STAY ONE STEP AHEAD OF CYBERCRIME

Cybercrime is now costing businesses as much as **$400 billion** annually and the threats are coming from places many people know very little about.[1] Fraudsters are flourishing in the Dark Web, a collection of websites and content buried deep beneath the surface web, where IP addresses are hidden and threat actors can operate anonymously.

IN THE DARK WEB

fraudsters sell data that has been stolen via phishing and malware attacks, offer criminal services for hire and provide tutorials on codebreaking. This drives the surge in cyberattacks targeting corporate infrastructure, yet companies are having a hard time keeping up with the onslaught.[2]

56%

Annual surge in online theft cases targeting intellectual property during 2015.[3] Consider the impact not only on your corporate assets but also the damage to your brand when customers learn of the privacy breach.

Annual losses from cybercrime. This can have a significant impact on corporate infrastructure, financial assets and even customer reputation.[4]

$400 BILLION

~75%

Of 46 surveyed cybersecurity managers and practitioners expect to fall prey to a cyberattack in 2016.[5] Awareness of the threats is high, but conventional security measures are designed to protect data only inside the firewall.

Percentage of organizations that do not have a response plan for cyberattacks, leaving them vulnerable to losses. It's critical for companies to generate a strategy that takes all cyber threats into account, including the ones that flow through the Dark Web.[6]

63%

MAKE THE DARK WEB PART OF YOUR DEFENSE STRATEGY

01 KNOW WHEN THREATS ARE COMING

Know when your organization is being targeted for cyberattacks by monitoring threats around the clock. Probing fraudster-to-fraudster conversations in cybercriminal networks can arm you with valuable intelligence to thwart an attack before it occurs, or minimize the damage afterward.

02 EFFICIENTLY MONITOR THE DARK WEB

Some organizations might be tempted to try their own hand at searching for cyberthreats in the Dark Web. But even a large team cannot efficiently achieve the coverage needed for any measurable success. Leverage smart technology to infiltrate networks with speed and efficiency.

03 EDUCATE YOUR EMPLOYEES, BUSINESS PARTNERS & CUSTOMERS

Raise awareness of fraudulent threats before they can impact your company. Create educational materials for both your own employees and anyone who exchanges sensitive data with your company. These efforts can improve the cost effectiveness of your security infrastructure.

04 WORK WITH LAW ENFORCEMENT

Increase the chances of shutting down fraudsters by handing over critical data to the authorities that have the resources to investigate criminal cases. Everyone benefits when you share threat data with relevant agencies that have data on different cases in aggregate. Leave criminal enforcement to the professionals.

FOR MORE INFORMATION, VISIT MARKMONITOR.COM/DARKWEB

1. Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," McAfee.com, June 2014. 2. United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime," UNDOC.org, February 2013. 3. PwC, "Global State of Information Security Survey 2016 ®," 2016. 4. Taylor, Harriet, "Hit Men, Drugs and Malicious Teens: the Darknet Is Going Mainstream," CNBC.com, May 19, 2016. 5. RSA Conference and ISACA, "State of Cybersecurity: Implications for 2016, ISACA.org, February 2016. 6. PwC, "Global State of Information Security Survey 2016 ®," 2016.

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics