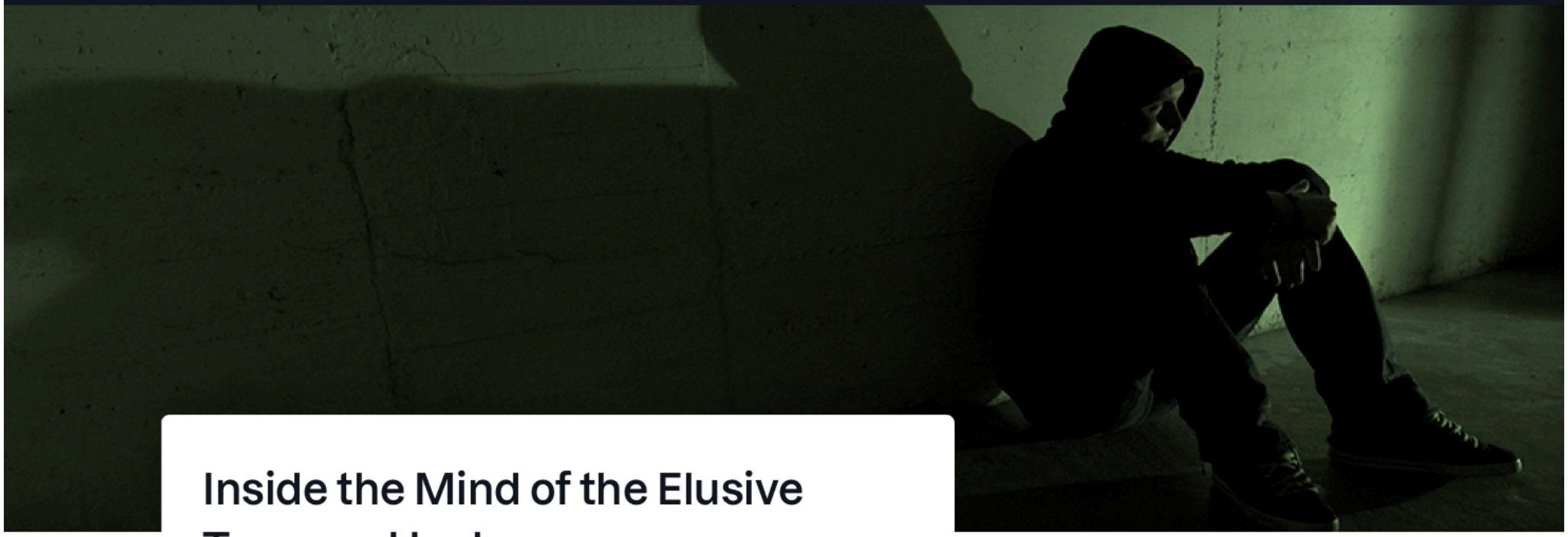

Inside the Mind of the Elusive Teenage Hacker

The attack on Uber by a 17-year-old hacker is a throwback to the old days of exploits, when attackers sought fame more than fortune. How should CISOs respond?

Perspective

DECEMBER 14, 2022

When Uber was **hacked in September**, it certainly wasn't the first time the ride-sharing company's systems had been breached, nor the **most serious** in terms of lost data. But it may have been the most humiliating.

Among other things, the attacker gained full administrative access to multiple Uber cloud platforms and accessed the company's financial data. Unlike most modern hackers, however, he didn't just steal data or hold it for ransom. He logged on to Uber's internal Slack and boasted about it. He went on to post links to pornographic images in the channel, as well as demand that the company pay its drivers better.

Then, as proof of the exploit, the attacker shared with security researchers **screenshots of system administrator control panels** he'd accessed using credentials stolen from an Uber senior engineer, posting on a Slack channel for white-hat hackers working on the side of companies.

Identify and contain adversaries before they can spread across your network.

"Bruh you breached Uber?" said a major malware aggregator to the hacker, in an alleged conversation shared on a Twitter thread.

When the alleged attacker was arrested by authorities in the U.K., he turned out to be a 17-year-old who is also suspected of obtaining the source code for the upcoming video game *Grand Theft Auto 6*. The teen from Oxfordshire is believed to be a member of the infamous Lapsus$ extortion group, whose members range in age from 16 to 21 and which has claimed Microsoft, Nvidia, and Okta among its victims. The Cyber Safety Review Board, a public-private arm of the U.S. Department of Homeland Security, **announced** earlier this month that it plans to issue actionable recommendations, like it did for the **first time** in 2022 with the **Log4j attacks**, for how organizations can protect themselves from the devious strategies of Lapsus$–style hacks.

15

The age of a hacker who, in 1982, wrote the first malware released in the wild

For overworked and under-resourced CISOs, hacks by people barely old enough to drive adds yet another threat to worry about: a new generation of bad actors who are doing it to show off for their friends (as with the Lulz hacking group in the old days) as much as for profit, and whose targets and attack vectors may be more difficult to anticipate.

New dogs, old tricks

If this all sounds strangely familiar, there's good reason.

Long before cybercrime became a **multitrillion-dollar** industry, hacking was something teenagers did for fun—to test their cyber skills, prove their geek street cred, or play pranks on friends.

