CYS401: Fundamentals of Cybersecurity

Class Activity 2

SCENARIO:

A small family-owned construction company made extensive use of online banking and automated clearing house (ACH) transfers. Employees logged in with both a company and user-specific ID and password. Two challenge questions had to be answered for transactions over $1,000.

The owner was notified that an ACH transfer of $10,000 was initiated by an unknown source. They contacted the bank and identified that in just one-week cyber criminals had made six transfers from the company bank accounts, totalling $550,000. How? One of their employees had opened an email from what they thought was a materials supplier but was instead a malicious email laced with malware from an imposter account. The malware was written specifically to steal the owner login credentials by monitoring the keystrokes.

ATTACK:

For the given scenario, identify and explain the type of Attack and the software attacker use to steal the credentials?

RESPONSE:

How should the company respond to this Attack? Briefly explain **TWO** actions that must be taken by the company.

IMPACT:

What could be the operational/ financial impact of above attack on the company.

SECURITY MEASURE/ CONTROLS:

What are some steps you think the company could have taken to prevent this incident in future?

Solution:

ATTACK:

The attack was a **phishing attack, more specifically a targeted spear-phishing/whaling attack**, in which the attacker impersonated a trusted materials supplier to deceive an employee into opening a malicious email. The email contained **malware in the form of a keylogger**, which monitored the employee's keystrokes and captured the owner's online banking login credentials. The keylogger may have been delivered through a **Trojan**, which disguises malicious software as legitimate or trusted content.

RESPONSE:

The company should take the following two immediate actions:

1. **Contain and report the attack:** The company should immediately contact the bank to **freeze the compromised account and disable the stolen login credentials** to prevent further unauthorized transactions. The incident should also be reported to the appropriate authorities for investigation.
2. **Remove the malware and secure access:** The infected device should be **isolated, wiped, and checked to ensure the keylogger has been completely removed**. After securing the device, all compromised passwords and security questions should be changed. The company should also implement **two-factor authentication (2FA)** using a separate trusted device or security token, so that stolen login credentials alone cannot be used to access the account.

IMPACT:

The attack could have a significant **financial and operational impact** on the company. Financially, the company suffered unauthorized ACH transfers totalling **$550,000**, resulting in a major direct financial loss and potentially additional recovery, investigation, and security costs. Operationally, the company may need to temporarily suspend online banking activities, isolate affected devices, and spend time investigating and recovering from the attack. The

compromise of login credentials also represents a **breach of confidentiality**, as sensitive authentication information was accessed by unauthorized attackers.

SECURITY MEASURE/ CONTROLS:

The company could have implemented several security controls to reduce the likelihood of this attack. Employees should receive regular **security awareness training** to recognize phishing emails, suspicious attachments, and impersonation attempts. The company should also use **email security solutions, updated antivirus/anti-malware software, and malware protection** to detect malicious emails and keyloggers. In addition, **two-factor authentication (2FA)** using a separate trusted device or security token should be required for online banking, rather than relying only on passwords and challenge questions. Strong password policies, regular software and antivirus updates, and routine data backups should also be implemented as part of a **defense-in-depth** approach.