LEARNING MADE EASY

Bolster Special Edition

Dark Web Monitoring

for dummies
A Wiley Brand

Find threats on the dark web

Organize threats and make them visible

Plan for remediation

Brought to you by

BOLSTER

Bill Sempf

About Bolster

Bolster’s AI technology protects organizations, brands, and consumers from bad actors across the internet. With world-class network scanning and detection large language model (LLM) technology built from the ground up, Bolster is creating a safer environment for consumers and businesses to thrive in the evolving digital economy. Trusted brands, from start-ups to Fortune 500 companies, rely on Bolster to detect and take down threats that target their customers, employees, or partners.

Dark Web Monitoring

Bolster Special Edition

by Bill Sempf

for dummies®
A Wiley Brand

Dark Web Monitoring For Dummies®, Bolster Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-19648-7 (pbk); ISBN 978-1-394-19649-4 (ebk); 978-1-394-28395-8 (epub)

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Editor: Elizabeth Kuball

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Client Account Manager: Cynthia Tweed

Production Editor: Saikarthick Kumarasamy

Special Help: Kaitlyn Graham and Monnia Deng

Table of Contents

Introduction

Keeping track of digital threats and planning action surrounding them is an ever-evolving chore. Even on the open web, there is a constant barrage of new attacks, new vulnerabilities, and new details to manage.

When the dark web gets looped in, everything becomes even more complicated. Access is difficult, threats are ephemeral, and remediation requirements differ from the open web.

The dark web is still an important part of the threat landscape. Not only can proof of compromise be discovered on the dark web, but sometimes threats can be proactively discovered. This makes for a powerful addition to your defense strategy. You must organize it well, however.

About This Book

Organizing threats and performing remediation is what this book is about. Bolster, a leader in the threat intelligence space, has dug into the problems and possibilities of monitoring the dark web. In these pages, you get an inside view on the process Bolster goes through to make the information out there useful.

You won't learn everything about the dark web in this book. You will, however, get a much better understanding of the kinds of threats that Bolster can help you find and what to do about them.

Foolish Assumptions

If you're in security management — particularly a chief information security officer (CISO), vice president of security, director of security, manager of security, or engineer of security operations — this book is certainly written with you in mind.

Network administrators and security analysts also stand to gain a lot from this book. As long as you have a moderate understanding of security infrastructure and tools, none of the technical details in the following pages will come as a surprise. Even if you don't have all those technical chops, you may be surprised by what you learn, so read on!

Icons Used in This Book

Throughout this book, you find some fun little icons in the margins that highlight particular types of text.

TIP

This icon marks pointers and practical hints that make your life easier.

REMEMBER

When you see this icon, you should take note and file away a tidbit for future reference.

TECHNICAL STUFF

This icon denotes techno-nerd stuff that you can ignore if you like.

Where to Go from Here

There are two paths from this point. The first is to learn more about the dark web. The second is to get a demo of Bolster and see if it meets your technical needs.

To learn more about the dark web, head to `www.torproject.org` and read heavily. The all-volunteer group that puts together TOR makes it super easy to get started.

To get a demo of Bolster AI (highly recommended), head to `https://bolster.ai` and click the Request Demo button in the upper-right corner.

But finishing reading this book first. Always a good idea.

IN THIS CHAPTER

- » **Getting to the dark web**
- » **Seeing what's on the dark web**
- » **Looking for threats**

Chapter 1 Introducing the Dark Web and Its Related Threats

The dark web. You hear it spoken of in hushed tones by the media, online experts, perhaps even your IT staff. It's almost like magic — that place online where folks in black hoodies and balaclavas hang out. If asked exactly where the dark web is and what it means for a company, though, suddenly everyone gets quiet.

No more of that. In this chapter, we show you how to get to the dark web and find the services hidden within. While you're there, you'll find the actors that play around on the dark web and the threats they lead you to.

No matter how you slice it, the Internet is just a collection of computers that all have agreed on a protocol. The dark web is no different. It does require a few extra steps to get to and some specialized knowledge to use, but you can get there in ten minutes from your home PC, and it doesn't require any more care to use than the Internet you're accustomed to. What's more, monitoring the threats is just as straightforward.

Another thing: None of us wear hoodies and balaclavas when we work. They're way too hot.

Navigating the Network

The dark web is a collection of applications only accessible through a sophisticated virtual private network (VPN) called The Onion Router (TOR). TOR is a free, volunteer-run network that conceals traffic by moving the requests and responses through several thousand relays (see Figure 1-1).

