Cyberattacks in 2021 that locked targets on the high-profile organizations

Organizations have been strengthening their servers and systems daily through all possible means. Yet, hackers try to find loopholes through different methods. Let's not deny that all secure setups have a loophole in one form or another. These loopholes are either dealt with ethically or exploited in different ways. Such is the threat in cybersecurity.

Cyber-attacks are not just on the "Big Fish." Hackers exploit all sorts of vulnerabilities that they see on a day-to-day basis.

The most common method of exploitation is through a ransomware attack. Here, the organization's data is encrypted so that the applications, files, databases, etc., can't be accessed. However, there would be threats to leak the encrypted data. A ransom is then demanded to provide access. Upon paying the ransom, the decryptor would be provided by the hackers to decrypt the encrypted data.

Cyber-attacks have been flooding in through multiple loopholes and affect different categories of organizations ranging from security organizations to daily-essential organizations like meat industries and fuel pipelines. Let's walk through some of the well-known cyber-attacks this year.

Colonial Pipeline

The Colonial Pipeline is a US pipeline that is considered to be one of the most significant and vital pipelines in the US. It runs from Texas carrying gasoline, diesel, and jet fuel to New York. Unfortunately, it was the victim of a ransomware attack in May 2021. The attack was considered a national threat as some of the pipeline's digital systems were affected, leading to a complete shutdown for a few days.

The attack was initiated by a Russian group of hackers named DarkSide. It was focused on the SCADA (Supervisory Control and Data Acquisition) systems of the Colonial Pipeline's I.T. servers. They gained access to the servers using a VPN account that a former employee abandoned. There are many conspiracy theories on how the credentials were obtained; however, the exact method remains unknown. Additionally, the Colonial Pipeline's servers didn't feature a multi-factor authentication, making it easier for the hacker group to breach the SCADA systems easily. The U.S. government shut down the systems to contain the attack's spread, but this led to a sudden closure of a critical fuel pipeline putting the consumers in a state of panic.

The Darkside malware works by disabling windows services, deleting volume copies, encrypting the local and network shares, and exporting the data to a C2 server. It then deletes its copy and posts the ransom note. The lack of a data exfiltration solution worsened the situation for the Colonial Pipeline as the export to a C2 server could've been stopped. The attackers stole about 100 gigabytes of data within two hours.

Even though all the concerned authorities were informed, the Colonial Pipeline ended up

paying the ransom demanded by the hacker group enabling the I.T. staff to regain control.

Acer

Taiwan-based computer giants Acer were hit by a REvil ransomware attack in March 2021. Images were leaked on REvil's website, which contained financial statements, bank communications, and bank balances. The group got access to the Acer systems via a Microsoft Exchange vulnerability, and multiple hackers have utilized this vulnerability against multiple organizations for ransom.

The hacker group demanded about 50 million USD as ransom. Acer, however, hasn't revealed whether or not they have paid the ransom. REvil had reportedly made over 100 million USD using their ransomware attacks on multiple organizations. But the story doesn't end there.

In October 2021, another hacker group, by the name of Desorden, attacked Acer again. They gave video proofs and claims of stealing 60 GB of data. A sample of Acer employees' login credentials and screenshots of Acer's Taiwan internal portal were shared by the hackers as proof of the attack. Desorden finally said that the intention of the attack was only to make Acer aware of its weak cybersecurity measures.

Kia Motors

Kia Motors America suffered a suspected attack by ransomware attackers named DoppelPaymer. This attack hugely impacted their online systems, including the Kia Owner Portal, UVO Mobile Apps, and the Consumer Affairs Web portal leading to a complete system outage. The attackers stated that they attacked Hyundai, Kia's parent company, which didn't appear to be affected by the attack. However, users of the UVO Mobile apps, like the UVO Link and the UVO e-Services, received error messages like SQL errors, bad certificates, etc. This made the buyers unable to get their cars from their dealerships. In addition, there was a forced shut down on the KIA Owner's portal following the attack.

DoppelPaymer attacks initially try to gain access via Emotet malware, usually delivered via phishing e-mails. Emotet uses underhanded methods to prevent detection and analysis. Emotet infections mainly arrive via a malicious script pushed to a device. However, the infection may be also via macro-enabled document files in some cases. Once the access is obtained, the malware downloads the other necessary tools required to carry out the attack. Valuable data is identified and exfiltrated before encryption.

The attackers demanded a ransom of 404 bitcoin ($20 million) for the decryptor and threatened to increase it to 600 bitcoin ($30 million) if they refused to pay within a week. Kia avoided this as a 'speculation,' and it is unknown whether KIA paid the ransom.

JBS S.A.

