CREDENTIAL THEFT

Credential theft is the oxygen of malicious activity: nearly always there, necessary, but never noticed. According to the 2016 Verizon® Data Breach Report, 63 percent of confirmed data breaches leveraged credentials, and the use of stolen credentials is the most common approach in web-app attacks. Credential theft is a staple in the playbooks of sophisticated attackers, like the Sofacy threat actor group, and unsophisticated attackers alike.

Attackers can target credentials in many ways; however, phishing and malware are the most notable and effective. Stolen credentials give attackers the same access and privileges as legitimate users. But credential theft can be prevented. Two-factor authentication/multi-factor authentication (2FA/MFA) and one-time passwords (OTP), in particular, can help prevent credential theft. Unit 42, the Palo Alto Networks® threat intelligence team, recently released an in-depth report on credential theft: how attackers steal credentials, what they do with stolen credentials, and how you can prevent credential theft.

WHAT’S AT RISK?

Because credentials form the backbone of access control for our personal and professional lives, people and organizations face a constant threat of credential theft. Not only that, because of password reuse, BYOD, shadow IT, and the mixing of personal and private information with services on computers and devices, credential theft threatens your employees face in their personal lives can threaten your organization as well.

When credentials are stolen, attackers use them to mount critical attacks, such as the data-destructive Shamoon 2 attacks, as well as execute major breaches that result in data theft or loss.

Successful credential theft attacks represent some of the greatest cybersecurity risks organizations face. In turn, the cybersecurity risks around credential theft are some of the greatest business risks organizations face.

ASSESS VULNERABILITIES

To ensure your organization is positioned to thwart credential theft, we recommend asking your CISO the following questions:

1. Do we have effective protections in place against credential phishing?
2. Can we prevent reuse of corporate passwords on non-corporate sites?
3. Can we protect critical applications by enforcing 2FA/MFA?

TAKE ACTION

Palo Alto Networks’ PAN-OS® 8.0 has new capabilities to prevent credential-based attacks, including stopping corporate password reuse, blocking access to known phishing sites, and enforcing policy-based multi-factor authentication at the network level.

Read the full report for more information on credential theft.