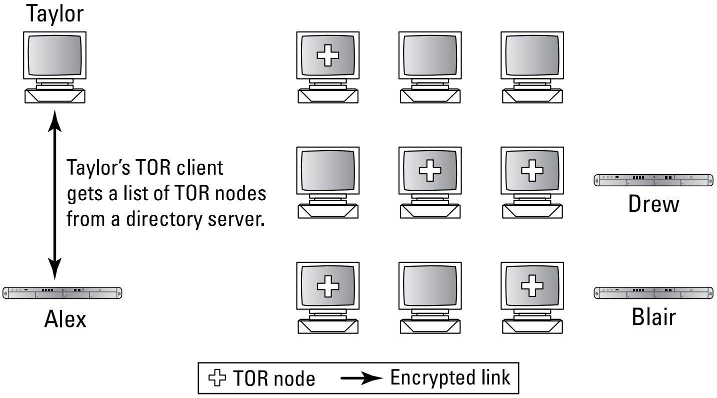

Taylor
Taylor's TOR client gets a list of TOR nodes from a directory server.
Alex
Drew
Blair
✚ TOR node
→ Encrypted link

FIGURE 1-1: How the TOR network and hidden services work.

After a computer is connected to TOR, it can make use of the applications found within. These applications can be anything any user wants to host, including websites, Internet Relay Chat (IRC) servers, Bitcoin exchanges, and mail servers.

TECHNICAL STUFF

TOR applications have their own special addressing format, which consists of a 256-bit public key from the generation of the HTTPS key pair, and the `.onion` top-level domain. For instance, once you're connected to TOR, the British Broadcasting Corporation (BBC) can be found at:

bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rcci
jh7745uqd.onion

Introducing the Players

The near-guarantee of private browsing and use of web applications is of interest to a number of wildly divergent groups, from activists and whistleblowers, to news media, researchers, and yes, criminals.

Many of these audiences are those who would like to hide their Internet traffic from their government. Some of this is understandable and laudable; some, less so. As with much technology, the dark web is a "gray market" tool. Sometimes it's very tough to determine who is on the right side of the equation.

Others are those directly interacting with a gray market. Sometimes, perfectly legal items or information in one country are illegal in other countries, and the only way to get those items is to make use of the privacy protection of TOR.

Still others are using hidden services legitimately for research or collection of information. In a way, that's who this book is for — folks watching for real tangible threats or potential future threats. The press, university researchers, and other information gatherers can benefit from the information only available on the dark web. Sometimes the privacy provided by TOR doesn't hurt either.

REMEMBER

Of course, there is more than a fair share of good old-fashioned black-hat criminals on the dark web. These are folks who are using the privacy that allows for anonymity to trade in user accounts, credit card numbers, identities, and, well, your company data. Finding those threats — and the criminals who stole the information — is the main goal of dark web threat monitoring and defense.

Extracting Threats out of the Noise

Hidden services are, by nature, hidden. A large body of specialized information is needed to scan the dark web, because one needs to know the `.onion` addresses for services of interest. These services may be web, mail, or chat, but knowing the end points where they live requires some research.

Watching the criminals do work to plan a malware attack on a company is harder, because that conversation is likely to be protected by credentials. Getting access is a little more involved.

Either way, the company looking to mitigate threats has a part to play, too. Protecting an organization's assets requires one of the hardest things to achieve: a List of Things.

The List of Things is a collection of important terms you want to keep an eye out for while gathering threats related to the company. Throughout this text, I recommend categories of items that you should add to the List of Things, until you have a solid collection of items.

Finding information for sale

The best way to find information for sale is just to look for it. Several search engines for the dark web are available, active, and accurate.

REMEMBER

When you're searching the dark web, however, remember that there is a hard wall between what's a hidden service, and what's on the open web but is about the dark web. It's not always obvious which is which. Take DuckDuckGo, for instance. It has a strong presence on the open web, but it can also search `.onion` sites for dark web material. You can't visit those sites unless you're connected to TOR, but you can find information related to hidden services there. Check it out at `https://duckduckgo.com`.

Watching campaigns get organized

Groups that are banding together to target a specific company in order to damage a brand, customize malware, or produce distributed denial of service (DDoS) attacks are trickier to discover. Usually, these campaigns are carried out by groups with known dark web membership, using ephemeral applications like IRC or password-protected applications like email.

Protecting key people and assets

All of it comes back to the List of Things. Knowing what you're trying to protect is a detailed but important job. Names, emails, dates of birth (DOBs), addresses, Internet Protocol (IP) numbers . . . anything that can be related to a person, business, or digital asset belongs on this list. You can find the process for making that list in Chapter 2.

IN THIS CHAPTER

- » Working with open-source tools
- » Looking for intelligence on the dark web
- » Isolating the tough parts of actionable monitoring

Chapter 2 Gathering Dark Web Intelligence about Your Company

Making use of the information on the dark web is not a simple task. There are some tools, yes, but you still need to find the services with access to the data you want — and then the challenges have just begun.

Fact is, a bunch of stuff must be found and analyzed before you can even get close to actionable monitoring. Criminals must be located, the applications they use must be discovered, and of course, it would be good to know if they're talking about your company or customers.

Then the intelligence gathering can begin. There are a whole bunch of tools to help you, so don't give up yet.

Making the Best Use of the Tools We Have

Some tools in the tool belt are manual — literally getting the tool to the point of impact and pressing the big red button. Others are automatic, like scanners and crawlers, which find those starting points and then kick things off on their own.

