illusive

Crèdentiãl-Thêft Attäckš

What is a credential-theft attack?

To reach sensitive network data, attackers attempt to compromise computers with the highest-privileged accounts. Attackers use these hosts and these accounts to retrieve passwords and hashes that can then be used to move laterally within the network without arousing suspicion.

In 85% of all breaches, attackers use stolen credentials

What is the risk?

Within a network, an employee is represented by a username and password which makes it difficult to differentiate between the activity of authorized users and that of an attacker who has gained access to credentials. In this way, attacks become identical to internal threats, making it difficult for traditional detection mechanisms to identify the malicious activity concealed as authorized behavior.

Credential theft is typically one of the first steps of an APT. For operational ease, modern networks are designed around memory caches. This means that, throughout a network, caches of credentials are constantly being created, waiting to be harvested by attackers. Having credentials such as passwords, and executing pass-the-hash attacks, enables attackers to move laterally, re-enter a network, and access business-data, customer details, sensitive financial information and so on.

How does the attack operate?

1. Compromise - access a host

2. Harvest - search the host's memory and cache for stored credentials

3. Execute - utilize credentials to perform malicious actions

What are the challenges?

Organizations are operated by employees. Generally, employees do not follow safety Best Practices; they use easily-remembered passwords, reuse them often, and store credentials on computers.

Endpoint solutions fail to detect credential-theft attacks. Additionally, time is on the attacker's side; they can take as much time as they need to move transparently throughout the network.

What would minimize the risk?

The risk is minimized if compromised hosts lie to attackers.

With illusive installed, Windows, FTP, SSH, RDP, and web-based credential-deceptions lure attackers away from valid credentials, divert attackers from sensitive data, and reveal attacks in real-time with source-based forensics.

Additionally, the illusive Attacker View™ allows you to visualize discoverable saved credentials and access, enabling you to limit unnecessary risks.

illusive integrates both engagement decoys and deceptive lures that dynamically change over time and diversify across endpoints and servers.