CrowdStrike White Paper

CROWDSTRIKE

EXPOSING THE OPEN, DEEP, AND DARK WEB AND BEYOND

How to identify external threats, protect your brand and mitigate risk

EXECUTIVE SUMMARY

Cybercrime is rampant. The internet is full of shady forums, marketplaces and communities where bad actors congregate and underground digital economies thrive. Adversaries are out to steal your data, exploit your brand and scam your customers. You need to gain visibility into the dark corners of the web to identify threats, address potential incidents and minimize risk to your critical assets. But most organizations simply don't have the time, budget or knowledge to navigate the hidden recesses of the internet.

This paper reviews the underground web ecosystem, describes some of the tactics adversaries use to steal data and commit fraud, and explains how CrowdStrike Falcon X Recon™ can help you identify potentially malicious and criminal activity at the source — quickly, easily and cost-effectively — by taking a proactive approach to threat management.

The average total cost of a data breach is $3.86 million USD.

IBM Security
Cost of a Data Breach Report 2020[1]

CYBERCRIMINALS ARE RAKING IN BILLIONS

eCrime is big business. Everything from stolen credentials, to bank card numbers, to confidential customer data and intellectual property is available for sale on hidden areas of the internet. Today's adversaries enjoy a robust underground economy and have a vast ecosystem at their disposal.

Bad actors can take advantage of open-source toolkits and on-demand ransomware, malware and phishing kits to easily carry out campaigns and commit crimes. Cybercriminals can buy and sell stolen data on countless criminal marketplaces. And adversaries can even find confidential information such as access credentials on open sites and public code repositories such as GitHub if they know where to look.[2]

Cybercrime can disrupt your business, impact your company's bottom line, tarnish your brand and lead to stiff regulatory fines and costly legal settlements. Security industry analysts project annual global cybercrime damages to reach $6 trillion USD in 2021.[3] And according to industry reports, the average total cost of a data breach is $3.86 million USD, which includes direct costs such as forensics expenses as well as indirect costs such as revenue loss due to reputational damage.[4]

1 **IBM Security Cost of a Data Breach Report 2020**

2 Developers often hard-code API keys and secrets into applications.

3 **Cybersecurity Ventures**, November 2020

4 **IBM Security Cost of a Data Breach Report 2020**

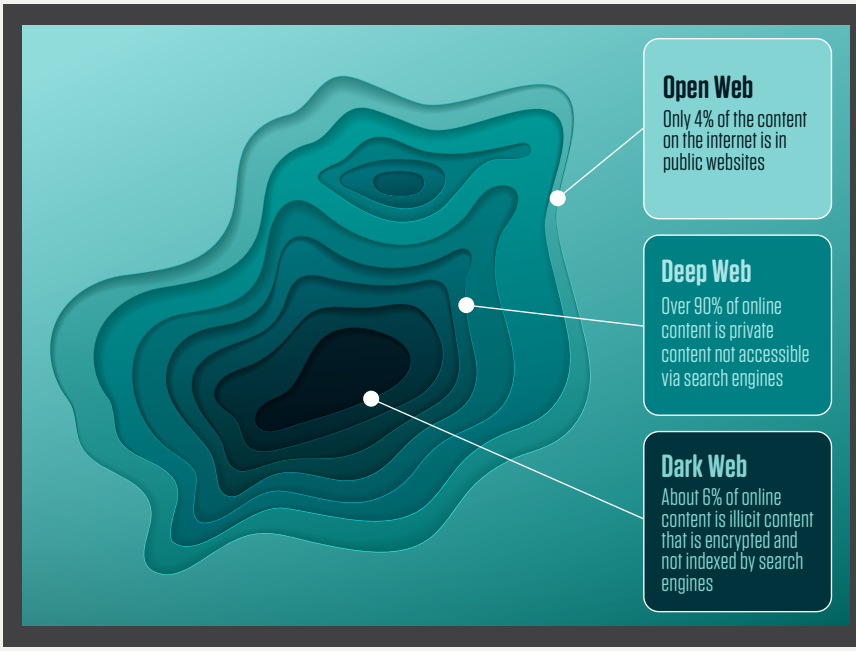
EXTERNAL THREATS ARE PERVASIVE

A wide variety of bad actors is lurking on the deep and dark web, and hiding in plain sight on the open web in blogs and social media sites. And to make matters worse, adversaries operate beyond the web, using messaging platforms, malicious mobile apps and other tools to carry out illicit activity. Organized cybercriminals, state-sponsored actors and hacktivists are always finding new ways to evade detection and wreak havoc. Every minute of every day, your organization is exposed to thousands of threat actors looking for opportunities to exploit your brand, steal your data and trick your customers. Table 1 shows examples of some common tactics that threat actors use.

