Dark Web 201

How to Leverage External Threat Hunting to Prevent Cyberattacks

www.intsights.com

Dark Web 201: How to Leverage External Threat Hunting to Prevent Cyberattacks

A necessary pillar of an effective cyber defense strategy is the capability to detect and mitigate threats at the earliest stages of the cyber kill chain. While internal and perimeter security solutions are critical to your security program, external threat intelligence gives you the ability to defend forward by eliminating threats outside the wire. This ebook is designed to provide a framework for security professionals on how to conduct effective external threat hunting on the dark web.

The dark web is a haven for cybercriminal activity. Accessible only through private browsers, like Tor, that enable anonymous browsing and communication, the dark web allows threat actors to operate in the shadows and maintain relative obscurity and anonymity. While most cybersecurity professionals are well aware of the dangers that lurk across the dark web, many do not have the time, knowledge, or tools at their disposal to identify, validate, and mitigate threats that are being orchestrated against them. The dark web, by far, provides the most challenging landscape for threat hunting due to its anonymous nature and inherent challenges in enforcing regulations.

The Dark Web 101
What Every Security Pro Should Know
INTSIGHTS

Dark Web 101

Learn what every cybersecurity professional needs to know about the how the dark web works and how cybercriminals use it to plot attacks.

DOWNLOAD YOUR COPY

Creating a Game Plan: You're Only as Good as Your Sources

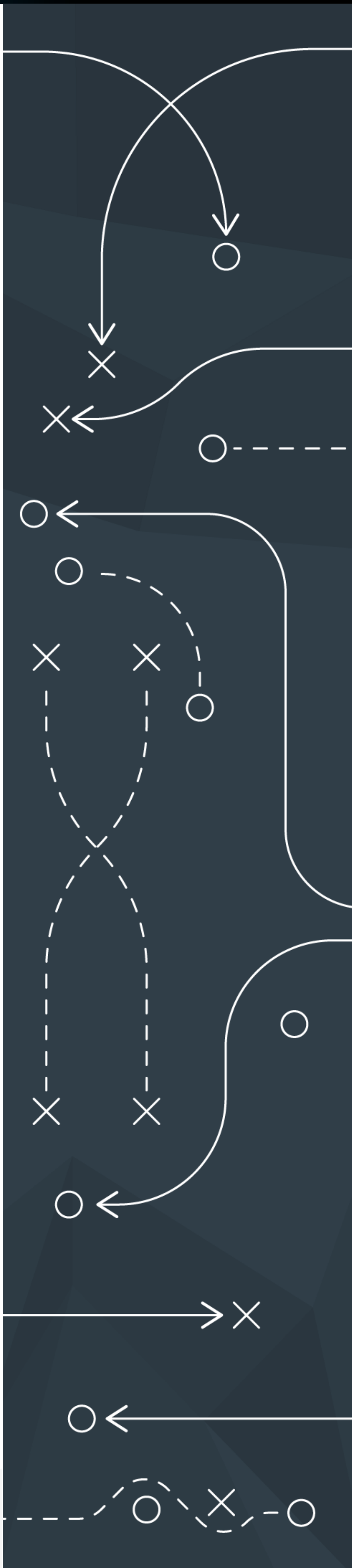
Strong intelligence starts with good sources. Your sources can be found in any place where you hunt for or gather intelligence, including black markets, hacker forums, and instant messaging groups, like Telegram, IQ, and Discord. It's much better to have one source of really strong intelligence than to have thousands that turn up very little. In addition, it's critical to map the threats, attack vectors, and source types that are most important to your unique organization, so you can focus on establishing the right mix of sources.

Each organization will have different sources and hunting methodologies based on its intelligence needs, weak points, common attack vectors, industry-specific threats, and more. For example, the ways a bank could be attacked are very different from the ways a healthcare organization might be. Therefore, threat hunters must tailor their efforts to the landscape surrounding their organizations and utilize sources that enable them to find relevant threats. Banks probably don't need to hunt for leaked medical records, and healthcare organizations probably don't care as much about stolen credit card numbers.

