Top 5 Reasons to Make Dark Web Cyber Defense a Priority

The Dark Web is increasingly becoming a host for a variety of criminal activity, where cybercriminals engage with each other offering everything from tutorials on codebreaking to criminal services for hire. The anonymous nature of the Dark Web allows fraudsters to operate their criminal enterprises with impunity and gives them a place where data stolen via cyberattacks can be bought and sold. These data breaches can have dire consequences for a company's operations and financial assets – and the fallout can impact a company's brand and customers. Here are five key reasons for IT security professionals to make a defensive strategy against Dark Web threats a top priority.

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

1 — Threats have more places to hide than you might realize

An astonishing 96% of all Internet content exists in the Deep Web and Dark Web. Deep Web pages are unindexed by search engines, and while many are legitimate, several cybercriminal networks can lurk in these vast hidden segments. Equally troubling is criminal activity that takes place in the Dark Web, where stolen credentials are sold but can't be tracked. Even outside of the Dark Web, conversations on websites that occur behind password-protected pages – such as social networks, chat forums and Pastebin sites– can serve as launching points for fraudulent and criminal activity.

2 — It isn't just your customers that are at risk: it's your network too

Traditional phishing and malware attacks have long targeted your customers by luring them to illegitimate sites where login credentials, personal and financial information may be compromised. But now threat actors are finding innovative ways to penetrate traditional IT defenses by targeting your employees in spear phishing campaigns and posing a threat to corporate infrastructure, intellectual property and financial assets.

3 — Traditional security measures don't go far enough

Deep Web and Dark Web cyberattacks are particularly problematic because threat actors operate in a medium that offers little visibility, and they are more adept at covering their tracks. Traditional IT security protocols can't give you much intelligence about the extent of a security breach and what specific remedy might lessen the impact. With nine out of 10 large organizations now suffering from some form of security breach[1], companies need to be on high alert and know how to react effectively when the time comes.

4 — Going after cybercriminals yourself is an uphill battle

To detect and identify cyberthreats, organizations typically take a manual approach, with security analysts doing the work of probing the Deep Web and Dark Web for potential threats. Even if they do identify a criminal network, attempts to build trust and penetrate it in any meaningful way is something that takes time and that most security teams are stretched too thin to accomplish on their own.

5 — The financial impact is significant and spreading

Cyberattacks cost businesses as much as $400 billion a year[2]. New examples of Dark Web attacks are surfacing every day, and they are impacting a growing number of industries. The most vulnerable are companies whose customers access financial or personal information online, including banking, healthcare and e-commerce companies. The danger to consumers can have a domino effect if stolen credentials are sold in the Dark Web, opening the door to further breaches of sensitive personal information.

For more information on developing a comprehensive strategy to combat Dark Web threats, please call us at **1-800-745-9229** or visit **www.markmonitor.com/darkweb**

[1] PwC 2015 Information Security Breaches Survey of UK Corporations. http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

[2] Lloyd's CEO: Cyberattacks cost companies $400 billion every year, Forbes.com. http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics