How are Credentials compromised?

PHISHING

- ***Send e-mails disguised as legitimate messages***
- ***Trick users into disclosing credentials***
- ***Deliver malware that captures credentials***

WATERING HOLES

- ***Target a popular site: social media, corporate intranet***
- ***Inject malware into the code of the legitimate website***
- ***Deliver malware to visitors that captures credentials***

MALVERISING

- ***Inject malware into legitimate online advertising networks***
- ***Deliver malware to visitors that captures credentials***

WEB ATTACKS

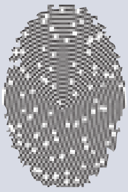
- ***Scan Internet-facing company assets for vulnerabilities***
- ***Move laterally through the network to discover credentials***
- ***Exploit discovered vulnerabilities to establish a foothold***

Why Monitoring for Exposed Credentials is Important

PROTECT AGAINST CREDENTIAL COMPROMISE

While there is always a risk that attackers will compromise a company's systems through advanced attacks, most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only by implementing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others - can organizations protect their business from the perils of the dark web.

WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?



- Send Spam from Compromised Email Account
- Deface Web Properties and Host Malicious content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

60% of Australians using the same or very similar passwords for multiple online services

Passwords are a twentieth-century solution to a modern-day problem. Unfortunately, user names and passwords are still the most common method for logging onto services including corporate networks, social media sites, e-commerce sites and others.

$1-$8 Typical price range for individual compromised credentials

A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing credentials. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers.

User names and passwords represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defenses can easily steal hundreds or even thousands of credentials at a time.

834,833 Average number of breached data records, including credentials, per Australian-based company

ACCUCOM

Accucom Systems Integration

Unit 25, 11 Brookhollow Avenue, Baulkham Hills NSW 2153
T 02 8825 5555 E sales@accucom.com.au W www.accucom.com.au