Either way, having an environment to run scripts safely isolated from your corporate network is an ideal starting point. Even better is finding someone else to do that part for you. Understanding how these tools work is important for knowing what intelligence is available.

Manual services

There are times when it makes sense to go and look around for yourself, or pay someone else to do so manually. The primary reason you might do this is to find hidden services, (see "Finding Those Hidden Services," later in this chapter).

REMEMBER

There is no quality search engine of the dark web, like a Google or Bing. The hard-to-find services are ephemeral (with some exceptions) and the `.onion` URLs that lead to them change often.

To this end, it often benefits a company to have an agent that keeps an eye on things. When leads are discovered, the scanners and crawlers can be used to really dig in and get the detail you want, but that first step can be done manually, if resources and training allow.

Scanners

A few reliable, open-source scanners can take the end points discovered from manual service research and find more that's worth indexing, researching, or scanning further:

- **Onioff** (`https://github.com/k4m4/onioff`) is a straightforward scanner that spiders from a starting `.onion` URL and produces a list of working sites. These sites can be fed to the other scanning and crawling tools to get higher-quality results.
- **Onionscan** (`https://github.com/s-rah/onionscan`) is an open-source scanner written in Go that helps researchers

monitor and track dark web sites. One of its principle features is the ability to correlate findings among several scanned sites. This is a sure sign of interest in a topic growing in the dark web community.

- **Onion-nmap** (`https://github.com/milesrichardson/docker-onion-nmap`) is exactly what it sounds like: a network mapping tool (or nmap) for the dark web. It accepts `.onion` URLs (perhaps from Onioff) and then effectively port-scans the server hosting the hidden service. Onion-nmap is very valuable for finding other applications that don't have web interfaces but benefit from the privacy features of TOR, such as IRC, Discord (a group discussion tool), or email.

Crawlers

If you've been around the World Wide Web long enough, you may remember having to submit your site to Yahoo! so it would be added to Yahoo!'s index for others to find. When you did that, you were submitting to Yahoo!'s crawler, Slurp, which would crawl through your site and add entries to Yahoo!'s searchable index. These crawlers do (and are constantly still doing) the same thing for the dark web:

- **TorBot** (`https://github.com/DedSecInside/TorBot`) is an old-fashioned spider, which follows hyperlinks from hidden service to hidden service. It's written in Python and, just like Google or Bing, saves some of the text of the site after it indexes it to make the information more useful to human threat intelligence researchers.
- **TorCrawl** (`https://github.com/MikeMeliz/TorCrawl.py`) is a newer spider written in Python. It specializes in passing the spidered pages to other tools easily, for analysis or keyword searching.
- **VigilantOnion** (`https://github.com/andreyglauzer/VigilantOnion`) is a rule-based spider that narrows down the results of the crawling to just the things that are of interest to the researcher. It's written in Python, with a Yara rule engine.
- **OnionIngestor** (`https://github.com/danieleperera/OnionIngestor`) is a Python tool that is based on the ThreatInjestor tool used for the visible web. One of its main features is crawling places on the visible web like Pastebin

(an online text storage tool) and social networks, for `.onion` sites and starting its crawling process there.

- **Darc** (`https://github.com/JarryShaw/darc`) is a spider that has gone commercial, but the open-source version is still available (and works well). It makes use of HTTP Request header fields to make sure the results expected are what is collected.

Fingerprinting

Fingerprinting is an architectural framework analysis method, not unlike what an enterprise architect may do with an existing, older project, or what a malware researcher may do with a command-and-control system. It's effectively classification of the results that have been returned by the scanners and crawlers.

Finding Those Hidden Services

Several search engines for the dark web are available, active, and accurate, such as Ahmia. Ahmia, shown in Figure 2-1, shows an active graph of hidden services that are indexed by the site.

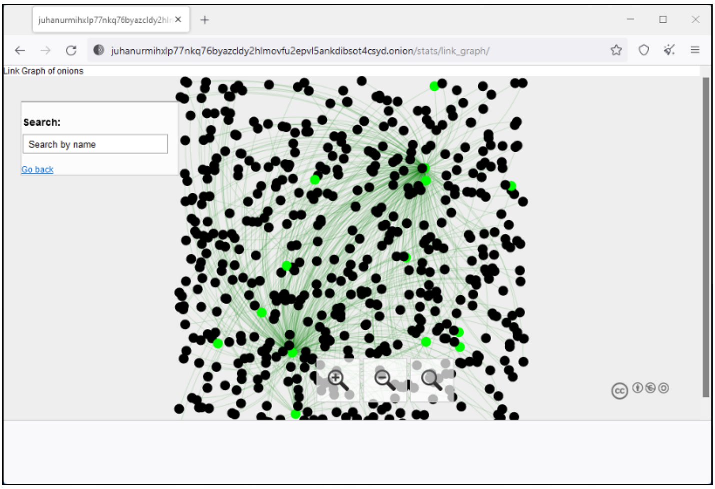

juhanurmihxlp77nkq76byazcldy2hl
juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/stats/link_graph/
Link Graph of onions
Search:
Search by name
Go back

FIGURE 2-1: Ahmia's hidden service network.

