Intranet feature story

X-Force IRIS thwarts heinous cyberattack on IBM Security client

It happened on a sunny Saturday afternoon last May. Kurt Rohrbacher, North America Lead, IBM X-Force Incident Response & Intelligence Services (a.k.a. IRIS), was hosting a barbecue when, just as his guests were arriving, his phone rang. It was his colleague Matt DeFir, an IRIS team lead. A suspicious threat was possibly moving into position for a full throttle attack on an IBM Security client.

IRIS: Prevent, detect, respond
Matt and the IRIS team were ready. They were used to swooping in to offer immediate help for clients with IBM Security Vision Retainers. Executives had called the IRIS Emergency Hotline, which set the IRIS team in motion. Using Carbon Black Response (CBR), the IRIS team learned that the attacker already had domain administrator level access to multiple systems in the client's IT environment, indicating a much broader incident than originally thought.

CBR intelligence data was pointing to the same threat actor responsible for several large-scale cyberattacks on Norsk Hydro, one of the world's largest producers of aluminum. The attacks ultimately paralyzed the company's computer networks, costing it some 450 million Norwegian crowns ($52 million) in damages. In the case of the IBM Security client, team experts surmised that the threat was probably financially motivated due to the company's extensive e-commerce platform and credit card access.

Elite 'undercover' force
Some might say that X-Force IRIS is IBM Security's best kept secret. The team is comprised of industry-leading, highly skilled security professionals experienced in investigating the world's largest breaches in both the public and private sectors.

IRIS teams often work as an elite undercover security force for clients to ensure that the right services and processes are in place. Then potential threats can be quickly identified, existing threats detected and contained, and in worst-case scenarios, response plans coordinated ahead of time.

Disaster averted
On that fateful Saturday afternoon, the IRIS team once again detected suspicious activity. Matt described to Kurt how the attacker had begun uploading "signed" ransomware (which cannot be detected by common security tools), and associated deployment scripts, ready to be pushed to more than 5,000 systems within the client's environment.

The IRIS team quietly went into stealth mode using Carbon Black to collect endpoint information, and QRadar to analyze network events, immediately blocking any execution of ransomware being deployed. At the same time, the client jumped into action, using their incident response playbook, blocking similar IP addresses at their firewall and resetting domain administrator level passwords, among other predetermined tactics.

Although the attack was successfully prevented in under eight hours on the same day, the job was not yet done. The team knew that the attacker was still present within the client's environment and could make another attempt at any time.

Follow the sun
The team used its "Follow the Sun" model to enable round-the-clock monitoring of the

client's environment. As the sun set in North America on a Saturday night, monitoring operations were smoothly transitioned over to the AP IRIS team. Says Kurt, "Our client came very close to taking a huge hit on their technology, resources, and revenue, not to mention extensive brand damage."

Lessons learned: Vision Retainers

"The advanced planning and ongoing communications put in place with a Vision Retainer are invaluable," says Ahmed Saleh, IRIS Global Partner & Director. "It truly enables IBM to showcase the client value of IRIS." Vision Retainers are a great tool, and important first step, for sellers interested in developing long-term relationships that lead to other opportunities.