Dan Tynan

Dan Tynan is an award-winning journalist whose work has appeared in Adweek, Fast Company, The Guardian, Wired, and too many other publications to mention.

Key takeaways

- Unlike older hackers, teens are often motivated by things like embarrassing a company and showing off their skills.
- They may also be members of criminal gangs that hack for fun as well as profit, making them tougher to anticipate.
- CISOs must adopt good cyber hygiene and zero trust approaches to prevent lateral movement.

Focal Point

Dedicated to helping business executives and IT leaders effectively use technology to connect with customers, empower employees and achieve better results.

> **Teenagers have always been interested in getting into things they shouldn't. And they tend to have both overwhelming curiosity and a feeling of invincibility.**
>
> Chris Prewitt, CTO/CISO, Inversion6

In 1982 the first malware released in the wild was called Elk Cloner. The virus was written that year by a 15-year-old named **Rich Skrenta**, who spread the code via floppy disk. It displayed a poem on Apple II computer screens and was utterly harmless.

It would be almost two decades before hackers created malware to intentionally steal data, and another half-dozen years before they developed the first **ransomware** software.

Now things appear to have come full circle, notes Chris Prewitt, CTO/CISO for Inversion6, a cybersecurity risk management provider. Like many CISOs, Prewitt grew up hacking, using "war dialers" to scan every local phone number to identify modems to target.

"Teenagers have always been interested in getting into things they shouldn't," Prewitt says. "And they tend to have both overwhelming curiosity and a feeling of invincibility."

[Read also: Before reporting on teen hackers, journalist Dan Tynan delved into the world of 'vishing'—an insidious way to trick unsuspecting workers into divulging sensitive data]

The key difference between then and now? Social media, especially YouTube and TikTok. In the past, hackers might be famous among their peers on a bulletin board or internet relay chat (IRC) group devoted to hacking, notes Prewitt. Now the audience is the world.

A search for "uber hacker" on TikTok turns up more than 5,000 videos with millions of views combined. (Online video also provides a rich source of tutorials for aspiring hackers, Prewitt says.)

"What's different is the amount of exposure someone can get for one of these 'stunt hacks,' " adds David Maynor, senior director of threat intelligence at Cybrary, a security training platform. "Ten or 20 years ago, a few niche communities might take note, but now it's part of the 24-hour news cycle with worldwide reach. For hackers looking for validation of their skills, you can't get a bigger stage than that."

For love or money?

The notion that young people are back to hacking simply for fun or notoriety is almost refreshing, says **Sam Curry**, a 23-year-old independent security researcher who began his career finding software errors as a **bug bounty hunter** when he was **still in high school**.

Curry communicated with the Uber hacker, aka "TeaPot," via the messaging app Telegram and confirmed the details of the attack.

> **Bruh you breached Uber?**
>
> A major malware aggregator

"Doing security stuff is such an easy way to feel important and boost your ego," says Curry. "If this person is part of Lapsus$, then he already has access to millions of dollars. He could honestly be tired of making money and just want to have fun."

TeaPot used login credentials stolen from an Uber contractor, then attacked weaknesses in the company's **multifactor authentication** process—repeatedly pinging the contractor to approve access until he or she finally gave in. From there, he managed to **move laterally** through the network, accessing multiple systems along the way.

[Read also: Some hackers don't stop at pinging—the business email compromise is a lucrative scam as close as your inbox]

MFA fatigue is a real problem, says John Gunn, CEO of Token, which is developing a ring that authenticates users based on their fingerprints. A good way to thwart attempts to hack single sign-on systems that allow users to access multiple platforms is to use authentication methods that can't be attacked remotely, such as biometrics, says Gunn.

Mounting a defense against Gen Z hackers

One difference between younger and older hackers is that the young guns tend to have a lot more time on their hands, Gunn adds. They might be willing to spend four to six months working on different techniques to find a way in. Otherwise, they're not really doing anything unique.

> **The best way to deal with hackers is to put them to work.**
>
> David Maynor, senior director of threat intelligence, Cybrary

The solution to protect against teen hackers is the same as those used to guard against professional cybercriminals and nation-state actors: good **cyber hygiene**.

CISOs can't protect everything equally, so they need to prioritize risk, determine which data and systems are most critical to business operations, and focus their resources on those, adds Prewitt.

[Read also: 5 steps to securing your organization's 'crown jewels' of data]

"What kind of business are you in from a risk perspective?" he says. "Which kinds of adversaries will want to attack you? In my experience, it's not that CISOs aren't managing the security technology well; it's that they don't understand the business well enough to know how to protect it."

Adopting a **zero trust** framework can also make it harder for attackers to move laterally once they've gained access, Prewitt says. That can reduce the attack surface and limit damage significantly.

Another way to handle young attackers? Hire them, says Maynor of Cybrary.

"I genuinely believe the best way to deal with hackers is to put them to work," he says. "CISOs should know that if the hacker hasn't committed serious crimes, he or she could be a perfect intern or entry-level employee."

Related

RSAC 2023 Preview: What CISOs (Need to) Know About Board Accountability

Report: Last Year's Top Finserv Cyber Threats to Intensify in 2023

What the Tech Sector Can Learn From TikTok: Trust Is Everything