BlueVoyant

Threat Report
SIM Swapping

SIM swapping is an attack vector in which cybercriminals hijack an individual's mobile phone number to compromise their target's online identity. This attack requires substantial effort (and sometimes cost) from attackers. Therefore, high-net-worth individuals or those in positions of corporate, governmental, or social influence are typically the targets of SIM swapping. Executives, celebrities, politicians, and investors have been the victims of high-profile compromises since SIM swapping surged to prominence in 2018.

Scope of Threat: A cybercriminal with access to a target's phone number can perform SMS (text) password resets for critical accounts held by the target such as: webmail, cryptocurrency holdings, banking, social media, online shopping and services.

How it Happens

The attacker typically gains access to the target's mobile phone number by:

- Blackmailing, bribing, or socially engineering a cell phone service provider employee to leverage their access to customer information or the mobile network itself, or;
- Constructing a profile of the target that contains sufficient PII (personally identifying information) to falsely authenticate themselves to the target's cell phone carrier. This can be achieved through service provider data breaches or by compiling PII data breaches.

For more information, please visit us online at www.bluevoyant.com/professional-services.

SIM Swapping and Phone Number Porting

Criminal groups that specialize in SIM swapping attacks have increasingly shifted their efforts towards phone number porting. "Porting" is when a mobile device number is moved to another cell phone carrier.

This technique allows an attacker access to the compromised phone number for days, whereas SIM swapping is typically resolved within hours. While more difficult to achieve, porting gives the attacker more time to conduct their fraudulent activities.

Attack Mitigation

- Establish a PIN code for your mobile carrier account. This can add a protective boundary for attacks that have targeted your PII. Unfortunately, this does not protect against attacks conducted with the assistance of malicious insiders.
- Prioritize authentication applications over SMS-based two-factor authentication. Apps such as Google's Authenticator, Okta, or Authy are associated with your physical device, not just your phone number.
- Use a physical authentication key for your critical accounts. (Don't forget to also deactivate SMS-based authorization).
- Be vigilant. Major service disruption such as failed message delivery should be acted upon immediately.