A Report on Recent Malware Incidents

By: Linto Baby

Cyberattacks have become a major issue for companies of all sizes. Hackers are getting smarter and are targeting critical services, causing widespread problems. This report looks at three major incidents to show how these attacks happen and the damage they can cause. We'll examine the attacks on Change Healthcare, customers of a data company called Snowflake, and the UK's National Health Service (NHS) through a partner company, Synnovis.

---

1. The Change Healthcare Attack: A Crisis for U.S. Healthcare

What Happened?
In February 2024, hackers attacked Change Healthcare, a company that is essential to the U.S. healthcare system. It handles about half of all medical claims in the country, acting as the middleman between doctors and insurance companies. The attack shut down their systems, which meant doctors and hospitals couldn't get paid. This caused a massive financial crisis for healthcare providers across the country, with many smaller clinics struggling to stay open. The hackers also stole the private health and personal information of roughly 190 million people, making it the largest healthcare data breach in U.S. history. The company ended up paying a $22 million ransom to the hackers, but this didn't solve the problem, as another group of hackers later tried to extort them using the same stolen data.

How Did the Hackers Get In?
The attack was successful because of a very basic security mistake. The hackers got into Change Healthcare's network through a remote access portal that wasn't protected with multi-factor authentication (MFA). MFA is a simple security step, like getting a code on your phone, that adds an extra layer of protection. Because this wasn't in place, the hackers only needed a single stolen password to get in. Once inside, they spent nine days moving through the network and stealing data before launching the main attack.
How Was It Fixed?
Change Healthcare had to disconnect its systems to stop the attack from spreading, which is what caused the nationwide outage. To help doctors and hospitals that were cut off from their money, the company's parent, UnitedHealth Group, provided over $6 billion in emergency loans. They slowly brought their systems back online, starting with pharmacies and then moving to payment and claims systems. The incident has led to multiple lawsuits and a

government investigation into the company's security practices.

---

2. The Snowflake Customer Breaches: A Password Problem

What Happened?
In mid-2024, many large companies, including Ticketmaster, AT&T, and Santander Bank, had their data stolen. At first, it looked like the data storage company they all used, Snowflake, had been hacked. However, investigations showed that Snowflake's own systems were secure. The problem was that the customers' accounts were not properly protected.
A group of hackers, focused on making money, stole huge amounts of data from about 165 different companies. They then tried to sell the data online or demanded ransom payments from the victims, asking for up to $5 million.

How Did the Hackers Get In?
The hackers used a simple but effective method: they logged into customer accounts using correct usernames and passwords. These passwords had been stolen over several years by "infostealer" malware—a type of virus that infects computers and steals saved login details. Some of the passwords used in the attack were stolen as far back as 2020.
The main reason the attack worked was that the victims had not enabled multi-factor authentication (MFA) on their Snowflake accounts. With only a password needed to log in, the hackers walked right in. Many of the stolen passwords came from the computers of outside contractors who often had access to multiple companies' systems.

How Was It Fixed?
Snowflake worked with cybersecurity firms to investigate and notified all the customers who were at risk. The solution for the affected companies was straightforward: turn on MFA, change all passwords, and set up rules to only allow logins from trusted locations. Because the attack was so widespread, Snowflake announced that it would start requiring MFA for all users by default, taking a more active role in its customers' security. Several people believed to be responsible for the attacks were later arrested.

---

3. The Synnovis Attack: Putting UK Patients in Danger

What Happened?
On June 3, 2024, a ransomware attack on Synnovis, a company that provides lab testing services for major London hospitals, created a public health crisis. The attack shut down their systems, making it impossible to process blood tests and other critical diagnostics.

As a result, hospitals had to cancel thousands of operations and appointments, including cancer treatments and C-sections. The attack caused direct harm to nearly 600 patients and was even linked to one patient's death. This showed how a cyberattack can have real-world, physical consequences.

How Did the Hackers Get In?
The attack was carried out by a Russian-linked hacker group called Qilin. While the exact entry point wasn't officially confirmed, reports suggest the hackers got in by using stolen credentials on a system that lacked two-factor authentication. Once inside, they used their ransomware to encrypt Synnovis's files, making them unusable. They also stole nearly 400GB of sensitive patient data before launching the main attack.
How Was It Fixed?
The NHS declared a "Critical Incident" and had to divert emergency patients to other hospitals. Lab staff had to switch back to using pen and paper, which dramatically slowed everything down. When Synnovis refused to pay the ransom, the Qilin group leaked the stolen patient data on the internet. The recovery has been very slow, and the disruption to patient care is expected to last for many months as hospitals work through the backlog of canceled tests and appointments.

What We Can Learn

These three attacks, though different, teach us some important lessons:

- **Basic Security Is Crucial:** Two of the three attacks could have been prevented by a simple, common security measure: multi-factor authentication. Forgetting the basics can lead to disaster.
- **Your Partners' Security Is Your Security:** All three incidents involved a "supply chain" problem, where the security of one company depended on another. Businesses need to make sure their partners are secure and have a backup plan in case one of them gets attacked.
- **Hackers Have More Ways to Get Paid:** Hackers don't just lock up files anymore. They steal data and threaten to leak it, or they just steal it to sell. This means that protecting data from being stolen is just as important as preventing systems from being shut down.

To stay safe, organizations should focus on getting the fundamentals right: use strong authentication everywhere, assume any of your partners could be a security risk, and have a solid plan for what to do when an attack happens.