Cyberattacks and their impacts

Valiveti manikanta bhuvanesh

19BCD7088

In my survey I found some of the cyberattacks during COVID 19 pandemic . Top 10 major attacks among them are :

1. **Toll Group**

   Toll Group tops the list because it was hit by ransomware twice in three months. As a precautionary measure, Toll has made the decision to shut down a number of systems in response to a cyber security incident.

   There immediate priority is to resume services to customers as soon as possible. The most recent attack occurred in May and involved a relatively new ransomware variant Nefilim.

2. **Marriott International**

   For the second time in two years, the popular hotel chain suffered a data breach. On March 31, Marriott said the information of 5.2 million guests was accessed using the login credentials of two employees at a franchise property .They confirmed that the login credentials were disabled, immediately began an investigation. Marriott said it has no reason to believe that the information included the Marriott Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers .They said information may have involved contact details and information relating to customer loyalty accounts, but not passwords.

3. **Magellan**

   On May 12, the healthcare insurance giant issued a letter to victims stating it had suffered a ransomware attack .Hackers had successfully exfiltrated logins, personal information and tax information. The scope of the attack included eight Magellan Health entities and approximately 365,000 patients may have been impacted. On April 11, 2020, Magellan discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan's systems after sending a phishing email.

4. Twitter

Twitter was breached in July by three individuals in an embarrassing incident that saw several high-profile Twitter accounts hijacked. Through a social engineering attack, later confirmed by Twitter to be phone phishing, the attackers stole employees' credentials and gained access to the company's internal management systems. Dozens of high-profile accounts including those of former President Barack Obama, Amazon CEO Jeff Bezos, and Tesla and SpaceX CEO Elon Musk, were hacked. Hackers then used the accounts to tweet out bitcoin scams that earned them over $100,000.

5. Garmin

The navigation tech supplier suffered a cyberattack that encrypted some of its systems and forced services offline. Though Garmin first reported it as an outage, the company revealed on July 27 that it was the victim of a cyberattack which resulted in the disruption of website functions, customer support, customer-facing applications, and company communications .The incident was a ransomware attack.

6. Clark County School District

The attack on the Clark County School District (CCSD) in Nevada revealed a new security risk: the exposure of student data. CCSD revealed it was hit by a ransomware attack on Aug. 27 which may have resulted in the theft of student data. After the district declined to pay the ransom, an update was posted saying it was aware of media reports claiming student data had been exposed on the internet as retribution.

7. Software AG

The German software giant was the victim of a double extortion attack that started on Oct. 3, which resulted in a forced shutdown of internal systems and ultimately a major data leak. Files were encrypted and stolen by operators behind the Clop ransomware. Software AG declined to pay as a result, the ransomware gang followed through with its promise and published confidential data on a data leak site including employees' passport details, internal emails and financial information.

8. Vastaamo Psychotherapy Centre

The largest private psychotherapy provider in Finland confirmed it had become the victim of a data breach on October 21, where hackers stole confidential patient records. The attack set a new precedent; rather than making demands of the organization, patients were blackmailed directly.

9. FireEye and SolarWinds supply chain attack victims

FireEye set off a chain of events on Dec. 8th when it disclosed that suspected nation-state hackers had breached the security vendor and obtained FireEye's red team tools. On Dec. 13, the company disclosed that the nation-state attack was the result of a massive supply chain attack on SolarWinds. FireEye dubbed the backdoor campaign "UNC2452" and said it allowed threat actors to gain access to numerous government and enterprise networks across the globe. Major tech companies such as Intel, Nvidia and Cisco disclosed they had received the malicious SolarWinds updates, though the companies said they've found no evidence that threat actors exploited the backdoors and breached their networks.

10. SolarWinds

The scope of the attack, the sophistication of the threat actors and the high-profile victims affected make this not only the biggest attack of 2020, but possibly of the decade. Threat actors, who had performed reconnaissance since March, planted a backdoor in SolarWinds' Orion platform, which was activated when customers updated the software .They said this attack was likely conducted by an outside nation-state and intended to be a narrow, extremely targeted and manually executed attack, as opposed to a broad, system-wide attack.

Risk Assessment on

https://www.indiabookstore.net/

S.NO	Risk	Risk prevention	Risk probability	Risk Impact
1	Out dated web server(nginx) leads to implementation of HTTP/2 that can allow for excessive memory consumption and possibly risk for dos attacks.	Upgrade webserver to new version	HIGH	HIGH
2	Missing secure flag for cookies: Since the Secure flag is not set on the cookie, the browser will send it over an unencrypted channel like http. So attacker intercept this channel.	Whenever a cookie contains sensitive information , then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.	HIGH	MEDIUM
3	Missing HttpOnly flag for cookies: it can be accessed by the JavaScript code running inside the web page .And leads attacker to hijack the web page	Ensure that the HttpOnly flag is set for all cookies.	HIGH	MEDIUM
4	Missing Strict-Transport-Security for Security header: This header instructs browser to initiate only https connection to web server and deny http connections .This http connection leads opening the possibility to eavesdrop on the network traffic and extract sensitive information	The Strict-Transport-Security HTTP header should be sent with each HTTPS response	MEDIUM	LOW
5	Missing X-XSS-Protection for Security header:It instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks	Set X-XSS-Protection header	LOW	LOW