**Data Breach Analysis Case Study Paper**

**Syniverse Breach**

**Nutalapati Avinash**

**April 2022**

**Introduction to Syniverse Breach**

Identification of the Breach

**Breach Disclosure:**

Syniverse Security Filing:

On a quiet last Monday of September, Syniverse disclosed an SEC filing in which it stated that it is the victim of a 5-year long Data Breach. On the other hand, Syniverse describes itself as the world's most connected corporation and wants to merge with M3-Brigade Acquisition II Corp, which is a special purpose acquisition company, to become a publicly-traded firm.

However, Syniverse managed to not disclose any further information on the breach. The gathered information along with the possibility of the attack life cycle in comparison to the rumors has been presented in the below report. Syniverse, a critical component of the global telecommunications infrastructure used by AT&T, T-Mobile, Verizon, and several other companies around the globe, including Vodafone and China Mobile, revealed that bad vectors had been present in its systems for years, affecting 200 plus of its clients and potentially millions of cellphone users around the world. Syniverse is a company that routes almost 700 billion SMSs every year and generates over $600 million in revenue.

Bad Vector could have had access to metadata of Calls and SMSs. Syniverse is an exchange centre for mobile network operators to transfer billing information back and forth. Its customer records and personal identifying information might also have been compromised. Syniverse's infrastructure is used when a user travels across nations, a process known as roaming in the telecommunications industry. Syniverse is in charge of SMS/MMS routing between various telecommunications agencies around the world, allowing for roaming. Only two companies play a significant role in the SMS/MMS routine while travelling. Syniverse also assists its 1250+ customers with sending SMS to their end-users by providing the necessary infrastructure and services. Only their EDT (Electronic Data Transfer) system was compromised, according to the breach information released by Syniverse, while their SMS system remained stable. There have been no reports of business impact among Syniverse's customers or the company itself.

**Source and Motivation of the attack**

Many researchers have speculated that the attack was carried out by a state-sponsored attack organization, although no one has ever refuted this theory. The assault might be carried out by any country's spy agency to obtain the Metadata of the user's Call/SMS records. This data is almost identical to Edward Snowden's whistleblowing on the NSA's citizen data collecting. The US government has refused to comment on the incident, and Syniverse representatives have maintained a similar stance. Despite this, no individual or organization has claimed credit for the attack. The attack appears to be motivated by data theft related to telecommunications corporate giants, as well as monitoring users’ day-to-day actions and financial data. All SMS containing information about bill payments, delivery updates, and confidential MFA details such as OTP has been compromised. This information would be used by the Bad Actor to obtain access to MFA-enabled applications and user accounts. This information may be used by a government agency, such as the NSA, to create a social network map of most of the world. Some govt. intelligence agencies require meta-data like this than actual call recordings. The cost of analyzing voice traffic is high, and it might be distracting. Call and location data provide a very high return on investment in terms of value versus effort. Only individual calls involving specific targets are of interest in actual traffic (voice and data). Meta-data is highly valuable to intelligence organizations as it identifies and monitors their targets.

**Technical Details**

It discovered that an unknown individual or organization had gained illegal access to its EDT (Electronic Data Transfer). On multiple occasions, Bad Vector got access to its internal network's databases. It's anticipated that the data of about 235 customers have been exposed. You might then wonder why all of this data isn't secured. Because there is no value in doing so, and it would be unlawful in some circumstances. In the case of call detail records, carriers must share this information with their customers, and most countries require such information to be available on-demand in the event of subpoenas and warrants. There are far too many people who require access.

