OVERVIEW

Credentials are the Keys

According to Verizon's 2019 Data Breach Investigations Report (DBIR), 52% of breaches involved "hacking" as a technique, and 70% of those hacking actions involve the use of stolen credentials. That's more than double any other category of hacking actions, including the use of backdoors, brute forcing, vulnerability exploitation, and SQL injection. All of these methods enable actors to spread from asset to asset within a network, stealing data, surveying further valuable targets, and preparing for future operations such as POS theft or even ransomware attacks.

So how do bad actors obtain these credentials? First, they can buy them, through marketplaces such as the now-shuttered xDedic marketplace. Second, they can use publicly available data breaches or password lists, or even infer them from past passwords. Third, they can steal them using tools like Mimikatz from accesses they may have already gained within the network. And finally, they can phish for them.

Given this broad list of methods to obtain credentials and their utility to attackers, it's not a stretch to say that nearly any breach involving an external actor involves some form of credential re-use. Even in the 2018 Marriott/Starwood Breach, where attackers had been in the network for multiple years, the investigation still found tools such as Mimikatz present, which speaks to their importance to maintaining access.

BEST PRACTICE

Credential Reuse Resulting in Data Breach

Resilience's Cyber Meteorology Framework models cyber risk trends and helps companies stay up-to-date with current best practices and mitigation guidance. Resilience's model for a data breach caused by cadential reuse recommend that organizations do the following to prevent and mitigate these attacks:

- Employ Multi Factor Authentication, most critically for the organization's Windows domain, but also for domain-connected resources
- Employ an Email Gateway and Conduct periodic phishing awareness training and tests
- Use endpoint detection and response (EDR) products
- Understand and monitor their DarkWeb exposure

INSURANCE

Breach of Privacy

When a credential reuse event happens, companies must determine whether they must comply with any law requiring notice to regulators and impacted individuals of the event. This notification step may give rise to a regulatory investigation or lawsuit. We are here to defend you with our robust liability coverage and strategic counsel partnerships you need to defend your enterprise.

Claims Example

A North American consumer staples company suspected a credential reuse data breach after Canadian and U.S. law enforcement flagged that consumer and employee information had emerged on the dark web. Resilience covered the costs of the legal and security investigation to determine the scope of the data breach and identify the effected population. Fulfilling its privacy law obligations, the company notified a large set of impacted individuals and multiple regulators. These costs were covered by the Resilience policy. Resilience also covered the defense and settlement of the resulting regulatory investigations and lawsuits.