991/cyber-crime/avaddon-ransomware-acer-finance-axa.html

Exploit: Ransomware

Acer Finance: Financial Advisors

Risk to Business: 2.307 = Severe

Avaddon ransomware came calling at Acer Finance. The Company offers risk management, mutual funds, analysis, financial planning, and advisory services. Acer Finance serves individuals, entrepreneurs, and institutional investors in France. The ransomware gang claims to have stolen confidential company information about clients and employees, and they're giving Acer Finance 240 hours to communicate and cooperate with them before start leaking the stolen valuable company documents. As proof of the hack, the group published several ID cards, personal documents, contracts, and a screenshot of the folders containing stolen data.

Individual Impact: At this time, no sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: No organization is safe from phishing. Every company should make stepping up phishing resistance training a priority to reduce the chance of falling prey to an attack.

Hong Kong – AXA

https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/

Exploit: Ransomware

AXA: Insurance Company

Risk to Business: 1.817 = Severe

The Avaddon ransomware group claimed on their leak site that they had stolen 3 TB of sensitive data from insurance giant AXA's Asian operations including the company's offices in Thailand, Malaysia, Hong Kong and the Philippines. The gang claims that the stolen data includes includes sensitive customer and busienss data. The attack may be connected to AXA's announcement that they would be dropping reimbursement for ransomware extortion payments when underwriting cyberinsurance policies in France.

Risk to Business: 1.773 = Severe

The group claims to have obtained 3 TB of data belonging to AXA including, customer medical reports (including those containing sexual health diagnosis), customer claims, payments to customers, customers' bank account scanned documents, material restricted to hospitals and doctors (private fraud investigations, agreements, denied reimbursements, contracts), identification documents such as National ID cards, passports and other sensitive data.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware attacks as a punishment for company actions is uncommon but not surprising. Ransomware gangs like Abaddon can quickly slip under the radar to do damage at the companies that they choose to target with a simple phishing email that packs deadly consequences.

Japan – Toshiba

https://www.cyberscoop.com/darkside-ransomware-toshiba-hack/

Exploit: Ransomware

Toshiba: Electronics Manufacturer

Risk to Business: 1.817 = Severe

European units of Japanese tech giant Toshiba are investigating a security incident in which scammers may have used a similar hacking tool to the malware used against IT systems at Colonial Pipeline. The company announced that it had been forced to disconnect network connections between Japan and Europe to stop the spread of ransomware. The attack is believed to have been perpetrated by the DarkSide ransomware gang. Toshiba Tec Group, a unit of the multinational conglomerate which makes printers and other technologies, said the firm had not yet confirmed that customer related information was leaked externally. The incident is under investigation and the company says that it has not paid any ransom.

Customers Impacted: Unknown

Individual Impact: No sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

How it Could Affect Your Business: By disrupting internal operations, ransomware can cause tremendous problems for multinational companies even if no data is stolen or systems encrypted.