news

July 2020 hack – one of the biggest in Twitter's history

Paweł Wałuszko 05.08.2020

This July will go down as a really bad month in Twitter's history. Personalities and prominent public figures such as Barack Obama, Joe Biden, Jeff Bezos and Elon Musk – to name a few – got their Twitter accounts compromised. The cybercriminals didn't spare corporations either: Apple and Uber's accounts also joined the spamming efforts, publishing Tweets such as the one below, urging people to take advantage of a one-time offer to double their money in Bitcoins.

Screen capture of Apple's Twitter account post at the time of the attack.

Source:https://commons.wikimedia.org/wiki/File:Twitter_bitcoin_spam_apple_2020-07-15_(uncensored).png

Overall, about 130 accounts got compromised. This may not seem like a large hack in terms of data loss or the number of accounts breached, however, it's a very significant event in terms of who fell a victim and what could have happened. Tweets coming from global-ranking politicians and corporations could lead to tremendous political and financial outcomes, impacting millions (if not billions!) around the globe.

How did it happen?

Theoretically, all significant Twitter accounts ought to be protected by 2FA: the two-factor authentication system, which should be difficult to breach, as it requires two devices to be accessed at the same time (for example, aside from typing in a password, a user is be prompted to type in a one-time code sent via SMS, in order to log-in). In fact, 2FA has been available to Twitter users for a while now, so it's safe to assume that this feature was turned on.

On the other hand, so far Twitter has been cryptic: we know that about 130 accounts got breached and some of them (not all) engaged in spamming activity. Although there is very little information on how the hack actually happened, the cybersecurity community is discussing two possible ways of breaching 2FA, which could have been used.

SIM Swapping & social engineering

Given that most often 2FA is done through a smartphone – such as by sending one-time passwords to be typed in – obtaining access to the victim's phone would be the goal for the hacker. Technologically this is very difficult to achieve: in order to hack a phone, the attacker must possess expert knowledge about Linux, containers and app permissions, not to mention the ability to track down the appropriate device and, on top of that, convince someone to execute malicious code on the device. This requires expert-level knowledge, a good amount of time and excellent interpersonal skills. Creating a social engineering attack targeting the network provider, on the other hand, is much easier.

In order to carry out a successful social engineering attack on a mobile network provider, the hacker needs to do a little bit of research: find out the target's interests, basic information about their whereabouts, details about spouses and past relationships. Luckily for hackers, this information is readily available on social media. On top of social media findings, there's also the *darknet*, where entire databases of cross-examined data are available for sale and download, especially on prominent public figures.

Armed with this knowledge, hackers begin the social engineering attack by e-mailing or calling the network provider. By successfully answering a few verification questions – such as "where did you meet your spouse?" – they gain access to the administrative side of the account.

With a little bit of creativity, e-mail verification can also be circumvented. Hackers impersonate public figures and claim they lost their smartphone, which coincidentally, also has access to their e-mail account. The network provider, having successfully verified their client through a series of questions has no reason not to update the current e-mail address to something different. After all, they're acting in the client's best interest, by helping them get up and running in times of trouble.

In the meantime, hackers also ask for the phone number associated with the account to be transferred to a new SIM card, as "not to lose the current number". If the request is approved, they have a full access to all text messages, including those coming from 2FA. As such, 2FA of every account – whether it would be Twitter or online banking – can be broken within minutes.

The victim, in the meantime, can be temporarily clueless. The phone might stop working, but that could be blamed on poor reception or software issues. If the attack is carried out at night, the victim might be completely unaware of the situation for hours, allowing hackers to reset as many accounts and passwords as they'd like.

Insiders

The second way to break 2FA is a simple act of bribery. According to one of the leading mobile network providers in the US. – Verizon – about 34% of all breaches are a direct result of an "insider" within a company. In its yearly *Insider Threat Report*, Verizon outlines 5 types of insiders to watch out for:

1. **The Careless Worker** – someone who is misusing assets, intentionally or unintentionally circumventing policies and technological solutions
2. **The Insider Agent** – someone solicited and bribed from the outside
3. **The Disgruntled Employee** – someone who intentionally causes harm to the company and acts out of negative emotions (such as terminated employee)
4. **The Malicious Insider** – a person who steals data for personal gain
5. **Feckless Third Party** – business partners who compromise security through negligence.

When it comes to the July Twitter hack, most likely we're dealing with an *Insider Agent*, who got solicited and bribed by hackers, in order to sell the access to internal Twitter administration panel. This scenario is supported by the fact that the hacker group responsible for the attack published a series of screenshots of Twitter's internal administration tools – something which Twitter calls "Agent Tools" and "Twitter Services UI" – on the Internet (for legal reasons we will not publish them here). If indeed hackers had access to these tools, resetting passwords, e-mail addresses and phone numbers associated with 2FA would have been a breeze.

Everyone can become an Insider

It is entirely possible that the Twitter employee whose credentials were used to access the Twitter Services UI unknowingly aided the hackers in carrying out the attack. Thoroughly prepared social engineering attacks are highly effective in getting their subjects to comply, and even prominent tech leaders fall victims. A good example is the 2018 Jeff Bezos smartphone hack, which also started out as an elaborate social engineering attack aimed at Amazon's CEO and sent through the popular WhatsApp messenger.

Impacts and consequences

Regardless of how the 2FA model was broken, there most likely will be legal and operational consequences of this situation. If the hackers utilized the SIM Swapping method, network providers will have to think about phasing out the "answer a series of questions to remotely prove your identity" modus operandi, or at least supplanting it with something more secure. However, this will be difficult, as there's a fine line between account security and customer dissatisfaction that can be crossed. On the one hand, customers want security. On the other, ease of access and ability to remotely manage services is also important.

If the July Twitter hack is a work of an *Insider Agent*, legal and financial consequences are to be expected. After all, someone willingly jeopardized the company for their own gain. However, this is also not set in stone, as it will be difficult to prove whether (for example) the password leak happened intentionally or by an accident. Since transactions of this nature are usually done through the *darknet* and remuneration is paid in cryptocurrencies, it might be downright impossible to prove financial gain and malicious intent. Moreover, if the employee fell a victim to a carefully-constructed social engineering attack – depending on the jurisdiction and laws – they might be protected by specific labor laws, protecting employees working in good faith from exactly these types of situations.

All-in-all, the July hack wouldn't have happened if it wasn't for the human factor problem, which is well-known within the cybersecurity sphere. For Internet giants such as Twitter, this hack might go down as a minor embarrassment or a security mishap. Perhaps this incident will not impact their bottom line at all, aside from forcing some internal changes to how security is handled from hereon. For SMBs, however, a breach of this scale might result in complete confidence loss of customers and business partners. As such, it's always a good idea to educate employees and conduct regular security audits, just in case.

05.08.2020

Paweł Wałuszko

Business Development Manager and Cybersecurity Expert at TestArmy CyberForces. Experienced IT manager with background form the Silicon Valley; open-source enthusiast.

Konferencje cybersecurity 2020. Aktualna lista

Ransomware – to pay or not to pay