The key to searching, of course, is to use your collection of search terms, that famous List of Things (see Chapter 1).

Fortunately, a number of legit companies make copies of these easily searchable Onion domains and store the information for metrics gathering. That's the kind of product that is mostly used to monitor services and create actionable guidance.

Notice that if you put a `.onion` URL in your browser, you get an error. If you're connected to TOR, however, you get a version of the BBC website that is hosted on a hidden service.

TIP

Check with a computer that is not connected to TOR, and go to the usual BBC site (`www.bbc.com`). There will be a delay in the news stories on the hidden service because updating the hidden service takes longer than updating the public website.

Using TOR to access these applications all but guarantees the user's privacy. Every request is passed through a number of different relays. Even if certain relays are controlled by folks who would like to remove the using party's privacy, it's unlikely to happen because the trip through TOR is different every time.

Guaranteed privacy is of interest to different kinds of users. As long as a user doesn't tell a hidden service who they are, there is no usable path back to that user.

Understanding Dark Web Monitoring Challenges

Many tools exist; many strategies exist. Combining them into workable campaigns requires understanding the tough parts of monitoring the dark web. The first campaign that must be addressed is the conversion of all the details into real threat intelligence for your business. The second campaign is about remediating the vulnerabilities that were discovered.

Threat intelligence

Threat intelligence on the dark web isn't really any different from threat intelligence on the visible web. There is a sliding scale with short- and long-term use information and high- and low-level information:

- Information on changing risk

- Tools and tactics of the attackers
- Specific, incoming attack details
- Malware indication

How this information moves along that scale is dependent on your company's threat model. Those few items should get you started.

What's more challenging is the ephemeral nature of hidden services and how that impacts the gathering of intelligence. That's where tools like Onionscan come in. Correlation is key when it comes to threat intelligence on the dark web.

Incident response

Now that there is a map of threats, what are we going to do? One of the major tools of standard incident response — the takedown request — is gone because who would it get sent to? Other than that, it's about the same. The incident response process modified for the dark web might look something like this:

1. **Analysis:** The first step is figuring out what the threat is. Are the customers in danger? Are the stores or the site? What information is being used? Personally identifiable information (PII) sales or malware? Something new? Analysis doesn't look different; there may just be less data than the team is used to.
2. **Containment:** Containment is where everything starts to get sticky. You can't just contact the hosting company and ask them to take down the pages in violation or block the users. No one knows who runs the server, owns the domain, or manages the hidden service. Containment is hard, and there just aren't a lot of good options. Still, you must continue ahead with mitigation.
3. **Eradication:** Eradication is also rough when dealing with dark web intelligence, but not as hard as containment. Especially if it's a malware attack or an insider-oriented attack, blocking access from point A to point B internally goes a long way toward getting rid of the problem.
4. **Recovery:** Recovery looks just like a traditional threat intelligence exercise. Stand back up what was stood down, and then add protection where needed. Then wait to start the cycle over.

IN THIS CHAPTER

- Separating the wheat from the chaff
- Keeping the findings relevant to you
- Putting automation to work
- Engaging playbooks with machine learning
- Meeting compliance needs

Chapter 3
Monitoring the Dark Web with a Modern Approach

It's time to take a more modern approach to threat intelligence when it comes to the dark web. Most existing tools will bury the user in information but provide no corroboration and no actionable findings.

Change is afoot. A new breed of threat intelligence tools that have a truly useful take on actionable threat intelligence, like Bolster, are starting to roll in findings from the dark web. They take advantage of the rich data to be gathered, while filtering the input to something manageable.

The key is comprehensively understanding the risks to be found and following established patterns for action. Risks on the dark web look different from those on the open web. Categorizing those risks and the insights that come from them is the first step in the path toward remediation.

Modern tools like Bolster start with the risks found on the dark web and work in, instead of starting with the known open web threats and working out. Moving forward with that model makes it possible to integrate the insights that found risks provide into the corporate security fabric itself.

Removing Noise from the Intelligence You Gather

One of the issues with threat intelligence is that there is a lot of it. Some of it matters; some of it doesn't. And some of the intelligence matters but needs to be streamlined. Stripping the wheat from the chaff is a core piece of modern dark web monitoring.

Dark web research is mostly listening to chatter. Message board posts, Internet Relay Chat (IRC) logs, and half-written malware are all stuff that shows up on the threat intel landscape, along with political discussion, flirting, and recipes. This information needs to be filtered and collated.

Filtration depends on brand-specific keywords (see the next section). The List of Things that you created to help focus intelligence also helps with removing noise (see Chapter 1).

Collation consists of batching threats up into little groups that can be used to prevent micromanagement of findings. Bolster does a good job of this, using machine learning to better organize findings and create actionable groups of threats (see Figure 3-1).