JBS, the world's largest meat producer headquartered in Sao Paolo, faced a cyber-attack on May 31, 2021. The attack disrupted their supply chains in the United States, Canada, and Australia. This attack was also considered a REvil ransomware attack. The systems had to be shut down as soon as the technical staff found irregularities in the working. The company was forced to stop all slaughtering activities across the United States. This attack hugely impacted the meat supply chains and created a sense of panic regarding food shortage. The demand started to increase, and so did the price of meat. The situation started to worsen, and the company was forced to shut down all activities. The method of a breach used by the attackers remains unknown. The technicians informed the authorities when they saw a message demanding ransom. $11 million worth of bitcoin was demanded as ransom by the attackers. Understanding the severity of the attack, JBS decided to avoid risks and paid the ransom demanded by the attackers.

Twitch Data Dump

One of the largest streaming platforms, Twitch, disclosed a data breach that led to vast amounts of sensitive data being leaked online. Over 100GB of data, including the platform's source code, was leaked online. In addition, the payments Twitch made to the top streamers on the platform were also leaked. The hacker, "4chan", revealed in a note that twitch data was breached and exposed online as the twitch community was too toxic.

The streamers' payments are sensitive data as the competition between streaming platforms is high, and a leak would entirely disrupt the competition. The attackers gained access due to a server configuration change that allowed improper access by any third party without proper authentication. Twitch also stated that the passwords of user accounts and the payment methods linked to accounts weren't leaked as part of the breach. They also ensured to reset the stream keys – the unique code used to broadcast to the correct Twitch account.

There was no negotiation or payment as this was not a ransomware attack. However, sensitive data was leaked online, creating chaos in the twitch community as streamers feared that the hackers tapped their payment methods. However, Twitter dealt with the issue with utmost importance and solved the issues with ease.

Kaseya VSA attack

Kaseya is a software company that manages networks, systems, and IT infrastructure. Kaseya was hit by a REvil attack which created chaos among its customers. REvil

targeted Kaseya's Virtual Systems Administrator software, a software that manages the entire IT structure of an organization. Upon infiltrating the VSA, REvil injected ransomware into the MSPs (Managed Service Providers). MSPs are customers of Kaseya who are assigned to handle the IT operations of other organizations. Through these MSPs, REvil spread the malware to the customers.

Thousands of customers and organizations were affected due to this attack. Kaseya identified that REvil exploited an authentication bypass vulnerability that helped break into the VSAs and distribute the malware through the systems. However, there wasn't a ransom demand that was disclosed, and hence, the details behind that remain unknown. Kaseya later released a security patch that dealt with the REvil VSA attack. The patch was deployed nine days after the attack and addressed all vulnerabilities of the attack.

CNA Financial Attack

CNA Financial is an insurance company in the U.S. It came under attack a few days after the Colonial Pipeline attack. The group that attacked CNA is unknown. The method/loophole that they exploited also remains undisclosed. The attack was a ransomware attack. "Phoenix locker," a variant of the "Hades" malware, was used to attack the systems of CNA. The attackers exported a massive chunk of data to a C2 server and encrypted the data.

The CNA's primary operations were attacked, and clients started to panic as CNA was considered to have one of the most secure servers. $40 million was demanded as ransom to provide the decryptor for the encrypted data. CNA ended up paying the ransom demanded by the attackers. They later resolved the loophole that the attackers used to exploit. The CSA cyber-attack is proof that even the systems that are considered the most secure can be attacked.

Brenntag

Brenntag is a chemical-distribution company that was under a cyberattack at the beginning of May. A hacker group by the name 'DarkSide' hacked into the systems of Brenntag, claiming access to sensitive data, including finances, contacts. Chemical formulae, etc. DarkSide provided Brenntag with proof on the same. About 150 GB of data was stolen and encrypted.

Darkside threatened to leak the data if Brenntag failed to respond. They demanded a ransom of 134 bitcoin, approximately $8million, and they ended up reducing the demand to $4.4 million. Brenntag ended up paying the ransom, fearing a data leak. DarkSide gained access to the systems through stolen user credentials. Brenntag lacked a multi-factor authentication setup, which gave DarkSide access to the internal systems.

Conclusion

There have been several methods of attacks in the past, and the most common ones were ransomware attacks. Exploits and loopholes were found in the systems of multiple organizations, and these loopholes were targeted for multiple purposes.

Phishing is considered the main reason for cyberattacks as it has been the easiest way of introducing malware into a system. Most mail servers have good fraud detection systems, yet some fraud emails bypass these systems. Avoiding such emails would reduce the risks of attacks to a great extent. The lack of multi-factor authentication also contributed hugely to the advent of cyber-attacks.

A new type of cyberattack comes out every day, and hence organizations are in a position where they update their security measures on a day-to-day basis. The more updated you are in security, the less chance you are attacked. Security patches released for different OSs on a regular basis which helps in preventing cyberattacks. Regular updates of devices help in keeping the devices secure. Devices enrolled in Hexnode can be regularly scheduled for software updates, which helps keep the security patches up-to-date.

Connecting to external/public Wi-Fi is also dangerous. Hexnode helps you ensure that enrolled devices are restricted to connect only to specified Wi-Fi. Browsing through multiple websites also opens the gate for malware. A file we consider safe might be malware in disguise. Web Content Filtering feature with Hexnode helps to block/allow specific websites.

