5 biggest ransomware attacks of 2020

!

The year 2020 saw a massive spike in ransomware attacks where hackers have stolen, taken over and encrypted critical data from top global companies. The estimated cost of ransomware attacks in 2020 was an astounding US$20 billion, considerably up from US$11.5 billion in 2019 and US$8 billion in 2018.

New ransomware types are exponentially increasing, which means that security professionals are spending most of their time playing catch up. Industry study reveals that new ransomware variants grew by 46% last year. The attacks are so prevalent that a business falls victim to a ransomware attack every 14 seconds. These numbers tell us that the threat is very real.

Let's take a look at some of the recent ransomware attacks that fleeced companies of millions of dollars:

1.Grubman Shire Meiselas & Sacks

This was one of the most well-known cases of 2020, especially because of the big names involved. Grubman Shire Meiselas & Sacks, a law firm that handles international celebrities such as Madonna, Bruce Springsteen, Lady Gaga, Mariah Carey, Nicki Minaj, and more, was hacked in mid-May by REvil, also popularly known as Sodinokibi. Media reports said that about 756 GB of private documents and correspondence with clients were stolen.

The hacker group had taken control over the personal information of its high profile clients, and demanded a US$21 million ransom, which was doubled later on. REvil claims to receive a US$365,000 payment, but the law firm has denied this.

2.Communications & Power Industries

Even IT professionals make mistakes. This was seen when a domain admin with high-level privileges from the California-based Communications & Power Industries (CPI) unassumingly clicked on a malicious link in mid-January while logged in to the system. This triggered a file-encrypted malware that spread across hundreds and thousands of computers on the company's network.

Multiple locations and onsite backups were affected by this attack. The hackers demanded a ransom of US$500,000 in exchange for a decryption key. Media reports said that the data in the custody of hackers comprised sensitive military data, and files related to Aegis, a naval weapons system. This prompted the company to quickly give in to the demands of hackers and retrieve the data.

3.University of California San Francisco

Sensitive personal information, especially healthcare data, is a goldmine for hackers. Seizing an opportunity, hackers launched malware that encrypted a few servers of UCSF's School of Medicine. They were able to lay their hands on some of the crucial academic work of the university.

The cybercriminals showed some data as proof and demanded an unknown sum of ransom. As the data was critical, UCSF agreed to pay a part of the ransom and ended up forking out about US$1.14 million in exchange of a decryption tool to retrieve the data. UCSF said it was able to quickly isolate breached IT systems and hence medical records of patients, university network and critical Covid-19 research being conducted were saved from the ransomware attack.

4.Travelex

On New Year's Eve last year, while the rest of the world was celebrating, Travelex was under attack by the Sodinokibi group of hackers. While the details of what was stolen was not revealed, it was enough to bring down the websites, apps and internal networks of the money exchange company, revealed media reports. Travelex was able to restart its business only a month and a half later in February 2020.

With business shut for several weeks, the incident disrupted cash deliveries and caused major losses to the company. Travelex ended up paying a ransom of US$2.3 million to the hackers to recover its data.

5.Cognizant

The biggest ransomware attack of 2020 was led on technology giant Cognizant. It costed the company a staggering US$50 to US$70 million in revenue loss, and recovery and mitigation efforts. In April this year, the Maze ransomware infected the company's network. This barred its work from home capabilities and encrypted its servers.

The attack was limited to the internal network and did not impact customer systems. As a result, employees could not access their email and communicate with each other. The company was able to recover and restore its services only three weeks later. It further incurred legal and consulting costs to investigate the attack, in addition to restoration and remediation.

Ransomware attacks lead to financial loss and damage your business and negatively impact your reputation, which takes years to build. Further, the restoration of the systems can take a fairly long time. What this means is that these things can make your customers very wary of doing business with you.

Preventing ransomware sometimes involves mundane and basic things like creating strong passwords, regularly updating your software and educating the workforce about the harmful effect of malware.

A crucial component of protecting your data and infrastructure from ransomware is to have a backup. However, the data needs to be protected even during transit and in storage. Parablu's BluVault, supported by BluKrypt, a secure container powered by enterprise-grade privacy gateway, ensures that your data is protected and encrypted even when it travels between your enterprise assets and the cloud. A safe and reliable backup of your data means that your business never has to be at the mercy of a malicious attacker.