After the threats are collected into groups and filtered, they can be prioritized and presented according to risk level and business preferences so you're ready to automate the appropriate response.

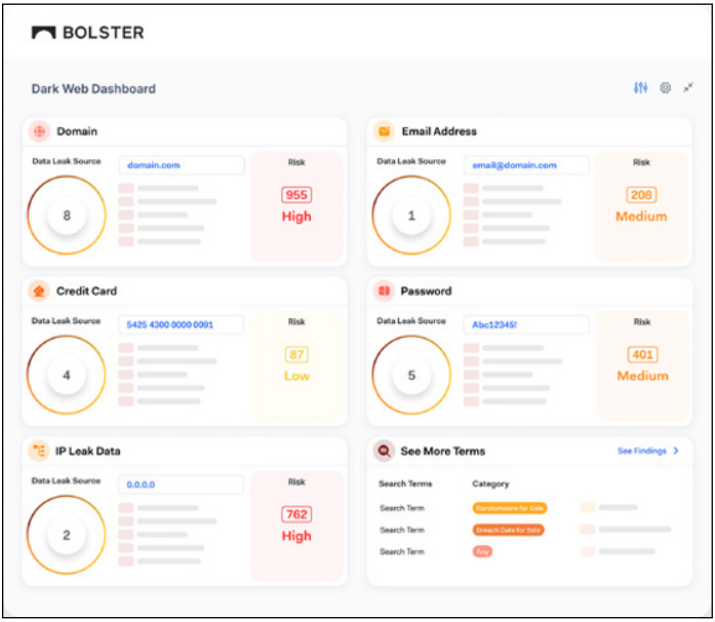


FIGURE 3-1: Bolster groups dark web threats into actionable entities specific to business preferences.

Focusing on Business Objectives

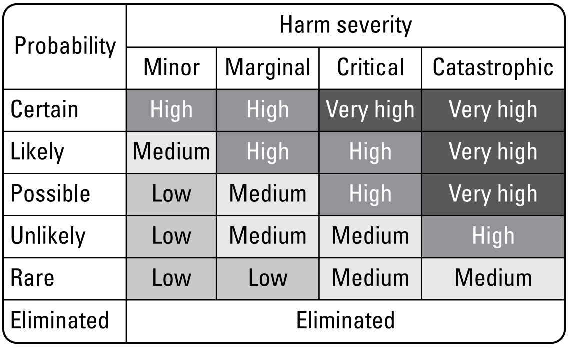
Prioritizing threats comes down to risk assessment. Risk assessment is a whole subfield of information security, within or independent of the dark web. At the most basic, you:

- Collect data about the threats discovered.
- Look at impact, likelihood, and other indicators.
- Calculate risk levels.

At first glance, it looks like the plan is to "just do it," which isn't helpful at all. Look a little more closely. Comprehensive analysis of the categories of risks provides the context needed to apply risks to findings. By using intent categories of the findings, you're able to apply a decision tree to more accurately appreciate the actual risk.

REMEMBER

Risk-level calculation is usually done using a risk matrix (like Figure 3-2), which has intent categories and risk categories.



Probability	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

FIGURE 3-2: A risk severity analysis matrix.

For example, leaked information has a complex arrangement with the risk categorization, and it has everything to do with context. If the company name is mentioned casually on a forum hosted on a hidden service, the risk is low, but it bears researching further. If intellectual property or secrets like application programming interface (API) keys or passwords are leaked, the risk is high, and immediate action is required.

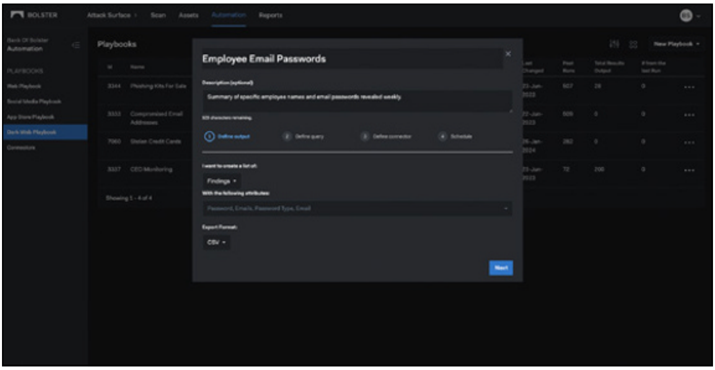
Tying the risks to categories allows for this kind of analysis. Each intent category and its associated risk category then has a rubric to guide the company toward successful remediation (rotating API keys, for instance).

Automating Risk Workflows

Now there is a list of things to do and an order to do them in. What's the best way to get everything done, assuming you worry about what to do down the line a bit? Automation, of course!

Another place where Bolster stands strong is in automating the workflows that best focus on your business objectives. Bolster provides a series of playbooks that handle specific categories of risks and walk through the remediation process recommended for the user.