Is this to imply that this unidentified individual was hacking people's phones and playing man-in-the-middle with traffic? Most likely not. If a state actor is involved, the Syniverse breach might be the product of social engineering, false shell firms, infiltration, or even extortion. However, it appears to be an operational or procedural error rather than a technical one, and this person could be quite skilled. Karsten Nohl, a mobile security researcher and cryptography expert from Germany, has been seen quoting that so all of this is related to supply chain security, where it's been proven time and time again that you're more likely to be hacked by one of your suppliers than you are by yourself, due to the multiplier effect and he also stated that it's simple to label text messaging as unsafe.**1**

**SS7 Vulnerability**

Signalling Technology number seven (SS7) which is also referred to as Common Channel Signaling System 7 in the United States is a system that connects two mobile phone networks. It was created in 1975 and has numerous variations. The American National Standards Institute and the European Telecommunications Standards Institute design the protocols used by the majority of networks. It is used to initiate the majority of public telephone calls over PSTN around the world (Public Switched Telephone Network). To eavesdrop on voice and text communications, SS7 attacks take advantage of the authentication capabilities of communication protocols built on top of the SS7 protocol. According to telecommunications specialists, all a cybercriminal needs to begin an SS7 attack on a computer running Linux and also the SS7 SDK. When a hacker successfully executes a MitM phishing attack, they obtain access to the same amounts and categories of data that are typically reserved for security services. Hackers can get important information by listening in on phone calls and text messages, as well as tracking device movements.

1 Securityweek.com. 2022. Telecoms Giant Syniverse Discloses Years-Long Data Breach | SecurityWeek.Com. [online] Available at: <https://www.securityweek.com/telecoms-giant-syniverse-discloses-years-long-data-breach> [Accessed 8 April 2022].

One of the objectives of SS7 attacks is a standard security measure utilized by many. Because SMS messages are unencrypted and hackers know how to intercept them, two-factor authentication (also known as 2FA) through SMS utilizing SS7 is fundamentally faulty. A cyber-criminal may reset your password to Google, Facebook, WhatsApp, or even your bank account if they have the code from the SMS in their hands. It doesn't take a genius to figure out that mounting a man-in-the-middle MitM phishing attack requires very little experience and equipment. With the majority of organizations relying on cellular connectivity for communication, SS7 assaults are a serious threat. It's vital to realize that hackers aren't solely interested in proprietary or secret information. The growing number of IoT devices that rely on mobile networks to send data is widening the danger landscape. Such attacks can result in the theft or disablement of mission-critical devices and services, as well as potentially damaging breaches of confidential information. Manufacturers are doing too little to alert firms employing IoT devices about potential security vulnerabilities in their goods, given the high stakes. This leaves network operators vulnerable to assaults via hacked customer IoT devices on their network.

**The time between initial exploit and detection**

Syniverse found out that their databases were breached in May 2016, and that a bad vector had gotten access to the company's systems on several occasions. However, it took Syniverse 5 years to discover the attack. In the process of research regarding the hack, an employee named Gary, who worked with Syniverse for about 9 years has spoken about the attack in an open form providing more insight into the hack.

Gary says Syniverse is responsible for routing SMS messages between operators. However, the hack was related to a different part of their product. It wasn’t their SMS system, rather their Electronic Data Transfer system was the major point of the attack. EDT is linked to their roaming clearing product, which receives roaming usage records (TAP records) at the user level, transfers them from a roaming visiting mobile operator to the home mobile operator, and creates the corresponding invoicing.**2**

Threat actors find this incredibly useful since it allows them to develop travel profiles for users all around the world, including the country of trip and duration of travel. They can also see information such as who they call/receive calls from, call duration, text messaging to/from, and data volume while travelling. It includes the user's MSISDN and IMSI. What is the significance of this? With a mobile MSISDN and IMSI, all of those SS7 vulnerabilities you've heard about in the past, where phone conversations and text messages may be intercepted, become a very straightforward thing to perform. It informs the threat actor when and how SS7 MIM attacks should be launched. It's typical of government-sponsored activity. This is something she has been researching for a long time. This hack has enormous ramifications in terms of national security. Which could be considered as important information yet came out from a direct source.

2 Schneier on security. Accessed April 8, 2022. <https://www.schneier.com/blog/archives/2021/10/synaverse-hack.html>

Hereby we could conclude that the contents of the Hacked data are Metadata of the communications of Call and SMS information.

