Dark Web: Understanding the Risks

Akino Chikada
Sr. Product Marketing Manager
MarkMonitor

Jack Johnson
Manager, Security Operations Center
MarkMonitor
Agenda

- What is the Dark Web?
- Why Should You Care?
- Use Cases: Knowing What You Can Find
- How Do You Tackle the Dark Web Problem?
What is the Dark Web?
What is the Dark Web?

**Surface Web**
Searchable with standard search engines like Google and browsed with standard browsers.

**Deep Web**
Sites that aren’t indexed by search engines, with the majority of content in access-controlled databases.

**Dark Web**
Websites that run on the “Darknet” – a covert network that uses anonymizing software such as TOR and aren’t accessible to search engines or by using traditional browsers.

96% of the internet is inaccessible via traditional search engines and browsers.
The anonymity of the Dark Web encourages extensive illegal activity.

57% of websites on Tor host illegal content.
Why Should You Care?
Cyberattacks are a Growing Concern

$400B
Cyberattacks cost businesses as much as $400 billion a year\(^1\)

9/10
Nearly 9 out of 10 large organizations surveyed now suffer some form of security breach\(^2\)

60%
At least 60% of brands will discover a breach of sensitive data\(^3\)

75%
Of breaches go undiscovered for weeks or months\(^4\)

\(\text{\textsuperscript{1}}\) Forbes.com, January 23, 2015
http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds

\(\text{\textsuperscript{2}}\) PwC 2015 Information Security Breaches Survey of UK Corporations

\(\text{\textsuperscript{3}}\) Forrester, November 12, 2014

\(\text{\textsuperscript{4}}\) MIT Sloan School of Management
Impact to Your Brand

Target data breach has lingering effect on customer service, reputation scores.

Study: Data Breaches Make Huge Impact On Brand Reputation
Use Cases: Knowing What You Can Find
Value of Data Found in the Dark Web

1. Prepare against planned attacks
2. Identify and resolve breaches
3. Remediate and analyze stolen credentials
   - Consumers
   - Business
4. Detect leaked intellectual property
5. Minimize exposure to third party breaches
6. Understand hacking tools and services
Planning of Physical Attacks

What Happened

- Alerted the bank of upcoming attack
- Bank contacted law enforcement
- On that date/time, law enforcement and bank increased security
- Result: the disruption to the bank was minimized
Identifying a Live Attack

What Happened

- Criminals are conducting a DDOS attack
- Organization alerted in real-time
- Pulled resources to recover promptly
Stolen Business Credentials

What Happened

- Fraudster shared a list of email addresses and passwords in a closed forum
- Among those, our system detected email-password pairs of our client’s employees, alerting the customer
- Company was able to work with employees to reset passwords and scan for unauthorized access
Stolen Business Credentials (2)

What Happened

- Fraudster is offering admin access to a thermal power plant in India
- If undetected, a common use by the buyer would be a ransomware attack
What Happened

- An engineer needed help with coding and posted proprietary code to a forum
- Company was alerted that proprietary code was being shared
- Company took action by hosting an internal educational session & conducted thorough review to ensure the code did not expose vulnerabilities to their system
Third Party Breaches

What Happened

- Fraudster starting to target healthcare clinics, stealing large patient databases (20K to 9M records each)
- While not the direct target, our client is exposed to regulatory and brand reputation risks
- Alerts immediately sent to our client, and resources enhanced throughout campaign
- Understanding vulnerabilities used by fraudster allowed for cyber intelligence cooperation reducing the risk for additional breaches.
What Happened

- In a forum, a hacker was sharing a “how to hack XX company” tutorial
- Company was alerted on this
- Company worked with security and engineers to fix vulnerabilities
- End result: Mitigate future hacks using that vulnerability
How Do You Tackle the Dark Web Problem?
Anonymity as a Challenge

Who do I send enforcements to?
Comprehensive Approach

- Security teams need to consider vulnerabilities **from all angles**
- An end-to-end brand protection strategy that is **cross-functional** is essential
- Visibility across the entire internet, across **all channels**
- **Taking action immediately** will reduce cost and damage
Proactively defend your organization with near real-time alerts of impending cyberattacks

DEEP AND DARK WEB THREAT MONITORING
Our solution gives you unprecedented visibility into areas beyond the surface web - the Deep Web, Dark Web, threat actor groups in social networks and other digital channels.

NEAR REAL-TIME ALERTS WITH ACTIONABLE INTELLIGENCE
We provide you with near real-time alerts that can occur before, during or after an attack to enable your organization to proactively identify and act against fraud to minimize damage.

SMART TECHNOLOGY TO INFILTRATE CYBERCRIMINAL NETWORKS
We leverage leading-edge robot technology that mimics human behavior to interact with cybercriminals and infiltrate their network, to give you a scalable way to gather intelligence.
Questions to Consider When Building Your Brand Protection Program

- How are you currently protecting your consumers from brand and fraud abuse?
- Is your security / brand protection program giving you the visibility you need?
- Do you have the right protocols in place so that you are able to take appropriate action?
- Do you have the right resources (personnel and technology) in place?
Thank You!

For information on MarkMonitor solutions, services and complimentary educational events:

- Contact via email:  field.marketing@markmonitor.com
- Visit our website:  www.markmonitor.com
- Contact via phone: US: 1 (800) 745 9229  Europe: +44 (0) 203 206 2220