Threat Agent Profile:

**Organization: “**[**The Community**](https://www.justice.gov/usao-edmi/pr/international-hacking-group-members-sentenced-sim-hijacking-conspiracy-resulted-theft)**”**

**Samuel Hazlett**

**Overview:**

A hacker group using the alias “The Community '' were responsible for a cryptocurrency heist that resulted in the group stealing around 10 million USD. The group's methods of achieving their goal is known as “SIM Hijacking” or “SIM Swapping”. A technique that is used to exploit a common cyber-security weakness within cell phones. The group was able to achieve this goal by either bribery of an employee working for a mobile phone provider resulting in SIM Hijacking. Another method that was used by the group was to call the mobile provider pretending to be the victim and request the mobile number to be changed to another SIM card resulting in a SIM Hijacking. Thus “The Community” was able to gain access to mobile phone numbers accessing all of the victim’s phone calls and short message service (SMS) message data being routed to devices controlled by “The Community”.

The group's methods allowed them to gain access to many victim’s mobile numbers and was reported in different states such as “California, Missouri, Michigan, Utah, Texas, New York and Illinois”(*United States Attorney’s Office Eastern District of Michigan*). Once “The Community” had control of victim’s mobile numbers the group advertently was able to gain control of online accounts such as a victim’s email, cloud storage, and Crypto wallet/ exchange accounts. The group would then reset passwords in the accounts and were able to bypass two step verification. Although the exact price and of what crypto was stolen is theorized by victim’s to range anywhere from 50,000 to 9 million USD.

**Goals:**

Although there is no specific event that highlights “The Community’s” goals I think that the States that were targeted Usually have a lot more money compared to other states, as well as a higher population. Specifically New York, California, and Texas highlight that they weren’t picking at random; they had specific targets in mind. Unfortunately their goals were achieved and they were able to gain access to the accounts of the victim’s and were able to secure the victim’s data.

**Mode of operation:**

The group seems to choose victims that lived in higher income states resulting victim’s being chosen. Also being able to look up area codes of different states and being able to target those in higher income areas within the states themselves. Also with a few google searches you are able to view people’s Crypto accounts, some Crypto related sites allow you to see other viewers accounts which also could have resulted in targeting.

The operations were primarily carried out by malicious actors who engaged in fraudulent activities, disguising themselves as unsuspecting victims. Their modus operandi involved manipulating individuals into unwittingly altering a victim's phone number, redirecting it to a compromised SIM card controlled by the perpetrator. This nefarious scheme allowed the actors to gain unauthorized access to the victim's communication channels and sensitive information, thereby exploiting their digital presence for malicious purposes.

Another method employed by the clandestine group known as "The Community" involved the illicit practice of bribing employees working at mobile phone stores. Through these illicit dealings, these individuals breached the personal information of their unsuspecting victims without the victims having any awareness of the intrusion. These corrupt store employees, lured by financial incentives or other inducements, compromised the security and privacy of customers by unlawfully accessing and disclosing sensitive data, thereby facilitating "The Community's" unauthorized access to confidential information and perpetrating their unlawful activities under the cover of secrecy.

The methods employed by "The Community" represent a sophisticated variant of phishing attacks, a form of cyber deception that has become increasingly prevalent in the digital landscape. In their elaborate ruse, the group adeptly assumes the personas of their intended victims, skillfully mimicking their online identities and behaviors. By meticulously crafting these deceptive facades, "The Community" not only gains access to sensitive information but also creates a false sense of trust and familiarity, exploiting the unsuspecting targets who may interact with them believing they are communicating with legitimate individuals. This intricate blend of deception and manipulation underscores the insidious nature of their cyber operations, highlighting the importance of vigilance and cybersecurity awareness in today's interconnected world.

**Level of motivation:**

The level of motivation among these hackers is notably high, ranking at an impressive 5 out of 6 on the scale. This heightened motivation stems from the relative ease with which each hacker was able to acquire vast quantities of sensitive information from their victims. This apparent ease of access can be attributed, in part, to the concerning state of security surrounding mobile phones, which is perceived as being relatively low. The combination of lax security measures, coupled with the efficiency of their tactics, has emboldened these hackers to pursue their illicit activities with fervor, knowing that they can exploit vulnerabilities in the system to their advantage. This elevated motivation underscores the urgent need for comprehensive security improvements in the mobile phone industry to mitigate the risks posed by such determined and audacious cyber threats.

**Capabilities and Constraints:**

The hacker group "The Community" exhibited remarkable capabilities that enabled them to rapidly amass a substantial number of victims in a remarkably short period. Their success in this endeavor can be attributed to the rather blunt, yet remarkably effective, nature of their phishing tactics. By deploying straightforward and direct phishing techniques, "The Community" managed to cast a wide net in the digital realm, ensnaring a multitude of unsuspecting individuals with their deceptively simple but highly convincing schemes. This swift accumulation of victims underscores the group's proficiency in exploiting human psychology and security vulnerabilities, highlighting the need for enhanced cybersecurity awareness and robust defenses against such agile and opportunistic threat actors.

While the primary constraint faced by the group revolved around passwords, their adaptability and resourcefulness were evident in overcoming this hurdle. Despite the ever-expanding adoption of two-step verification as a security measure, "The Community" demonstrated their capability to circumvent these safeguards swiftly. Their approach involved cleverly resetting two-step verification settings, which included altering the authorized fingerprint or facial recognition data, granting them unauthorized access to the victim's accounts.

This maneuver was particularly effective in cases where their victims did employ two-step verification, as it allowed "The Community" to outsmart even the most stringent security measures. However, it's worth noting that individuals who had not activated two-step verification might have been more vulnerable, potentially providing a window of opportunity for the group to access their accounts with relative ease. This highlights the critical importance of implementing robust security practices, including two-step verification, to safeguard digital assets against increasingly sophisticated threat actors like "The Community."

**References:**

* Eastern District of Michigan , U. S. A. O. (2019, May 9). Nine individuals connected to a hacking group charged with online identity theft and other related charges. Eastern District of Michigan | Nine Individuals Connected to a Hacking Group Charged With Online Identity Theft and Other Related Charges | United States Department of Justice. <https://www.justice.gov/usao-edmi/pr/nine-individuals-connected-hacking-group-charged-online-identity-theft-and-other>
* Eastern District of Michigan , U. S. A. O. (2021, November 30). International Hacking Group members sentenced for SIM hijacking conspiracy that resulted in the theft of millions in cryptocurrency. Eastern District of Michigan | International Hacking Group Members Sentenced for SIM Hijacking Conspiracy That Resulted in the Theft of Millions in Cryptocurrency | United States Department of Justice. <https://www.justice.gov/usao-edmi/pr/international-hacking-group-members-sentenced-sim-hijacking-conspiracy-resulted-theft>