There are many different types of sources across the dark web where you can find threats, and these source types often specialize in a certain area of cybercrime or information trade. Here are some common "sub-categories" of dark web sources:

- **General Markets:** These markets offer almost anything for sale, including drugs, weapons, credit card dumps, miscellaneous services, digital products, counterfeit merchandise, and much more.
- **PII & PHI:** These markets sell personal identifiable information (PII), like Social Security Numbers (U.S. Market), mailing and email addresses, and dates of birth.
- **Credit Cards:** These markets and forums are dedicated to buying, selling, and sharing leaked or stolen credit cards. They can often be purchased in bulk or individually.
- **Digital Identities:** These are relatively new sites on the dark web that sell stolen "digital fingerprints" of a user's web browsing device (i.e., IP address, OS information, time zone, user behavior). These sites enable the purchaser to impersonate a legitimate online user and circumvent standard security protocols. Some examples of these sites include the Genesis Market and Richlogs.
- **Information Trading:** This can include stolen databases, leaked documents, trade secrets, and more.
- **Remote Access:** These sites sell and trade Shells (exploits) and remote access via RDP, VNC, or other access to hacked servers.
- **Personal Documents:** This might include stolen passports, driver's licenses, social security cards, or fake IDs.
- **Electronic Wallets:** These sites sell access to stolen or compromised wallets, typically containing Bitcoin or other cryptocurrencies

If there's one constant across the dark web, it's change. These dark web sources of cybercriminal activity are never permanent, often being shut down by law enforcement or taken offline by administrators to avoid getting caught. Staying on top of the latest movements and popular hubs is a tricky task given the elusive nature of the threat actors using them. That's why becoming an active member of the community can open the door for threat hunters to stay on top of the constant change and access the most valuable sources across the dark web.

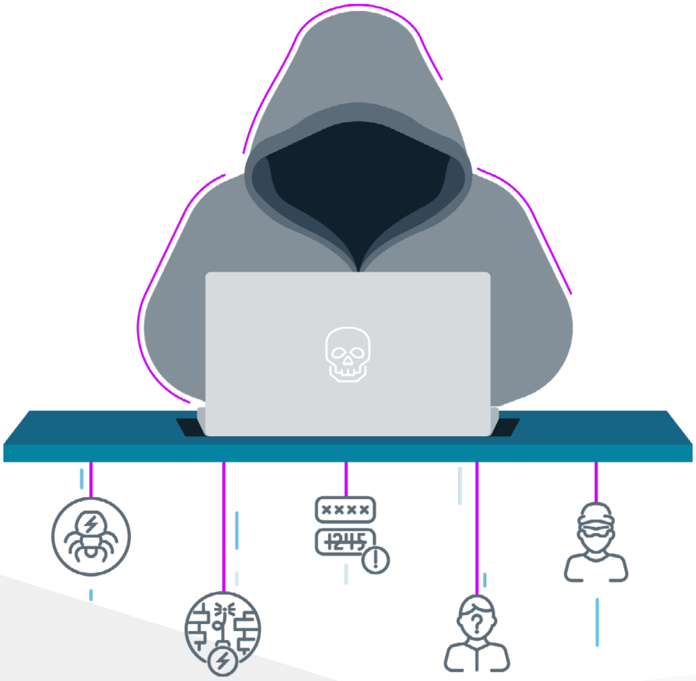


Establishing Access: Venturing Behind Enemy Lines

Cybercriminals and other threat actors are intentionally deceptive, and will try to avoid being identified in any way possible. This makes searching for sources challenging – where do you begin? To compound the challenge, activity hubs are periodically shut down by law enforcement with no notice, forcing threat actors and threat hunters alike to adapt on the fly and find new sources for trade and information exchanges. Since most dark web activity takes place on the Tor browser, which anonymizes users and isolates each site, it can be difficult to keep track of forums and black markets, which are often unindexed and only accessible via obscure URLs.

During the past year, there have been several notable shutdowns – Altenen was shut down by Israeli authorities in May 2018, and Dream Market voluntarily closed its doors at the end of April 2019, which may or may not have been part of a law enforcement sting. Deep Dot Web, Valhalla, and Wall Street Market were shut down by authorities soon thereafter. Going back a couple of years, AlphaBay and Hansa were shut down in July 2017. The more popular a site becomes, the more likely it is to be shut down or taken offline.

These closures and shutdowns of large-scale markets in recent years show there is no singular source of cybercriminal activity. Tracking emerging black markets can be helpful, but the best intelligence is often gathered by assimilation into cybercriminal watering holes. Threat hunters must earn the trust of cybercriminals to become accepted into those communities, which can be a complex and risky task – one that CISOs often outsource to experienced professionals.



What is the Tor browser?

