THREAT ACTORS: CYBER CRIMINALS

Threat Actors: Cyber Criminals - CyberVista

April 4, 2017

Welcome to the second installment of our Threat Actor Profile series, where we analyze the main categories of actors that represent a threat to your organization. This series is designed for executives. Because we understand the unique roles and responsibilities of executives and corporate leadership, we're focused on cyber risk as an enterprise risk—and help explain it without getting lost in the weeds. Our second threat actor group is cyber criminals.

The Hacks You've Heard Of, The Hackers You Haven't

You've probably become familiar with their exploits by watching the news: they're disruptive, unpredictable, and can do millions of dollars in damage. Hackers for hire, botnet operators, tech-savvy identity thieves, and cyberterrorist groups: all are considered types of cyber criminals.

This class of attackers is the most prolific and diverse. They operate independently, in small teams, or in sprawling syndicates. While nation state actors hack to project power and influence, cyber criminals tend to target organizations for financial gain. They search for valuable financial information and personal data, such as healthcare or banking records. Their attacks also involve stealing user credentials for paid services, as well as collecting Personally Identifiable Information (PII) like names, addresses, social security numbers, and credit card data. Equally as valuable are attacks targeting proprietary information: the crown jewels of any organization.

The 2014 JPMorgan Chase (JPMC) hack was one example of a large-scale operation by cyber criminals. Three individuals managed to cause more than $100 million in damage as part of a plan to start their own stock brokerage business. The hack remains the largest cyber attack on a financial institution in history.

“A Brave New World of Hacking For Profit”

In July of 2014, JPMorgan Chase’s security team discovered that more than 1 million customer accounts were accessed by an unknown entity. Worse still, that intruder had been moving, undetected, through their network for more than a month.

JPMorgan Chase quickly disclosed the breach to customers and brought the FBI on board to track down the attackers. One important factor complicated the recovery, however: the incident defied the expectations of the investigators, who initially and mistakenly assumed that the attack was linked to the Russian government. The information that the attackers stole seemed strange to law enforcement: even though the hack affected a financial institution, no financial records were taken – just PII.

It took several months to discover the actual culprits of the hack: two Israelis and an American. The cyber criminals exploited several known vulnerabilities – which were unpatched on JPMC computers – to initially break into their network. Despite JPMorgan Chase’s rapid response, the attack still took years to recover from due to the abnormal attack profile, scale of the intrusion, and sensitivity of the compromised data.

The FBI soon learned that the JMPC breach was just the tip of the iceberg. In total, the same group of hackers had targeted nine other financial institutions alongside JPMorgan Chase. E-Trade, Ameritrade Holding Corp, Dow Jones, Fidelity Investments, and Scotttrade were all compromised as part of the combined attack – but they didn’t realize it until the JPMC investigation was underway.

The three hackers weren’t just using the information to gain insight into the stock market; they were at the center of a complex web of illegality. Using the data stolen from the financial institutions, they set up hundreds of fake identities and dummy accounts, building up a fraudulent investment business. According to law enforcement, they would game the system by first buying up penny stock. They would then “blast out misleading emails to dupe others into buying a company’s stock too and quickly drive up its price.” Inevitably, there was a crash – but the attackers had already cashed out.

The attackers’ criminal portfolio also included operating an online gambling business, an unlicensed Bitcoin currency exchange, and a “shady firm that processed payments for illegal pharmaceutical suppliers.” According to Preet Bharara, the U.S. attorney in the Southern District of New York who prosecuted the case, the incident “showcases a brave new world of hacking for profit. It was securities fraud on steroids.”

Cyber Criminals: Resourceful and Unpredictable

The biggest mistake organizations can make about cyber criminals is underestimating them. Incorrect assumptions about the capabilities of the JPMorgan Chase attackers was one major misstep in the investigation. Because the breach was so massive and impacted so many organizations, law enforcement incorrectly assumed that a nation state must have been behind it.

Every organization has valuable information, so any organization can be targeted by cyber criminals. Moreover, even smaller-scale attacks can cause millions of dollars in damage.

Executive Actions and Considerations

- **Patch early, patch often.** Every hack starts with an initial intrusion, so prioritize improving your defenses. The JPMorgan Chase attackers used known vulnerabilities to gain unauthorized access. Closing these gaps in your security takes diligence, but it's a simple process that can make all the difference. Support your security team and ensure they have the tools and know how to patch.
- **Be adaptable.** The threat environment is constantly changing. Make sure your security team stays apprised of attacks directed at your industry partners by checking the annual threat reports published by credible cybersecurity companies, including Verizon's "Data Breach Investigation Report" (DBIR) and FireEye's "Annual Cyber Threat Reports." Ensure you are briefed quarterly.
- **Don't forget about "Haxposure."** While the JPMorgan Chase hack involved the theft of PII, cyber criminals also steal internal secrets and embarrassing information about companies. Leaks damage an organization's reputation and destroy customer trust, which can be difficult to rebuild. A culture of security must start at the top. Make sure the entire company participates in security awareness and cyber best practices.