Cole Ramos

IST590-Instuctor Anastacia Webster

May 17, 2018

**Credential Theft**

Credential theft is the process of stealing credential, and is commonly use exploits, which rely on weaknesses in security defenses. Corporate credential theft is usually a targeted effort. Attackers scour social media sites such as LinkedIn, searching for specific users whose credentials will grant access to critical data and information. The phishing emails and websites utilized in corporate credential theft are much more sophisticated than those used for consumer credential theft. Attackers put a great deal of effort into making these emails and websites look nearly identical to legitimate corporate applications and communications. (Paloalto)

Credential abuse, the endgame of a credential-based attack, is the actual use of compromised passwords to authenticate applications and steal data. (Paloalto)

Once an attacker gets ahold of user credentials and passwords, they can sell the credentials in the cybercrime underground or use them to compromise an organization’s network, bypassing all security measures to keep an adversary out, move laterally within the network and steal data. (Paloalto)

In an unsegmented environment, an attacker can move freely across an organization’s network. If the environment is segregated and provides visibility across users and applications, security measures can be put in place to prevent an attacker from moving laterally and gaining access to critical data. (Paloalto)

Once an attacker has the credentials to operate like a valid user, there is very little that can be done to identify an intruder and validate if that user is really the person their credentials claim them to be. Organizations commonly implement multi-factor authentication within applications to require users to validate their identity more than once. (Paloalto) However, doing this for every individual application used within the organization is not scalable. Implementing policy-based, multi-factor authentication at the network layer, meaning in the firewall, will provide the needed scale and end-user ease of use.

The Palo Alto Networks Next-Generation Security Platform stops the credential-based attack lifecycle in multiple places, from the theft of credentials to the abuse of stolen credentials. The combined prevention capabilities of the Next-Generation Firewall, Threat Prevention, WildFire and URL Filtering stops known, and unknown attacks used for the theft and abuse of credentials, while GlobalProtect extends protections from the platform to mobile workforces and provides additional measures to identify users and devices that are accessing applications. (Paloalto)

Most of the attacks are stolen password which is one of the oldest attacks in the book, but most effective. Some companies offer software that will prevent this type of attack from happing.

Stop users from submitting password-based corporate credentials to unknown sites. Block access to known phishing sites with PAN-DB URL Filtering, using the latest global threat intelligence updated every five minutes. Protect critical applications and stop attackers from using stolen credentials to conduct lateral movement with policy-based multi-factor authentication enforced at the network level. (Paloalto) We must remember that most attack like this come from social engineering.

In conclusion credential theft attacks that security awareness training plays a role as the first line of defense. Unfortunately, there is no guarantee that employees will identify a phishing attempt 100 percent of the time. To minimize credential theft, corporate credentials should be limited to approved applications, and usage should be blocked from unlikely or unknown applications and sites. Security products be capable of blocking corporate credentials from ever leaving the organization’s network and prevented from being submitted to malicious sites. (Paloalto)

References

https://www.paloaltonetworks.com/products/innovations/credential-theft-prevention

https://www.paloaltonetworks.com/cyberpedia/what-is-a-credential-based-attack