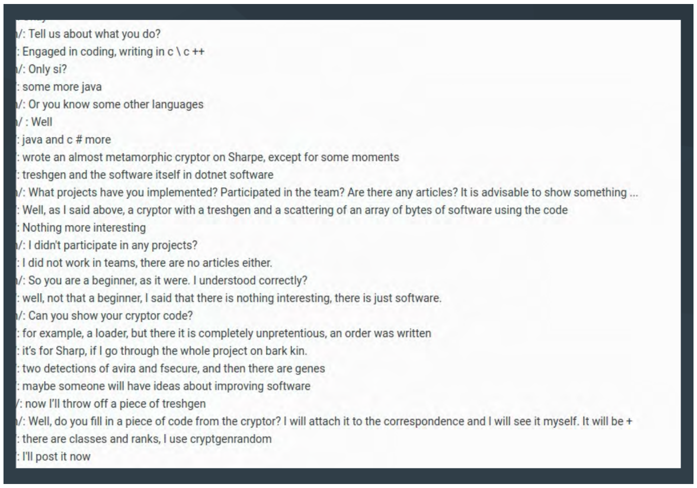
Tor is a dark web browser that was originally created by the United States Naval Research Laboratory in 2002 as an anonymous communication tool for intelligence agencies. Ever since, it has become the go-to tool for cybercriminals, cybersecurity professionals, researchers, academics, and law enforcement alike. Tor works by randomly routing a user's encrypted traffic through a series of connected volunteered systems, called relays. This ensures activity cannot be traced back to the end user. Tor users can access special sites with .onion domains, which can only be accessed through Tor browsers.

Tor is now maintained by The Tor Project, a non-profit 501c3 organization based in Massachusetts. While funding is provided by a number of foundations, corporations, and individuals, the vast majority of the Tor Project's funding continues to come from the U.S. Government. Despite this, Tor is largely unregulated – in part due to its anonymous nature – allowing cybercriminals and hackers to form a thriving ecosystem.

Assimilating Into the Hacker Community

Threat hunters are faced with a daunting task: infiltrating advanced hacking and cybercrime communities where the barriers to entry are substantial. In order to be accepted into these communities, new users often must pass a series of tests – both literal tests and tests of character – to prove they are both technically capable and, most importantly, not working with law enforcement or cybersecurity groups or companies. In sophisticated forums, you must demonstrate your technical prowess by passing rigorous, challenging tests that sometimes require a referral just to take these exams.

The language barrier is one of the biggest challenges threat hunters face – not necessarily in terms of being fluent in certain languages, but, rather, being fluent in cybercriminal jargon. The slightest slip-ups can expose threat hunters as undesirables and lead to instant bans from the communities they are trying to access. Even worse, if your true identity is discovered, it makes you and your company instant targets for hackers.



```
/: Tell us about what you do?
: Engaged in coding, writing in c \ c ++
/: Only si?
: some more java
/: Or you know some other languages
/ : Well
: java and c # more
: wrote an almost metamorphic cryptor on Sharpe, except for some moments
: treshgen and the software itself in dotnet software
/: What projects have you implemented? Participated in the team? Are there any articles? It is advisable to show something ...
: Well, as I said above, a cryptor with a treshgen and a scattering of an array of bytes of software using the code
: Nothing more interesting
/: I didn't participate in any projects?
: I did not work in teams, there are no articles either.
/: So you are a beginner, as it were. I understood correctly?
: well, not that a beginner, I said that there is nothing interesting, there is just software.
/: Can you show your cryptor code?
: for example, a loader, but there it is completely unpretentious, an order was written
: it's for Sharp, if I go through the whole project on bark kin.
: two detections of avira and fsecure, and then there are genes
: maybe someone will have ideas about improving software
/: now I'll throw off a piece of treshgen
/: Well, do you fill in a piece of code from the cryptor? I will attach it to the correspondence and I will see it myself. It will be +
: there are classes and ranks, I use cryptgenrandom
: I'll post it now
```

Figure 1: A forum moderator tests a user attempting to gain access to a forum (translated from Russian). The user failed the exam and was denied entry into the community, despite demonstrating some technical knowledge.