Imagine a situation in which you have a collection of users whose private information, like a login password, was found online. The information was discovered on a hidden service, which is now unreachable. This is a common enough occurrence that a playbook for the category of password could be used, using a Bolster feature shown in Figure 3-3. Each of the found users should be emailed and told to change their passwords, for instance. Automating this workflow with Bolster playbooks brings that remediation into a modern era.



Employee Email Passwords

Description (optional)

Summary of specific employee names and email passwords revealed weekly.

I want to create a list of: Findings

With the following attributes: Password, Emails, Password Type, Email

Export Format: CSV

FIGURE 3-3: Adding a risk workflow.

Leveraging Machine Learning

No matter how you slice it, a lot of data comes back from threat intelligence. Categorization or not, a bunch of details are present.

Utilizing a machine learning model that handles further organization of this data makes everyone's life a lot easier. But not without a little effort.

Machine learning models are also excellent at finding more threats. For instance, the logo example in "Focusing On Business Objectives," earlier in this chapter, is well accomplished by a machine learning model. With enough examples of the correct logo in the model, finding similar but different logos will be trivial after the model is trained.

Both of these types of models — collection and image similarity — along with most other models, are awesome when trained. But they need to be trained, and that's where the work comes in. Leveraging technology with pre-trained large language models (LLMs) to recognize logo, text, and copyright misuse, as well as image similarity, will make your life easier.

TIP

Trained models will bring solid benefits to the threat intelligence game. What's more, models can be used to train models. Aside from the fact that this is mind-bending in and of itself, it's pretty cool in the final result.

Something that machine learning is already well established to hold expertise in is determining intent. For instance, if the scanners discover a number of emails in a list with a common company domain, the machine learning model could infer that a phishing attack is being planned. If those emails include what looks like passwords, the model could infer that a credential theft had already taken place.

These findings are placed in separate categories and, as such, are given separate workflows with different remediation steps. Thanks to the machine learning model, much of this work can be completed without any human interaction whatsoever, after the models are trained. Bolster uses several pretrained models for threat analysis, always with the option of running detected threats through your team to confirm whether you have been compromised and at what severity.

Implementing the Less Obvious Requirements

Enough of all this philosophical stuff. Time for the nitty-gritty: nonfunctional requirements. If you're interested in keeping the feds happy, or your manager happy, or the users happy, then this is the section for you. Did I miss anyone? The government, the boss, the user base? Perhaps the criminals, but they'll be unhappy no matter what.

Compliance

Compliance is a tricky subject in security, because the laws tend to lag behind reality, leading to the question, "Do you want to be compliant, or do you want to be secure?” This is unfortunately still true in the world of threat intelligence.

Dark web monitoring, and the threat intelligence that it brings, is more about security than compliance. That said, when the auditors do come, be they industry or government, a threat-intelligence focus can be very compelling.

An audit shows the items that should be protected, the items that are protected, and how they’re protected. For instance, in general, companies are required to be able to report where data is being handled. The company is responsible for knowing if the data isn’t handled properly. Finding, categorizing, and remediating improper handling matters just as much for dark web compromises as it does for the open web.

TECHNICAL STUFF

The dark web is even showing up on insurance forms today. For example, “Does your company monitor the dark web for threats against you or your industry?” and “Are threats discovered being tracked and reviewed periodically?” are questions that are often on cyber insurance applications.

Reporting

The hierarchy of reporting is straightforward, and as it turns out, it’s something Bolster does very well. To your managers, you may want to say, “We have *x* number of this threat and *y* number of that threat, and they’re handled by the relevant playbooks.” To the people doing the actual remediation and cyber defense work, you’ll want to give details so they can maintain oversight on the playbook and tweak the remediation plan as necessary.

Bolster providers dark web monitoring users with access to live status reports of dark web threats targeting their business and consumers. With actionable, easy-to-comprehend dark web threat reports, risk summaries for managers, auditors, or even the board is straightforward.

Ease of use

No tool will be used if it’s hard to use — that’s just a fact. Dark web threat intelligence brings a lot of details, and the more you make the users manage all those threads, the more will get dropped. The more that gets dropped, the more frustrated the users get.

Again, Bolster's use of playbooks and machine learning models comes to the rescue. Using this model, the priority is set using risk categorization, and only the most critical risks rise to the surface. This system, along with preset playbooks for remediation assistance, are key to easy-to-use monitoring software. Use of machine learning to further hone the results over time leads to a smooth, streamlined approach to dark web monitoring.

IN THIS CHAPTER

- **Reviewing the benefits of dark web monitoring with Bolster**
- **Counting the financial benefits**
- **Looking out for digital vandalism**
- **Working within the compliance environment**

Chapter 4
Measuring the Importance of Actionable Dark Web Monitoring

You may have noticed how a pretty large collection of threat intelligence is sitting around on the dark web. The next important step is making sure that the most significant pieces of actionable threat landscape are being handled effectively, and then identifying what impact they're having.

All the threats that have been collected from Bolster's scanning technology, or your threat intel tool of choice, make up a sort of security posture for your organization. This is valuable intelligence in and of itself, because it determines, among other things, what should earn your defense dollars.

