Scattered Spider Case Study

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

In the unnamed major hospitality company, the threat group caused as much disruption as possible after failing to deploy their ransomware. What implications does this have for IT and Security teams developing incident response processes?

The case with the unnamed major hospitality company demonstrates that IT and Security teams must design incident response processes if attackers can still cause as much damage as possible regardless of their failure in deploying their ransomware. It is advisable that IT and Security teams must still adhere strongly to the cybersecurity standards and security incident procedures, such as segmenting the network for quick isolation/containment of threats, strong backs, and recovery procedures. The early detection of their vulnerabilities and making sure that those vulnerabilities are addressed also help to block as much threat as possible. Together, they should be able to help improve operational and financial impact for future security incidents.

Groups such as Scattered Spider and Lapsus$ have demonstrated an impressive ability to gather intelligence and conduct thorough reconnaissance on their targets. What steps can organizations take to mitigate the risks of social engineering attacks?

Groups such as Scattered Spider and Lapsus$ used harvest credentials to add a two-factor authentication token through a support method weakness. Subsequently they accessed users' emails through a legacy one-factor protocol to verify the new token. As legacy one-factor protocol clearly demonstrates vulnerabilities to cybercrimes, it is apparent that IT and security teams must transition the entire systems to the new multi-factor authentication framework. Also, they must require strict identity verifications before allowing anyone to make changes in their accounts, such as adding new tokens or extra trusted devices. This can include processes such as obtaining manager approvals, callback procedures, and more. Finally, all email and cloud services must enforce strict authentication standards as well. Since these services are often utilized to reset passwords and verify identities, compromising these could allow cybercriminals to target multiple systems.

While both MGM Resorts and Caesars Entertainment faced cyber attacks, they responded to the incidents in distinct ways. How did their approaches differ, and what factors contributed to these divergent strategies?

Both MGM Resorts and Caesars Entertainment were targeted by what appeared to be the same cybercrime groups. MGM decided not to pay a ransom, but it had to shut down most of its IT operations for weeks and work with external cybersecurity consultants to recover their systems.

On the other hand, Caesars chose to pay $15 million in ransom to restore its systems as quickly as possible, most likely because it determined that paying would be a net benefit compared to prolonged disruption of their IT operations. In fact, Caesars' SEC 8-K filing stated that the payment had virtually no material effect on its financial condition. Although paying ransoms may incentivize threat groups to continue their unlawful activities, it may have been the optimal choice for both companies to minimize customer impact, and avoid extended revenue losses, especially given its strong financial position and the high costs associated with long term system outages.