Visibility management

Enable Dark Web Monitoring into existing CybrHawk SIEM

CybrHawk
Transforming Cybersecurity

1. Summary of service capabilities

Background: Cybercrime is now a top priority for all organizations, often resulting in irreparable damage to the organization and its leadership team. Phishing attacks are responsible for over 90% of all breaches, where cybercriminal steals corporate credentials or use other forms of social engineering.

Being aware when corporate credentials have been lost helps prevents these types of attacks and provides an opportunity to inform the employees of impeding phishing attacks.

Many employees use their corporate credentials to sign up to third party sites on the internet. When the third-party gets breached and corporate credentials get lost, cybercriminals can exploit your systems by reusing stolen credentials as an attack vector.

A new opportunity to further strengthen security posture was identified – which is monitoring when corporate records are part of third-party breaches, appearing for sale on various online forums and in data dumps.

Enabling monitoring of dark web will provide these new capabilities:

- Identify corporate records appearing in data dumps (emails, passwords, documents);
- Discover corporate accounts that have been a victim of third-party breaches;
- Receive early warnings as an automated alert or analyst driven;
- Identify employees that share credentials with nonbusiness internet services;
- Incorporate dark web data into regular reporting.

Benefits to the business are to reduce the risk from breaches and provide assurance:

- Prevent account takeover;
- Prevent breaches from leaked corporate credentials ;
- An opportunity to control and expect targeted phishing attacks;
- Retain historical, time series report of incidents;
- Through targeted security awareness, improve account security;

The service involves automated and manual scanning of known and unknown locations where data dumps appear.

In partnership with organizations that specialize in dark web discovery, the manual scanning involves over 100 human researchers, or “personas” that have “infiltrated” the dark web and monitor indicators.

The automated scanning uses various web crawlers, forum scrapers that analyze the data in order to expose relevant indicators. The automated process is enhanced continuously, with the addition of new public search engines such as Shodan.

The SLA is based on the following parameters: breach date and discovery date. Breach date is the date when the breach occurred, discovery date is when the leaked data was discovered.

CybrHawk SIEM will generate an alert immediately or within 1 hour of the discovery date.

In summary, the service will provide actionable insights to help reduce the risk from breaches, improve existing awareness and provide ongoing assurance.

Figure 1 high level overview of third-party breaches