Speaking of dollars, reviewing the financial and brand assets of the company is another important part of determining actionable intelligence. The dark web is arguably the very best place to find potential threats and completed attacks.

Chapter 3 covers compliance. In this chapter, we cover the important distinctions between potential and completed attacks, as well as how a tool like Bolster can help sort them out.

Reviewing Your Security Posture

Tools like Bolster promote efficiency because they collate threat findings for easy management and reduction of log toil. The availability of the details already broken down into insightful categories and collections gives your organization the rare opportunity to really review your security posture in nitty-gritty detail, without spending hours and hours collecting the data yourself.

Identity

Unquestionably, identity is the most discovered threat intelligence finding on the dark web. Why? In part, it goes back to the two kinds of identity that are important:

- **Internal accounts:** Known usernames, employee names or emails, and executive information. These relate more to attacks on your company specifically, perhaps to further build a malware attack, perform phishing campaigns, or just find weaknesses in your digital border and take advantage of that.
- **Customer information:** Usually personal information for sale, the least of which may include names and dates of birth (which is still bad). The worst case is credit card numbers or passwords. Credit card numbers are obviously bad, but passwords may give access to personal accounts and harm people who reuse passwords across different websites.

Intellectual property

Intellectual property is found solidly in the corporate camp. The general public thinks that malware is largely for causing damage within an organization, but that just isn't true. A full 25 percent of malware acts silently, allowing an attacker to come in and look around to find things for sale. If your company has a "secret sauce," that would be a fantastic choice from an attacker's perspective.

Inventorying intellectual property risks is hard. Keywords to search for to generate the list of items to search for, or List of Things, are hard to come by. Most often, this intellectual property risk falls in the malware camp for discovery and analysis by your company. That's how the bad actors will get in.

Source integrity

Intellectual property leakage can take many forms, and the "secret sauce" is only part of it. Source code, internal network information, cloud configuration, large language models (LLMs), even application programming interface (API) keys and passwords fall into the source integrity category.

Source code itself is often a significant part of the corporate security posture. Theft of underlying source code — and then the sale of said code on the dark web — potentially leaks all these examples. Looking for known unique values, understood turns of phrase, or even developer names or identifying material is the core of protecting source integrity.

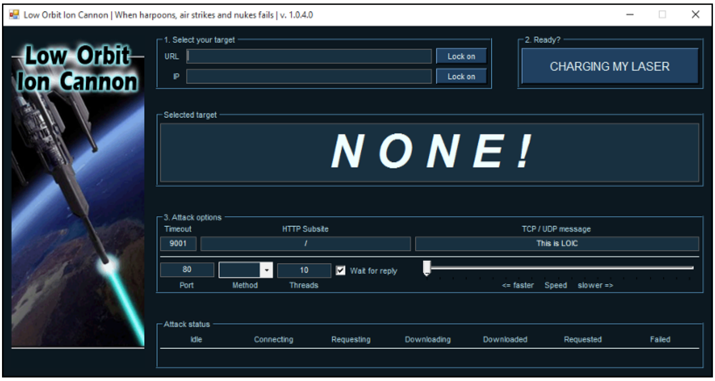
Malware

Malware comes in a number of shapes and sizes, but it has one common trait: Your internal network details in the criminals' source code is a bad, bad thing.

Security posture is heavily influenced by what the malware is for. Some are just designed to provide a path in for the attacker to look around. Sometimes it's designed for reputation damage. Some is ransomware, which is a very different kind of problem that is beyond the scope of this fine publication (but test your backups).

TECHNICAL STUFF

Host the Low Orbit Ion Cannon (LOIC) in Microsoft Azure, give it a target, push the button, and there you go. Check out the user interface in Figure 4-1. Denial-of-service (DoS) attacks can be devastating depending on your corporate model, and they're hard to find. Tools like Bolster, which is designed to categorize chatter on hidden services or the open web, are extraordinarily important when seeking information and threat levels for obscure attacks like DoS attacks.



Timeout: 9001
HTTP Subsite: /
TCP / UDP message: This is LOIC
Port: 80
Method:
Threads: 10
☑ Wait for reply
<= faster Speed slower =>

FIGURE 4-1: User interface for the Low Orbit Ion Cannon.

Protecting Financial Assets

In the end, nearly all threats come down to money. The bad actors can sell assets they steal, or take payment for damaging a brand, or collect a ransom, or straight up take the money and run.

Actionable monitoring of the threat landscape using a tool like Bolster will save your company money, full stop. Proactively or reactively, handling the problem at the outset is how best to protect your cash box.

Of course, knowing ahead of time that there is ransomware with your name on it may allow you to completely prevent an attack from ever occurring. That's the best way to protect assets for certain.

Protecting assets reactively is a little harder. After assets are in the hands of the criminals, reducing the value of those assets to the criminals is the only way to effectively protect the bottom line.

