5 Ways the Dark Web Endangers Businesses

The dark web today isn't the same as it was a few years ago. It is constantly evolving, with businesses facing new threats and fresh dangers all the time. That's why it pays to be familiar with possible sources of trouble to keep risks down to a minimum. **Here are the top five dark web threats that organizations face today.**

1 INITIAL ACCESS BROKERS (IAB)

These cybercriminals provide access to secure networks for a fee. Sometimes, IABs are hackers that have cracked those secure networks themselves, but they can also be traders in credentials that have been stolen or sold to them by a malicious insider. Today, there are **more than 300 IABs** operating on the dark web.

2 MALICIOUS INSIDERS

The dark web makes it easy for disgruntled employees to harm their employers and make a quick buck. Malicious insiders can sell their legitimate credentials to IABs or other bad actors, or also sell proprietary data, like customer lists and intellectual property, in dark web markets. Malicious insider actions, like selling credentials, are the cause of an estimated **25% of data breaches**.

3 CYBERCRIME-AS-A-SERVICE (CAAS)

The gig economy has spread to the dark web, resulting in a huge pool of freelance cybercrime specialists. Cybercriminals no longer need to be hackers — they can simply hire them. Offshoots of this economy include Ransomware-as-a-Service (RaaS) groups offering ransomware based on the Software-as-a-Service (SaaS) model and Phishing-as-a-Service (PhaaS) operations that can conduct complete phishing attacks for a low fee. Bad actors can hire PhaaS services to do their phishing for them for **$800 or less per month**.

4 DARK WEB DATA

There is a tremendous amount of information floating around on the dark web that has been snatched through successful cyberattacks or sold to interested buyers, and none of it is good for businesses. That data can include stolen customer records, hacked payment cards and illegally obtained proprietary data. An estimated **60% of the data** on the dark web could harm businesses, especially the vast quantities of stolen credentials available in dark web markets.

5 OPERATION TECHNOLOGY (OT) & INDUSTRIAL CONTROL SYSTEMS (ICS)

Information about OT or ICS is a goldmine for bad actors, including Advanced Persistent Threat groups (APTs). This information is obtained through theft, like in a ransomware attack, purchased from other bad actors or harvested from a data dump. Exposed OT and ICS data makes it easier for cybercriminals to conduct successful cyberattacks against infrastructure and manufacturing targets. An estimated **one in seven cyberattacks** gives the bad guys access to sensitive information about OT or ICS.

While these aren't the only dangers that emerge from the dark web to hurt organizations, the danger of damage from dark web sources can be mitigated with smart defensive strategies and the right security solutions. Learn more about the dark web and the solutions that help mitigate dark web danger in The IT Professionals Guide to Dark Web Defense.

Download our eBook

SECURITY *SUITE*