An IBM Hacker Breaks Down High-Profile Attacks

On September 19, 2022, an 18-year-old cyberattacker known as “teapotuberhacker” (aka TeaPot) allegedly breached the Slack messages of game developer Rockstar Games. Using this access, they pilfered over 90 videos of the upcoming Grand Theft Auto VI game. They then posted those videos on the fan website GTAForums.com. Gamers got an unsanctioned sneak peek of game footage, characters, plot points and other critical details. It was a game developer’s worst nightmare. In addition, the malicious actor claimed responsibility for a similar security breach affecting ride-sharing company Uber just a week prior. According to reports, they infiltrated the company’s Slack by tricking an employee into granting them access. Then, they spammed the employees with multi-factor authentication (MFA) push notifications until they gained access to internal systems, where they could browse the source code. Incidents like the Rockstar and Uber hacks should serve as a warning to all CISOs. Proper security must consider the role info-hungry actors and audiences can play when dealing with sensitive information and intellectual property. Stephanie Carruthers, Chief People Hacker for the X-Force Red team at IBM Security, broke down how the incident at Uber happened and what helps prevent these types of attacks.

“But We Have MFA”

First, Carruthers believes one potential and even likely scenario is the person targeted at Uber may have been a contractor. The hacker likely purchased stolen credentials belonging to this contractor on the dark web — as an initial step in their social engineering campaign. The attacker likely then used those credentials to log into one of Uber’s systems. However, Uber had multi-factor authentication (MFA) in place, and the attacker was asked to validate their identity multiple times. According to reports, “TeaPot” contacted the target victim directly with a phone call, pretended to be IT, and asked them to approve the MFA requests. Once they did, the attacker logged in and could access different systems, including Slack and other sensitive areas. “The key lesson here is that just because you have measures like MFA in place, it doesn’t mean you’re secure or that attacks can’t happen to you,” Carruthers said. “For a very long time, a lot of organizations were saying, ‘Oh, we have MFA, so we’re not worried.’ That’s not a good mindset, as demonstrated in this specific case.” As part of her role with X-Force, Carruthers conducts social engineering assessments for organizations. She has been doing MFA bypass techniques for clients for several years. “That mindset of having a false sense of security is one of the things I think organizations still aren’t grasping because they think they have the tools in place so that it can’t happen to them.”

Social Engineering Tests Can Help Prevent These Types of Attacks

According to Carruthers, social engineering tests fall into two buckets: remote and onsite. She and her team look at phishing, voice phishing and smishing for remote tests. The onsite piece involves the X-Force team showing up in person and essentially breaking and entering a client’s network. During the testing, the X-Force teams attempt to coerce employees into giving them information that would allow them to breach systems — and take note of those who try to stop them and those who do not. The team’s remote test focuses on an increasingly popular method: layering the methods together almost like an attack chain. Instead of only conducting a phishing campaign, this adds another step to the mix. “What we’ll do, just like you saw in this Uber attack, is follow up on the phish with phone calls,” Carruthers said. “Targets will tell us the phish sounded suspicious but then thank us for calling because we have a friendly voice. And they’ll actually comply with what that phishing email requested. But it’s interesting to see

attackers starting to layer on social engineering approaches rather than just hoping one of their phishing emails work." She explained that the team's odds of success go up threefold when following up with a phone call. According to IBM's 2022 X-Force Threat Intelligence Index, the click rate for the average targeted phishing campaign was 17.8%. Targeted phishing campaigns that added phone calls (vishing, or voice phishing) were three times more effective, netting a click from 53.2% of victims.

What Is OSINT — and How It Helps Attackers Succeed

For bad actors, the more intelligence they have on their target, the better. Attackers typically gather intelligence by scraping data readily available from public sources, called open source intelligence (OSINT). Thanks to social media and publicly-documented online activities, attackers can easily profile an organization or employee. Carruthers says she's spending more time today doing OSINT than ever before. "Actively getting info on a company is so important because that gives us all of the bits and pieces to build that campaign that's going to be realistic to our targets," she said. "We often look for people who have access to more sensitive information, and I wouldn't be surprised if that person (in the Uber hack) was picked because of the access they had." For Carruthers, it's critical to understand what information is out there about employees and organizations. "That digital footprint could be leveraged against them," she said. "I can't tell you how many times clients come back to us saying they couldn't believe we found all these things. A little piece of information that seems harmless could be the cherry on top of our campaign that makes it look much more realistic."

Tangible Hack Prevention Strategies

While multi-factor authentication can be bypassed, it is still a critical security tool. However, Carruthers suggests that organizations consider deploying a physical device like a Fido2 token. This option shouldn't be too difficult to manage for small to medium-sized businesses. "Next, I recommend using password managers with long, complex master passwords so they can't be guessed or cracked or anything like that," she said. "Those are some of the best practices for applications like Slack." Of course, no hacking prevention strategies that address social engineering would be complete without security awareness. Carruthers advises organizations to be aware of attacks out in the wild and be ready to address them. "Companies need to actually go through and review what's included in their current training, and whether it's addressing the realistic attacks happening today against their organization," she said. For example, the training may teach employees not to give their passwords to anyone over the phone. But when an attacker calls, they may not ask for your password. Instead, they may ask you to log in to a website that they control. Organizations will want to ensure their training is always fresh and interactive and that employees stay engaged. The final piece of advice from Carruthers is for companies to refrain from relying too heavily on security tools. "It's so easy to say that you can purchase a certain security tool and that you'll never have to worry about being phished again," she said. The key takeaways here are:

- Incorporate physical devices into MFA. This builds a significant roadblock for attackers.
- Try to minimize your digital footprint. Avoid oversharing in public forums like social media.
- Use password managers. This way, employees only need to remember one password.
- Bolster security awareness programs with particular focus on social engineering threats. Far too often, security awareness misses this key element.
- Don't rely too heavily on security tools. They can only take your security posture so far.

Mark Stone – Security Intelligence