* Length of the Call.
* Cost of the Call.
* Callers, and Receivers Mobile Numbers.
* Content of the SMS.
* Location of the Calls.
* Travel history of international travellers.
* Call/SMS billing information.

**MITRE ATT&CK Framework**

To view the MITRE ATT&CK mappings, click on the below excel sheet.



**Response and recovery actions were taken by the Syniverse**

Syniverse spends a lot of money to protect itself from such dangers, and it may have to spend even more money to fix problems created by physical, technological, and cybersecurity breaches. Syniverse may not be able to install security measures promptly, or if they are implemented, they may be bypassed.

These events could result in operations being disrupted, increased lawsuit risks, misstated or misused financial data, and the loss of Syniverse's intellectual property. Furthermore, if any information about Syniverse's customers, such as payment information or personal data, was the target of or misappropriated in a successful cybersecurity attack against Syniverse, Syniverse could face investigations, litigation, or other claims from affected customers and data protection regulators in multiple jurisdictions. Furthermore, if another provider of mission-critical mobile communications services suffers a high-profile security breach or cyberattack, Syniverse's customers, suppliers, vendors, and prospective customers, suppliers, and vendors may lose faith in the security of these business models in general, harming Syniverse's reputation and brand image.

**Notifications to impacted users and authorities**

Syniverse has notified all affected consumers/customers of the illegal access where appropriate, and the company has determined that no further action, including consumer notification, is required at this time. According to Syniverse, there was no attempt to profit from the unauthorized behaviour, and there was no evidence of an intent to impair the company's or its guests' activities. Syniverse has not been informed of and does not expect, any significant impact from these events on its daily operations or services, or on its ability to penetrate or reuse data. Syniverse had and still has cyber insurance, which it anticipates to cover a large portion of its costs in investigating and responding to this incident.

**My assessment of the breach’s impact on regulations and industry, related breaches**

While Syniverse believes it has identified and adequately remedied the vulnerabilities that led to the above-mentioned incidents, there can be no guarantee that it will not discover evidence of data exfiltration or misuse of its IT systems as a result of the May 2021 Incident, or that it will not suffer a future cyber-attack with similar consequences. As a result of such exfiltration, customer data, Syniverse's trade secrets or other intellectual property, personal information of its employees, sensitive information of its customers, suppliers, and vendors, and material financial and other information related to its business could all be exposed or misappropriated. Any of this information being made public might have a significant negative impact on Syniverse's company, reputation, financial situation, and results of operations.

**What would I have done differently if I was handling post-breach procedures**

If I were in charge of the Post-Breach Procedures, I would call the Security, Network, and Infrastructure teams to discuss the breach and the steps taken throughout the investigation. I would have inquired as to what may be done better and any issues encountered during the mitigation/patching of the detected vulnerability and subsequent breach. Is patient number zero recognized and isolated? I'd gather all of the necessary information on the data leak and send each customer an individual note informing them of the breach. However, Syniverse has failed to notify government agencies and disclose all information as required by law. Among the found vulnerabilities responsible for the attack are Syniverse and other significant communications businesses.

Among the identified vulnerabilities responsible for the breach, it was discovered that Syniverse and other major telecommunication companies were still using the legacy EOL SS7 protocol, which I would try to upgrade to the most recent version or at the very least implement industry-accepted security tools/models to improve the company's overall security posture. Identify the gaps and instruct the staff/employees on the components of the breach that must be addressed. Risk analysis and cost estimation took place.

**Conclusion**

Syniverse announced the security vulnerability in an August SEC filing as it prepared to go public at a $2.85 billion valuation through a merger with M3-Brigade Acquisition II Corp., a special purpose acquisition company (SPAC). The corporation started with the statement that "no evidence of intent to disrupt its operations or those of its customers was observed, and no attempt to monetize the unlawful conduct was made."**3** Syniverse has not experienced and does not expect, any meaningful impact from these events on its day-to-day operations or services, or on its ability to access or process data.

