CS 6261: Security Incident Response

The Grinch Case Study

Minjoo Kim
Georgia Institute of Technology
Atlanta, GA, USA
Email: mkim908@gatech.edu

Working with law enforcement had no benefit to Georgia Tech from an incident response perspective, but did aid other organizations and ultimately led to the arrest of those responsible and substantial degradation to the broader crime ring. Would you have chosen to partner with law enforcement, allowing the attackers to persist in the environment, or only address the incident for Georgia Tech? Please explain your decision.

I would have chosen to partner with law enforcement, even if it meant allowing the crime ring to persist in the environment for a limited time.

First and foremost, allowing attackers to remain in the system was somewhat acceptable because the security team was able to control the risk. The security team was able to detect anomalies early and prevent the crime ring from damaging the system or spread malware. The crime ring's methods were not to sophisticated and the security team was able to secure the known compromised accounts while monitoring attacker's behavior through VPN and log management.

While only addressing the incident for Georgia Tech could have alleviated immediate risk, Georgia Tech was not the only target of the crime ring; it was a whole operation that targeted numerous organizations simultaneously. It could have been possible for Georgia Tech to just block the accounts every time the schools receive similar attacks, but it would not have been possible to address the root cause of the attack if law enforcement was not involved.

Bringing in the FBI made it possible for investigators to get a holistic overview of what was happening. Also, it was able to connect this specific case across multiple agencies that have become a target for this specific crime ring, which could not have been possible for Georgia Tech to do alone. Although this partnership did not necessarily have the school stop the attack faster, it was certainly conducive as a preventative measure that could deter future harm to Georgia Tech and other institutions.

How does understanding how a crime ring operates aid in incident response processes?

Having a profound knowledge of how each crime ring operates can greatly bolster the security incident response process by helping the security team understand the full pattern of the attack and respond accordingly.

First, Georgia Tech was able to understand that the crime ring in question was not too sophisticated and was not technically adept. Only a few people in the ring were actually able to perform rudimentary phishing attacks, which were even worse than periodic phishing email exercises done at Georgia Tech. Even simple training in phishing email was more than enough to deter future attacks.

The school was able to figure out how the money was getting stolen from which accounts. The attackers often used the credentials to make changes in their payrolls, commit tax fraud, and more. It was also notable that they did not necessarily target the highest paid employees within the school. Understanding their target helped the security team realize where they were going to be attacked. Ultimately, the team was able to take preventative measures to deter future attacks; some examples include resetting passwords, applying two-factor authentication, and more.

Knowing how the group operated allowed Georgia Tech to learn that simply blocking individual accounts was not enough to solve this problem. The crime ring often reused accounts and techniques across multiple targets. If Georgia Tech was not aware of this tactic, it would have just encouraged the targets to just reset their passwords while the attack would continue elsewhere.