Tactic	Examples
Impersonate your brand in emails, SMS messages, social media sites, mobile apps and websites	■ Phishing attacks that harvest credentials or other confidential data from unsuspecting consumers ■ Counterfeiting schemes that sell fake products under your brand name ■ Supply chain scams that fool suppliers to commit fraud or theft
Steal and resell confidential company information and data	■ Credentials (such as user IDs, passwords and API keys) to IT systems and business-critical applications ■ Internal documents, intellectual property, confidential employee data and privileged communications ■ Customer data including personally identifiable information (PII) and protected health information (PHI) ■ Corporate credit cards, SWIFT numbers and passport numbers
Run retail scams	■ Fake gift cards, coupon codes and loyalty points
Buy and sell malware, hacking tools and services	■ Keyloggers, password stealers and social media hacking tools ■ Exploit kits, malware generators and trojans ■ Crypting, spam and deepfake services

Table 1. Examples of common threat actor tactics

OPEN WEB vs. DEEP WEB vs. DARK WEB — WHAT'S THE DIFFERENCE?



The open web includes any content that is indexed by search engines and shows up in search results in Google, Bing, etc.

The deep web contains a wealth of private content that is not indexed or accessible via a search engine. It includes anything that requires sign-in credentials and includes content that explicitly blocks web crawlers from indexing.

The dark web is only accessible using a special browser like Tor (The Onion Router) or I2P. It is the underbelly of the internet and home to stolen information, illegal goods, and a myriad of criminal forums and shady activity.

A PROACTIVE APPROACH IS YOUR BEST DEFENSE AGAINST EXTERNAL THREATS

Bad actors can damage your company's reputation and cost your company money. You need to take a proactive approach to identifying and mitigating external threats — but regularly taking the pulse on the vast and dynamic underground web is a daunting proposition that is beyond the reach of most businesses.

Few organizations have the necessary budget and the right people to design, deploy and manage a massively scalable data collection engine. And few know how to navigate the dark underbelly of the internet.

Monitoring the hidden corners of the web is a significant undertaking:

- **Keeping pace with change is a full-time job.** The criminal ecosystem is constantly evolving — there are always new sites, forums and actors to track.
- **Credentials to illicit sites are difficult to obtain.** Access to illicit sites can be difficult because some sites are invitation only.
- **You have to be clever and stealthy.** If bad actors know they are being watched (or monitored by a bot), they will cut you off.
- **You must continuously capture and preserve raw intelligence data.** Malicious activity can be transient. Sites can disappear in days or even hours, and bad actors frequently delete incriminating posts, so you need to gather data while you can.

If your company is like most, you simply don't have the time, knowledge or wherewithal to monitor the hidden recesses of the internet for malicious activity. CrowdStrike can help by providing the experience, technology and dedicated professionals to help you stay one step ahead of the bad guys.

CROWDSTRIKE FALCON X RECON: DIGITAL RISK RECONNAISSANCE FOR THE OPEN, DEEP, AND DARK WEB AND BEYOND

CrowdStrike Falcon X Recon exposes potentially malicious activity from the open, deep, and dark web and beyond, helping you increase visibility, protect your brand and reduce risk. The solution proactively collects data and monitors activity from millions of restricted webpages, criminal forums, marketplaces, paste sites, leak sites, social media platforms and messaging platforms, providing valuable insights into suspicious behavior associated with your brand. With Falcon X Recon, you can perform queries in real time to uncover fraud, data breaches, phishing campaigns and other cyber threats. In addition, the solution continuously monitors surreptitious sites for malicious activity, providing automatic notification of potential risks.

Falcon X Recon is built on the cloud-native CrowdStrike Falcon® platform for ultimate simplicity and time-to-value. With Falcon X Recon there's nothing to deploy or administer, so you can focus your valuable time and resources on identifying threats and protecting your business. The CrowdStrike® solution is backed by a team of experienced professionals dedicated to helping you improve situational awareness.

COLLECT

Falcon X Recon collects raw intelligence data at scale, automatically mining data from millions of hidden webpages and thousands of restricted sites where criminals meet, buy and sell. The solution gleans data from restricted forums, marketplaces, app stores, paste sites and more.

With Falcon X Recon you can fly under the radar, gathering real-time intelligence data from illicit sites without detection. The solution captures and preserves data so threat actors can't cover their tracks by removing posts or taking down sites. You can use Falcon X Recon to identify imminent threats and disrupt adversaries, and to take the pulse on criminal chatter and activity. You can also use it to track and examine historical data to identify trends and behavioral patterns.

INVESTIGATE

Falcon X Recon makes it easy to discover and investigate external threats to your business. The solution provides simple-to-use wizards, with predefined search criteria like brand names, executives, domains, vulnerabilities and email addresses. You can perform ad hoc queries in real time, or continuously monitor the underground web, using custom rules to efficiently sift through raw intelligence data.

Falcon X Recon displays investigation results in concise, easy-to-understand cards. You can view the original threat actor posts, along with context about the actor and the site. Foreign-language posts, including hacker slang, can be instantly translated to English. (The machine translation supports 18 foreign languages.)

