DenaliTEK Stops Cyber Attack for Local Energy Consulting Firm

17:27 EST SOC alerts to a suspicious PowerShell.

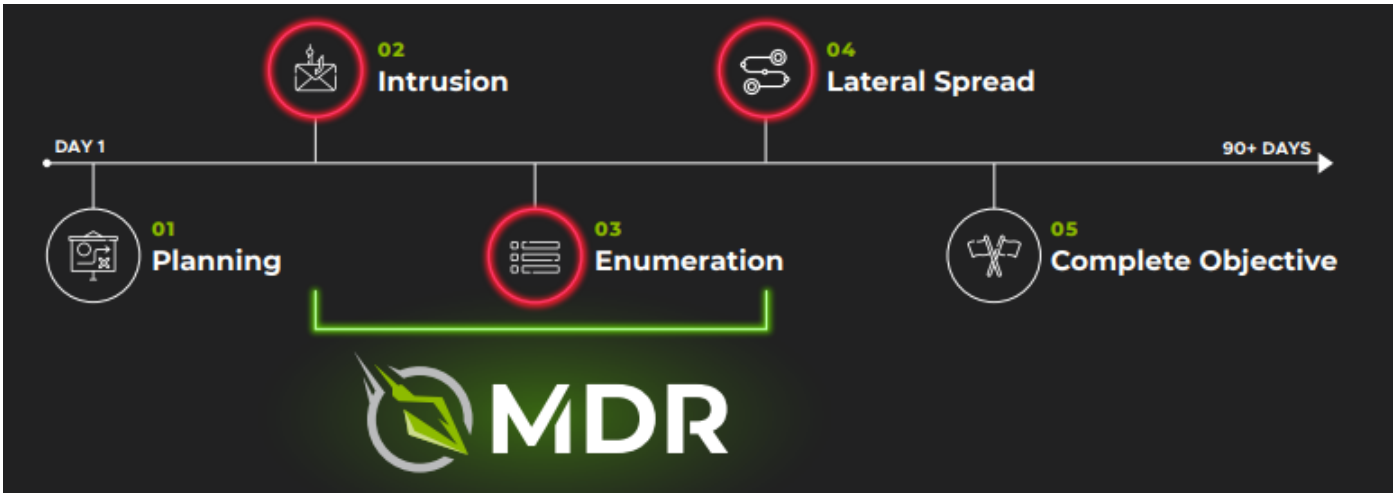
17:40 EST SOC MDR Analyst triages alert and raises for first time PowerShell observed.

18:32 EST SOC Senior MDR Analyst isolates the workstation after observation of successful C2 callout from malware.

18:39 EST SOC calls customer to inform them of the incident.

13 min. Time between initial detection and response
52 min. Time between response and isolation

Disrupting the Hacker Timeline



Blackpoint SOC vs. The Hacker Timeline

When an attack occurs, detection and response times determine whether attackers succeed in their efforts. Stopping lateral spread before it occurs is paramount and this is where real-time detection and immediate response come into play. Blackpoint Cyber's true, 24/7 MDR fights back threats within minutes, closing the gap between the identification of an event and the actual response and remediation. By immediately isolating endpoints, Blackpoint's technology stops the threat from moving laterally into other systems.

Blackpoint's managed detection and response (MDR) platform combines network visualization, tradecraft detection, and endpoint security to rapidly detect and neutralize lateral spread in its earliest stages. Faster than any other solution on the market, we designed our technology to harness metadata around suspicious events, hacker tradecraft, and remote privileged activity to catch what others miss and take real action before cyberthreats can spread.

blackpointcyber.com
+1 410.203.1604
info@blackpointcyber.com

Summary: Detainment & Post-Incident Actions

The Energy Consulting Firm was identified to be running suspicious PowerShell with no additional indicators of compromise. Shortly after, the device called out to a malicious Command & Control server outside the organization, also known as a Botnet. After identifying the malicious communication, Blackpoint SOC isolated the affected device and contacted DenaliTEK to give a report and provide the actionable steps for remediation.

Had the SOC not been involved, it is impossible to tell how long the breach would have lasted and how much of the Energy Consulting Firm's data would have been at risk. After the initial breach, malicious actors can take time to escalate privileges and propagate ransomware through a network to encrypt or exfiltrate sensitive data. **This is called 'lateral spread'.** The longer actors stay undetected within a breached network, the more they can spread and affect various systems.

For many organizations, rising cases of sophisticated cyberattacks have shown how even next-generation security tools such as firewalls, anti-virus, and anti-malware are not enough to fight back cybercriminals. While both anti-virus and anti-malware solutions are useful in providing protection against known viruses and malware, they simply cannot thwart dedicated criminals leveraging newer attack methods such as ransomware and zero-day exploits.

Why Blackpoint?

Our mission is to provide unified, 24/7 detection and response services to our valued customers.

"**Great Solutions, Great Partner Relationships.** Blackpoint Cyber gives me great peace of mind and an added layer of defense against cybercriminals. The fact that behavior is being monitored 24/7 with a qualified team of security experts allows me to focus on customer care. When something does come up, the team is able to take quick action to isolate the behavior and prevent additional harm."

Matt K Sr Vice President | Mid-Market (51-1000 emp.)