Solution spotlight | **Monitoring the dark web**

Kingdom of Bahrain | 28 April 2021

keypoint

The dark web - a very concealed part of the web that few legitimate users will ever encounter - is often linked to criminal intent and illegal content. Making up about five percent of all internet content, the dark web includes a broad array of malware - including keyloggers, botnets, ransomware and phishing - that could be used against organisations to undermine their brand or cause reputational damage; disrupt businesses through distributed denial of service (DDoS) attacks; or cause direct financial losses as a result of intellectual property thefts or espionage.

Compromised data - including financial and medical records - can be exploited by a range of malicious actors. To help businesses in Bahrain deal with the broad risks posed by the dark web, Keypoint is offering a service that helps monitor the dark web and businesses' exposure to it.

What can be monitored?

Keypoint's dark web tool can continuously monitor a wide range of locations and sites, including:

- Hidden chat rooms
- Private websites
- Peer-to-peer networks
- Internet relay chat (IRC) channels
- Social media platforms
- Black market sites
- Botnets

What kind of compromised data can be found - and where?

- Dark web chatrooms: data in hidden IRCs
- Hacking sites: data from hacked websites or data dumps
- Hidden theft forums: data published within a hacking forum or community
- P2P file leaks: data leaked from a peer-to-peer file-sharing programme or network
- Social media posts: data posted on social media platforms
- C2 servers or malware: data harvested through botnets or on a command and control (C2) server

How can Keypoint help you monitor threats from malicious actors on the dark web?

Keypoint offers a range of dark web services, including:

- A SaaS alert platform that continuously monitors the dark web
- A prospecting tool that performs live searches monthly
- An email monitoring tool that can help to protect high-level targets

What are the limitations to this service?

- Hackers often get data - including usernames, passwords and credit card details - from databases that are widely available on the dark web. Once this information hits public forums, it has probably been used and sold multiple times - making it extremely difficult to track its usage.
- Leaks of encrypted data may not be detected - leak alerts are based on the availability of that data on the dark web.

For more details on our dark web monitoring services, please contact us.

Contact us:

Srikant Ranganathan
Senior director | IT consulting
srikant.ranganathan@keypoint.com
+973 3626 6286

Sagar Rao
Assistant manager | IT consulting
sagar.rao@keypoint.com
+973 3374 9112