

# Scenario Vignette 2: Watering Hole Attack

## Discussion Questions

- Who in your organization would respond to this incident and how?
- What are their roles and responsibilities?
- What resources and capabilities are required to respond to this incident?
- Are essential personnel trained to respond to this scenario?
- What actions would your organization take based on this information?
- Does your organization have policies and procedures for sharing threat information?

### Quench the Thirst

- Organizations that have intellectual property or are perceived to have something of value often become targets for cyber espionage or theft. One technique malicious actors use is watering holes.
- The main purpose behind watering holes is to steal information or conduct espionage activities. Hackers' motivations are to steal intellectual property, personal information, or gain access to sensitive computer systems.
- Watering hole attacks are very difficult to detect.

### Thirsty?

- D-day: Employees receive an email from the training division. The email states each employee must complete mandatory training by the end of the week. Contained within the email is a link to the trusted training website.
  - » The subject of the training: Keeping Your Information Safe During the Holidays.
  - » A malicious actor has discovered that employees of the target company are visiting the trusted training website and plants malware in the website.
  - » As employees access the trusted website the target company systems become infected.

- D +1: Employees who have attempted to email the completed training certificate report having trouble with the link. They report their systems are hung up. Not all employees are having the same issue though.
  - » IT personnel troubleshoot the issue and realize one of the browsers is incompatible with the training website. The employees are then instructed to use a different browser to complete the training.
- D +2: Employees who successfully completed training report they are unable to log into their organization-specific application. The error message states, "You are already logged in at another location. Please log off from that location first."
- D +3: While investigating the log on error, IT personnel notice the individual's credentials are logged into the application from an overseas Internet Protocol address and a large amount of data has been exfiltrated.
- D +4: Analysis is conducted on all machines that exhibit the error message. IT personnel discover sophisticated malware was uploaded from the trusted training website.

# Scenario Vignette 3: Cyber-Induced Power Outage

## Discussion Questions

- What are your organization's essential functions and how could they be impacted by a cyber attack?
- What are the information sharing processes for both internal and external stakeholders during a power outage?
- Do you have defined cybersecurity incident escalation criteria, notifications, activations and/or courses of action?
- If your organization is unable to manage the incident internally, what processes are in place to request and manage additional resources?
- What other cyber-related communications has occurred or is required (e.g. public information, reporting mandates, etc.)?

### Got Power?

- Many organizations outsource security monitoring of Industrial Control System (ICS) /Supervisory Control and Data Acquisition (SCADA) systems to a third-party vendor in order to save on manpower.
- These third-party vendors often remotely control key systems and provide updates to those systems when needed.
- Sometimes a bad update is pushed, creating a vulnerability and an opportunity for malicious actors to upload malware.
  - » This malware may sit on the network just watching (sniffing) the traffic, collecting information on various systems.
  - » Once a critical system is identified, a malicious actor conducts a test to ascertain the malware's effectiveness. A successful test could lead to a full scale cyber attack, resulting in rolling brown outs or a black out.
- A third-party vendor provides continuous monitoring of ICS and SCADA systems, capable of remotely controlling key systems.
- D-1: The vendor notices there is a new update for printers on the operational system and proceeds with installation.
- D+2: Network personnel notice one of the operational printers is attempting to contact an unknown IP address.
- D+4: The organization experiences a short power outage. Investigation doesn't find anything unusual.
- D+5: News reports state a blizzard is forecasted for the area.
- D+7: During the night, third party vendors monitoring the ICS and SCADA systems notice an increasing imbalance between reactive and real power. As the imbalance increases, rolling brown outs begin to affect the region. As the imbalance continues to increase, a black out occurs leaving thousands without power.
- D+8: IT personnel and emergency crews attempt to get the power restored. Investigation into the system does not yield any clues to the cause of the power outage.
- D+9: The blizzard impedes efforts to restore power and many blame the snow for the power outage. Various organizations begin to activate their COOP plans.
- D+10 (AM): As crews work around the clock, IT personnel uncover a series of false commands that were issued to the operational network which caused the imbalance.
- D+10 (PM): IT personnel repair the affected system and the power is restored.
- D+15: Further investigation reveals that Dark Energy 3 was installed via the update to the printer that was connected to the operational network.