Casino plays its cards right to avoid hacking

AT A GLANCE

Long considered to be the leaders in physical security, casinos have adapted to the increasing demand for network and internetwork connectivity for gambling devices and backend systems. For example, slot machines communicate with each other inside a casino and between casino properties. Loyalty reward points systems act in a similar fashion. Combine these technologies with high staff turnover and initial security strengths can weaken as network vulnerabilities allow attackers to work around these physical barriers.

CLIENT CHALLENGE

For one casino, the protection of their guests, infrastructure, and revenue was their mission. Physical security was implemented, but changes in infrastructure, staff, and technology over the years created uncertainty about the strength of network security and the design of the network architecture. While the casino had experienced minimal issues, an assessment of how their people, processes, and technologies would handle a targeted attack by a concerted threat agent was needed.

APPROACH

The casino engaged Coalfire to perform a complete red team attack. The scope for testing included all physical, social, and logical vectors of attack. Coalfire began the attack by harvesting email addresses of employees from public Internet sources, including social media, press releases, and corporate directories. Using these email addresses, Coalfire then performed a successful spear-phishing attack, gathering a handful of logins and passwords. With these stolen credentials, Coalfire consultants gained access to the internal network via the casino's VPN. Then by exploiting vulnerabilities found throughout the network, Coalfire ultimately gained administrator-level access to the environment.

RESULTS

The access gained was not merely technical, and the impact was huge. It was used to access hotel guest information through the reservation systems, and it allowed Coalfire to add points to the consultants' reward cards that could then be converted to cash. The Coalfire team also gained access to vault and cashier cage computers sufficient to set up a false line of credit and perform wire transfers at will, plus provide complimentary meals and services. Finally, the team demonstrated access – yet stopped short of attacking – the gaming and slot machine networks.

To prevent similar attacks from being carried out by real adversaries, Coalfire provided specific strategic and tactical recommendations that were prioritized and tailored to the environment. Stronger password policies, improved user awareness training, and two-factor authentication were cost-effective recommendations that virtually eliminated the threat posed by external attackers. Further recommendations also included testing domain and network architecture, developing an incident response plan, and establishing software audit and alert procedures. As a result, they increased the security strength to repel an insider threat and the ability to detect and respond to unknown future attacks.

THE ELEMENTS OF RED TEAM PENETRATION TESTING

Coalfire's red team testing provides you with the ultimate real-world test of your people, processes, and technology. Throughout the course of testing, Coalfire's experts identify and exploit weaknesses throughout the physical, social, and logical environments of your company to evaluate the effectiveness of your security program.

> ***"We thought [our] security program was among the best in the industry. This proved how our entire operation could be brought to a halt in the matter of a few days. We have moved quickly on the recommendations made by Coalfire and have been able to eliminate the possibility of these attacks to negatively impact us."*** **—CASINO EXECUTIVE**

Red teaming a company includes multiple attack vectors from:

- **Social** – Locate email contact information of employees at various levels and deploy spear-phishing campaigns to gain login credentials and access to systems through email and phone attacks.
- **Physical** – Perform in-person attempts to exploit physical access controls such as locks, alarms, staff, or "kiosks" to access your network and internal systems.
- **Technical** – Exploit vulnerabilities found in applications, hosts, or networks.

Coalfire's penetration testers are certified to assess target networks and systems to find security vulnerabilities using industry best practice technical and non-technical techniques.

About Coalfire

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. **www.coalfire.com**

COALFIRE