Apart from online methods, malware can creep in through offline methods too. Connecting a USB device is one of the easiest ways for malware to enter devices. Blocking external USB drives can be done effectively using Hexnode UEM, which ensures malware doesn't creep in even through the most straightforward methods.

Blacklisting/Whitelisting apps also ensure that apps from unknown/external sources are not installed in devices. Malware can enter our devices in multiple ways. Closing the gap for security breaches is the only way to keep systems secure as there is no absolute protection.

As quoted by Sun Tzu, "Don't depend on the enemy not coming; depend rather on being ready for him."

- Lockout: With Hexnode you can also formulate a lockout policy that defines how long the device is locked out following some invalid password submissions.

These password policies can be applied to Android, iOS, macOS, and Windows devices, remotely. So, enforce strong password protection for your devices from a single platform with Hexnode UEM.

Bypassing email phishing attempts

According to a recent study by Proofpoint 75% of organizations around the world faced phishing in some way, type or form. In the Data Breach Investigations Report by Verizon, it was found that 96% of phishing attempts were made via email. These attackers understand the weakest link and they exploit it to the maximum. When an employee is a victim of a phishing attack within your corporate network, your entire corporate data is in jeopardy.

With Hexnode's email management capabilities, you can stave off phishing attacks without breaking a sweat.

- Email domains can be configured so that the employees can only open emails received from managed domains. They can also only download attachments from managed domains.
- Hexnode can ensure that emails aren't opened in an unmanaged app. This is possible with the blacklist/whitelist function.
- Copy and paste can also be disabled for emails so that employees don't accidentally cause a data breach.

Phishing is one of the most prevalent forms of cybersecurity attacks out there. Even though most companies do provide phishing awareness training to their employees, it's always better to have a plan to face these scenarios head-on.

Keep tabs on your apps

Nowadays, every app you download asks for a million permissions. Not really bothered about it, we just accept all of them blindly. In a corporate setting, this could spell danger. Furthermore, what if the employee blindly downloads an app from an untrustworthy source, that's a recipe for a full-blown data breach.

Hexnode can mitigate these risks with its app management capabilities:

- **Custom app store**: Create a repository for the apps you think the employees would require. These custom app stores can house applications that are native to that particular platform and even in-house applications. This ensures that the employee doesn't have to leave the safe digital work environment to access the apps they require. The apps can be formed into groups or catalogs for easier deployment.

- **App lifecycle management**: Hexnode can manage everything, starting from the app's installation to its uninstallation. This includes update management, version changes, etc.
- **App permission and configuration management**: You can decide what all permission an app could get away with on the work devices you have deployed with Hexnode. You can place restrictions on certain permissions if you feel it would tamper with the organization's security. You can also place configurations on the apps present in the employee's work device that can restrict them from indulging in any malicious activity.
- **App blacklisting/ whitelisting**: Blacklist or whitelist apps that you feel could cause a security issue. This can be applied across all devices, all at once.
- **Work app and personal apps**: The risk posed by BYO devices are too big to be ignored. If data that is meant to be opened in a work app is opened in a personal app, it could lead to a data breach. Hexnode provides segregation for work and personal apps, so that managed and unmanaged data never mingle.

Protecting corporate networks

In the current cybersecurity landscape, the role of enterprise network security is quite important. Malicious entities can tap into your corporate network and launch cyber-attacks that could very well compromise the entire functioning of your organization. As Hexnode UEM has the capability to control many of the access points for such attacks, it would be paramount for enterprises of all sizes to incorporate such software. So, how exactly can Hexnode help you with network security?

Wi-Fi Configuration: Wi-Fi settings can be configured via Hexnode to connect devices to a corporate network. Over the air, an administrator can push Wi-Fi configurations to a managed device. Users can join the network without having to enter or share their Wi-Fi passwords.

Deploying VPN: A VPN improves security by allowing users to communicate and share data via a private and secure network. This keeps it safe from potential threats and from the public network. As a result, a virtual network is an effective security solution that can be remotely configured with Hexnode UEM.

SCEP: Security threats caused by accessing work emails, Wi-Fi, VPN, etc., from unauthorized devices, can be solved by authenticating them with digital certificates. Hexnode UEM allows you to configure SCEP and enforce certificate-based authentication for Wi-Fi, VPN, Email, etc., on your devices.

Global HTTP proxy settings: With Hexnode you can ensure that all HTTP data flow through proxy servers. By controlling the flow of the data, you can ensure that your network is protected from possible threats.

Web content filtering: With whitelisting and blacklisting capabilities, Hexnode can ensure that your employees don't access malicious content while on the corporate network.

Bottom line

The pressure of protecting your organization against hordes of malicious entities is ever mounting. Most organizations feel they won't be a victim of a cyber-attack until they experience it themselves. It's always better to be aware and be prepared against any contingencies and Hexnode UEM can surely help you with that.