www.pipelinepub.com
Volume 18, Issue 1

Minting a New Strategy: Lessons from a Security Breach

By: Dmitry Kurbatov

If history is any guide, the 2021 Mint Mobile breach will soon be forgotten (if it hasn't been already). This is one reason why breaches never seem to end: each attack is frozen in time, an unfortunate episode consigned to oblivion rather than used to chart the course ahead. In this case, it's almost worse—the hack wasn't even the most devastating or sophisticated or distinctive intrusion of its kind. Moving on to the next big bad thing is almost understandable.

But perhaps that's also why it should be taken seriously as a learning moment. If this breach was fairly common in many aspects, then we're likely to see more just like it. Rather than repress the memory and get past it, the best option is to use it to develop better defenses.

First, some background: Mint Mobile is a mobile virtual network operator (MVNO) selling phone services on the T-Mobile network. The company has been praised for its disruptive approach and has won accolades as a value carrier. In late 2019, it got attention far outside its traditional base when movie star Ryan Reynolds acquired an ownership stake.

Then, in mid-July of 2021, Mint Mobile notified certain customers that unauthorized parties had gained access to their account information, and that a small number of those subscribers were being temporarily ported to another carrier. There was no public acknowledgement or announcement, just a short email to an unspecified number of customers.

The message stated that "we immediately took steps to reverse the process and restore your service; an unauthorized individual potentially gained access to some of your information, which may have included your name, address, telephone number, email address, password, bill amount, international call detail information, telephone number, account number, and subscription features.” The email, unsurprisingly, sparked a flurry of Reddit comments and unanswered questions on the identity of the hacker(s) and their intended purpose.

Behind the scenes

Let’s pull back the curtain a little. Using this attack as a backdrop, how do cybercriminals go about putting these attacks into play?

Unfortunately, there are numerous strategies and entry points that hackers can use. For example, they can leverage an online subscriber's personal account or customer management system—if credentials are compromised, the hackers potentially gain full access to operations like number porting. They can also fake number porting requests to the customer service center and SIM swap-alike types of attack.

To be clear, we don’t yet know how many subscribers were (or will be) affected. But we can still game out some scenarios.

If very few subscribers were affected, the attack was most likely executed by compromising a subscriber's personal account or customer management system. The most effective method of compromising a personal account, even all these years into the digital era, is still a phishing attack. It may have also occurred through a social engineering operation. For example, a sophisticated hacker calls customer support, tells a tale of having lost a phone, and asks to change the SIM card, or otherwise fools the operator into restoring access to a customer management system. It’s very common, really simple, and highly effective—and how most SIM swap frauds take place.

If a larger number of customers were affected, hackers were perhaps able to get credentials for the CRM system used by the MVNO staff to deal with subscribers. This can also happen through bribing or otherwise involving an insider.

If huge amounts of data were leaked, it indicates a hacker gained access to company systems. When hackers can gain access to full customer databases (CRM, billing, and so on), it can mean they’ve acquired an administrator’s level of access. Of course, this may also have been achieved through a sophisticated phishing attack.

None of this is new or even surprising. Personal information is such a juicy target, and a pathway to so many avenues for monetization, that these attacks are sadly both routine and devastating. Nor is it only smaller players being invaded—global conglomerates have greater resources allocated for defense, yet they are just as likely to be compromised.

We all know that even the most sweeping attacks can fade from memory quite fast, often because there are inevitably worse episodes to worry about. But for those with a memory, let’s take a brief look back. In the summer of 2014, the customer portal at the French branch of mobile network operator and Internet service provider Orange France was hacked for the second time in a three-month period; 1.3 million users' data was stolen from the gateway of a software platform that sent promotional messages. In July 2017, millions of Verizon customers had their records exposed. The vulnerability was at Nice Systems, which facilitated customer service calls, and the records were breached through an unprotected Amazon S3 storage server. Later in the same year, T-Mobile identified a bug that allowed hackers to access customers' personal data, including the IMSI, a standardized unique number that identifies subscribers.