NOTIFY

Falcon X Recon provides automatic notifications of suspicious activity. You can set up custom rules to flag potentially malicious or criminal behavior. You can categorize and prioritize alerts, and define how frequently they are generated (immediately, daily or weekly) and which individuals and teams receive them. You can send alerts to IT security and operations teams, as well as other parts of the organization that need to know about confidential data loss, scams and abuse, such as the marketing, legal, human resources and fraud departments.

KEY BENEFITS

Increase visibility: Automatically extract data from millions of restricted and underground sites, without detection

Mitigate risk: Receive real-time notifications of potential threats to your brand and your business

Streamline investigations: Perform ad-hoc queries quickly and easily, with intuitive and actionable results

Gain insights: Monitor criminal activity, historical trends and emerging threats

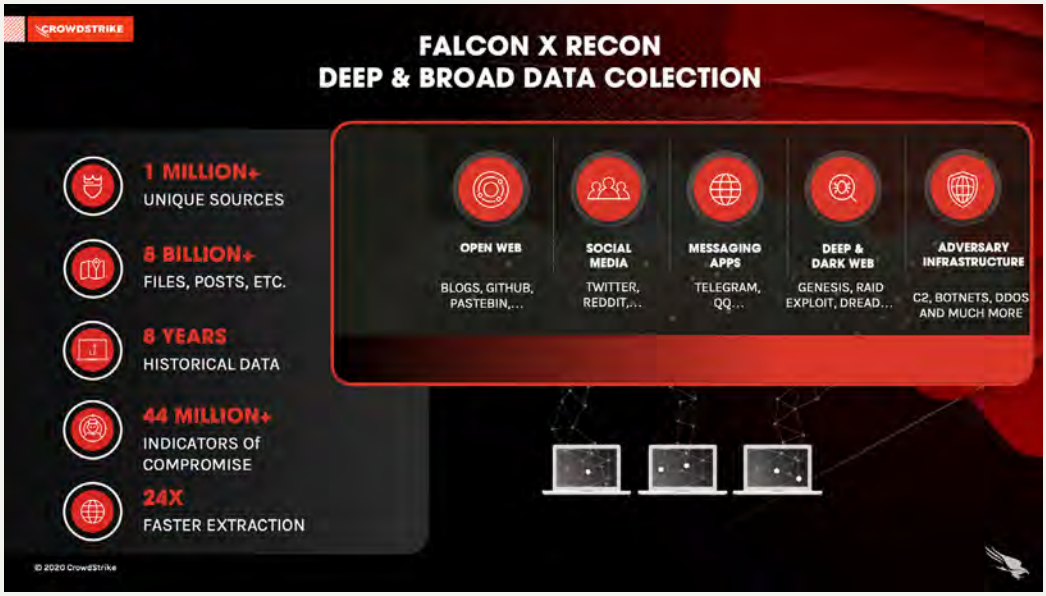
Accelerate time-to-value: Take immediate action against digital risk with a cloud-native platform backed by experts

WHY FALCON X RECON?

Falcon X Recon provides deep insights into the underground web, helping you identify and investigate external threats to your business with unmatched speed and unrivaled coverage.

The massively scalable, high-performance CrowdStrike solution:

- Constantly gathers data from over 1 million unique sources, maintaining over 8 billion pages, messages and files, and extracting data 24 times faster than competitive solutions
- Provides visibility into historical adversary activity data
- Delivers over 44 million indicators of compromise
- Uses honeypots and honeynets scattered across the globe to lure adversaries and identify botnets, DDoS attacks and other online threats to your business



FALCON X RECON+: MANAGED THREAT MONITORING

CrowdStrike has introduced Falcon X Recon+™ to simplify the process of hunting for external threats to brands, employees and sensitive data on the open, deep and dark web. By offloading this effort to CrowdStrike, Falcon X Recon+ increases the effectiveness of your security team, while reducing the time, skills and effort required to battle sophisticated adversaries.

CrowdStrike experts manage the effort of monitoring, triaging, assessing and mitigating threats across the criminal underground so you can focus on your business. Our experts monitor, on your behalf, data from restricted forums, marketplaces, messaging platforms, social media posts, data leak sites and much more to provide relevant, real-time warnings and identify data exposure and threats to your business.

Falcon X Recon+ threat experts assess and recommend effective mitigation steps, enabling you to act decisively with proactive steps to prevent and detect future attacks. The mitigation steps may include CrowdStrike facilitating the process of taking down malicious content that may threaten your brand or reputation, such as deleting harmful social media posts, removing data from paste sites, and removing spoofed or impersonated domains.

CONCLUSION

Bad actors are lurking in the dark corners of the internet looking to steal your data, scam your customers and take advantage of your company's good name. Take action with Falcon X Recon. The solution lets you proactively uncover fraud, data breaches, phishing campaigns and other online threats targeting your company.

To learn how Falcon X Recon can help your company identify external threats and mitigate risk, visit **https://www.crowdstrike.com/products/threat-intelligence/falcon-x-recon/**

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – end to ends and cloud workloads, identity, and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® Platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, customers benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**