3 Vice.com. 2022. *Company That Routes Billions of Text Messages Quietly Says It Was Hacked*. [online] Available at: <https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked> [Accessed 8 April 2022].

Syniverse has had and continues to have, cyber insurance that it expects to pay a significant percentage of its costs in investigating and responding to this incident. Syniverse may not be a household brand among customers, but it is one of the largest firms in the world when it comes to the telephone infrastructure that allows larger companies such as Verizon or AT&T to function daily. Given how much of a disaster Syniverse has become in recent years, it's honestly surprising that more stuff like this hasn't happened, the former Syniverse employee told Motherboard in 2019. The FBI and the FCC did not immediately respond to requests for comment. A request for comment was sent to CISA (Cybersecurity and Infrastructure Agency), which did not respond. AT&T, T-Mobile, Vodafone, Telefonica, China Mobile, and America Movil did not respond to a request for comment. Verizon has remained silent on the subject.

**Bibliography**

Vice.com. 2022. *Company That Routes Billions of Text Messages Quietly Says It Was Hacked*. [online] Available at: <https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked> [Accessed 8 April 2022].

Vice.com. 2022. *Inside SS7, the Insecure Global Cell Network That's Used to Track Phones*. [online] Available at: <https://www.vice.com/en/article/d73dzm/inside-ss7-the-insecure-global-cell-network-thats-used-to-track-phones> [Accessed 8 April 2022].

A step by Step Guide to SS7 attacks. FirstPoint. (2021, May 19). Retrieved April 8, 2022, from <https://www.firstpoint-mg.com/blog/ss7-attack-guide/>

Guardian News and Media. (2016, April 19). SS7 hack explained: What can you do about it? The Guardian. Retrieved April 8, 2022, from <https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls>

Fierce Wireless. 2022. Syniverse quietly reveals 5-year data breach. [online] Available at: <https://www.fiercewireless.com/wireless/syniverse-quietly-reveals-hackers-had-access-to-database-over-5-years> [Accessed 8 April 2022].

Securityweek.com. 2022. Telecoms Giant Syniverse Discloses Years-Long Data Breach | SecurityWeek.Com. [online] Available at: <https://www.securityweek.com/telecoms-giant-syniverse-discloses-years-long-data-breach> [Accessed 8 April 2022].

Todd, D., 2022. Massive Text Data Breach Could Have Circumvented 2FA. [online] Secureworld.io. Available at: <https://www.secureworld.io/industry-news/text-data-breach-2fa> [Accessed 8 April 2022].

The Verge. 2022. A text message routing company suffered a five-year-long breach. [online] Available at: <https://www.theverge.com/2021/10/6/22713543/syniverse-hack-five-years-text-messages> [Accessed 8 April 2022].

Schneier on security. Accessed April 8, 2022. <https://www.schneier.com/blog/archives/2021/10/synaverse-hack.html>

Schwartz, Mathew J., and Ron Ross. “Breach of Syniverse Reveals Yet Another Supply Chain Attack.” Data Breach Today. Accessed April 8, 2022. <https://www.databreachtoday.com/breach-syniverse-reveals-yet-another-supply-chain-attack-a-17692?rf=2021-10-08_ENEWS_SUB_DBT__Slot1_ART17692&amp;mkt_tok=MDUxLVpYSS0yMzcAAAF__4klLt3tLeJ3patf9dfSTe_uenO4xWAu5kUHBzNHYmvKFODY2elPgSkyf0csbSzyFHa9nGCD1ZfiWeJzr80FOHU-Mq7jPVJtn2SM0JA5evSZ71U>

Burgess, David Allen. “Who Is Syniverse, Anyway?” Medium. Telecom Experts, October 7, 2021. <https://medium.com/telecom-expert/who-is-syniverse-anyway-d102d6830059>

ATT&CK® navigator. Accessed April 8, 2022. <https://mitre-attack.github.io/attack-navigator/>