For instance, if customer credentials were stolen, quickly identifying what data is exposed through the Bolster dashboard so you can immediately ask the impacted users to change their passwords would significantly reduce the value of the list. Remind them to turn on two-factor authentication too, if it's available!

Defending the Brand

Brand impersonation is less often about money and more often about spite. Defending the brand is still an important part of the overall importance of threat modeling in general and dark web threat intelligence in particular.

TIP

Bolster AI's industry-leading machine learning models and LLMs will help to find planned or implemented brand impersonation. Although it's tempting to think that any mention of a brand on an Internet Relay Chat (IRC) channel that is hosted on a hidden service is referencing brand impersonation, it isn't necessarily. Even if it were, it's important to know what's being planned.

The issue is that translating general chatter is nontrivial. A trained machine learning model can make it easier, but not foolproof. Of the dark web threats covered in this book, the importance of brand can't be understated, but it still remains the hardest to discover, collate, and remediate.

Meeting Compliance Regulations

Earlier, we discuss compliance mostly from the perspective of a consumer of threat intelligence for convincing the auditor of effort. There are two significant exceptions to this where the importance of actionable intelligence shows up: Systems and Organizations Controls 2 (SOC 2) and the General Data Protection Regulation (GDPR).

TIP

Three of the five SOC 2 principles are covered in monitoring the dark web:

- Security
- Confidentiality
- Privacy

If a SOC 2 certificate is your organization's goal, dark web monitoring is a great start. Dark web monitoring dramatically reduces the time it takes to detect a breach and reduces the value of any assets that have been stolen. Also, with the correct playbooks in place, like the ones offered through Bolster's platform, you can defend customers and employees and their personal information on the dark web.

GDPR is a European Union (EU) standard for privacy for which the collation capability of Bolster is well used. Minor leaks of data can often go unnoticed in an overall security breach, but they’re nearly always either put up for sale on the dark web or talked about on hidden services. Although the GDPR doesn’t require dark web monitoring, keeping an eye out will certainly future-proof your security posture against what will surely become part of the regulation.

These standards bodies are becoming more common and broader in scope throughout the world. Protection of consumer data through the requirement of understanding what’s handling that data is a core concern, and monitoring the dark web is an important part of that control.

Chapter 5
Ten (or So) Threats to Watch

A remarkable number of threats are out there, on the dark web and the open web. Here are a few that have been discussed in this book, plus a couple of new ones to chew on:

- **Employee emails:** The email addresses of key players in your company should certainly be on the collection of search terms you'll use to hone your threat research. Finding any of those emails in discussion forums, source code, or just general chatter is a bad thing. Remediation isn't easy, but it's time to be on alert.
- **User accounts and passwords:** User accounts and passwords are harder to look for than you may imagine. Folks reuse emails for several applications, so finding an email of one of your users with a password doesn't necessarily mean it was stolen from you.
- **Internal network details:** Internet Protocol (IP) addresses along with internal server names, test URLs for applications, and other internal data is a certain sign that an application is soon to be under attack. The bad actors need to know where the front door is.

- **Customer emails:** Like user accounts, this is hard to find, which is why it's on this list. Just because a customer email is in a dark web forum doesn't mean you're at risk. People use their email addresses for lots of things. Still, this is a threat that should be considered.
- **Brand discussion:** General chitchat about a brand is often a harbinger of vandalism. Folks talk to one another about a company that they disagree with and try to form a posse of folks with different skill sets to run the attack. Certainly worth watching.
- **Users' personal information:** If you're storing personally identifiable information for users, selections from that list should certainly be on your List of Things. Perhaps even creating some fake information stored in your data source so you aren't searching for real personally identifiable information (PII) is a consideration.
- **Malware:** Trying to categorize information gathered from source code is nontrivial. That said, it pays off if something is found. Internal company details inside of malware is an almost certain indication of compromise.
- **Data for sale:** Does your company have data that is unique? Again, toss a few honeypots in that store and see what you come up with. You don't have to search for the real data, but you'll know if you've been compromised.
- **Ransomware:** Not unlike general malware, ransomware is bad code that will encrypt your data and require a purchased key to recover it. It can be found the same way malware is found — internal details in source code, but combined with well-known encryption algorithms.

Gain visibility into dark web threats

The dark web is spoken of breathlessly by the press, C-level executives, and consultants the world over. Fact is, there is surprisingly little difference between the dark web and the open web, except how you get there and who hangs out there. The trick is to get actionable monitoring on it, eyes open in the dark as it were. Only then can real remediation of dark web threats begin.

Inside…

- Find threats on the dark web
- Determine risk of discovered threats
- Make use of intelligence tools
- Organize remediation
- Keep an eye on the changing landscape
- Visualize business-critical threats with Bolster
- See how you did

BOLSTER

Bill Sempf is an author, developer, and application security specialist who spends way too much time on the wrong side of the Internet tracks. His 30 years of Internet experience is primarily focused on keeping people safe online, despite their best efforts.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-19648-7
Not For Resale

9 781394 196487

for dummies®
A Wiley Brand