This list could be much longer, but the question remains: why do these attacks keep taking place?

Looking at why

It's simple—as with many other businesses, the information telecoms companies keep on their customers is a veritable goldmine. By themselves, details on names, addresses, phone numbers, passwords and more can be hugely valuable. But the benefits don't end there: this information helps hackers acquire two-factor authentication (2FA) codes, which are commonly used to help protect a given account from unauthorized access by requiring an additional code. For example, 2FA can support an email address authentication method. This makes a breach the gateway to even more confidential details.

Second, there's the issue of identity theft. While sometimes played for laughs in entertainment programs, this is in many ways the ultimate violation of personal space. In the digital era, the hijacked persona is used to commit a wide range of fraud and other crimes. It can take the victim months, even years, to undo the damage.

Mitigating these attacks is not simple, and no strategy is immutable. But even in the absence of guarantees, there are multiple steps organizations can take to make breaches far more difficult—ideally to the point where attackers will eventually give up trying.

Warding off the next breach

First, the security protocols must ensure that compromise of the customer management system is fundamentally impossible. Customer data isn't just a marketing tool, it's the number-one business asset; losing it undermines faith in the operation. This is an unacceptable risk for the mobile network operator.

There are some common-sense steps that can be taken here. For example, resist the temptation to collect every piece of data possible, and focus only on what's needed most to help marketing initiatives. This decreases hackers' interest and increases customer confidence. On a related note, limit access to this data—not every person in marketing needs to see it, and it helps security because every access point involves some potential vulnerability. Perhaps most importantly, ensure ongoing subscriber education about the perils of fraud, and encourage measures such as stronger passwords.

Second it is critical to monitor the technical aspect of unauthorized intrusions and develop behavioral analysis to respond in real time. There are technology offerings available for this vital function, and they constantly undergo innovation and enhancement. It's important for security professionals in this discipline to stay aware of the latest advances and make sure that all appropriate solutions are deployed.

This enables optimal visibility of users and their devices as they log on and empowers security professionals to verify compliance mandates in all environments: data center, cloud and more.

Finally, the porting procedure, which we may learn played a critical role in the Mint Mobile episode, must be implemented with greater security. As it stands now, even the most rudimentary social engineering techniques—many of which have been around for years—are surprisingly successful. When advanced technologies can be breached with simple tactics, there's clearly room for improvement.

Fortunately, there's a growing list of viable technologies, including multifactor authentication, biometrics, security PINs, behavioral heuristics and more. Rather than deploy a generic approach, MNOs can and should develop a mix of solutions that best meets their specific needs.

Looking ahead, adopting a security framework based on an industry standard model, such as NIST, is a good first step for a comprehensive approach to cybersecurity. The framework must have different components for identifying, protecting and detecting risks, and responding to and recovering from incidents.

Technologies now available can offer a comprehensive picture of activity within the entire network, identify security flaws and threats from the existing infrastructure, through virtualization, non-standalone 5G (NSA-5G) and all the way to a standalone 5G (SA-5G) network. Modern tools can automatically detect attempts to penetrate the OSS network and identify hacker presence on virtualized infrastructure based on multiple indicators including use of hacker tools and backdoor transmission of data to attackers' servers, which effectively nullify advanced persistent threats (APT).

But the work needs to go beyond implementing technologies. It's equally important to address security issues within mobile networks. This requires a comprehensive approach that should include, at minimum, assessment and monitoring. There are thousands of base stations around the world that need security testing. So do core networks, especially those running on virtualization infrastructure; vendors deliver solutions as a black box, making it difficult to uncover what is inside the infrastructure. Security must also be non-intrusive, supporting the process without becoming an obstacle.

There are no easy fixes here: telecom network security is a big issue and deserves big consideration. The endless parade of breaches suggests that even the small issues remain a problem. Changing this equation must be a top priority.