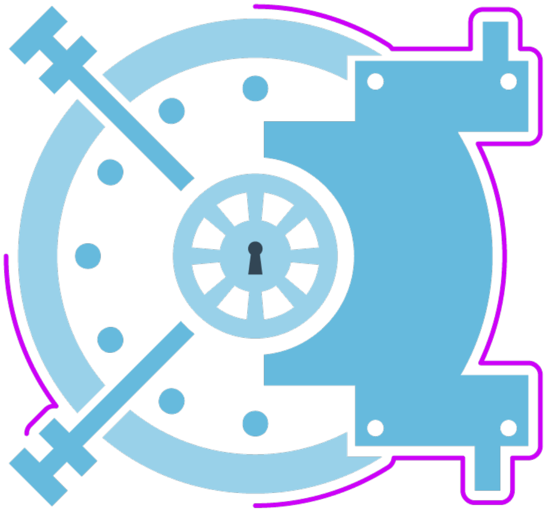
To further complicate matters, even those experienced with cybercriminal lingo might be considered suspicious if they attempt to gain access using a new avatar. It is therefore critical to spend time cultivating an active persona, sharing useful information with other users, and contributing on more publicly accessible dark web forums to prove your credibility. It's also important to take part in these forums at odd hours of the day. It's easy for hackers to sniff out a threat hunter via avatars that only log in from 9 to 5.

Think of it like tending a vegetable garden: If you spend more time feeding and weeding it, you'll eventually yield better quality crops. If you do the bare minimum and neglect your plants, they will eventually wither and you'll have to start over.

Security Measures and Identity Protection

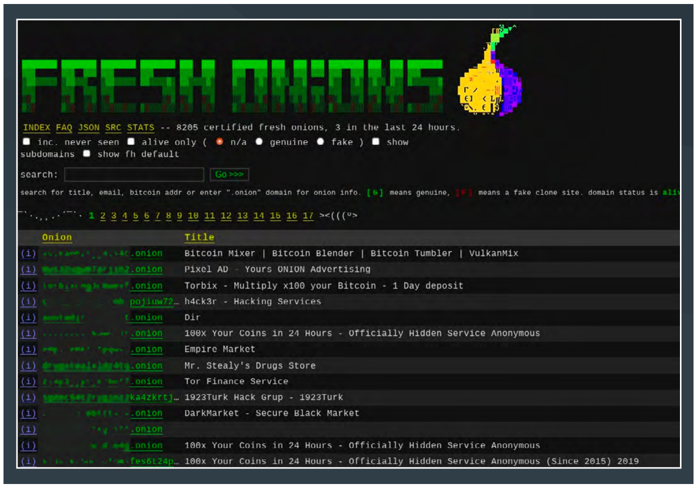
Even on the anonymized dark web, identity protection is crucial for threat hunters. Although your connection is anonymous, your device can still be hacked or infected, which can expose your true identity. Before venturing onto the dark web, you should invest in security tools that will help ensure your identity does not risk exposure. Some examples include using a virtual private network (VPN) and/or proxy, and setting up a virtual machine before connecting via Tor. As always, it's wise to implement multiple layers of security to decrease the chance of being outed (or doxxed, as it's referred to online).

Moderators of cybercriminal hangouts are actively searching for threat hunters, law enforcement agents, and other dark web users who are seeking to thwart their efforts. They constantly analyze users to find holes in their backstories or other clues that might expose them as oppositional. Threat hunters must operate with caution to avoid putting themselves and their organizations at risk.



Staying on Top of New Sources

The dark web is a volatile place, with new websites, markets, and forums constantly being spun up, moved, and taken down. Hackers like to move around and quickly shift the sites they use in their attempts to avoid law enforcement. To be an effective threat hunter, you need to constantly monitor for – and gain access to – new sources that can be used for intelligence gathering.



INDEX FAQ JSON SRC STATS -- 8205 certified fresh onions, 3 in the last 24 hours.

□ inc. never seen □ alive only (● n/a ○ genuine ○ fake) □ show subdomains □ show fh default

search: Go >>>

search for title, email, bitcoin addr or enter ".onion" domain for onion info. [G] means genuine, [F] means a fake clone site. domain status is ali

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 ><(((º>

	Onion	Title
(i)	[redacted].onion	Bitcoin Mixer | Bitcoin Blender | Bitcoin Tumbler | VulkanMix
(i)	[redacted].onion	Pixel AD - Yours ONION Advertising
(i)	[redacted].onion	Torbix - Multiply x100 your Bitcoin - 1 Day deposit
(i)	[redacted]pojiuw72…	h4ck3r - Hacking Services
(i)	[redacted].onion	Dir
(i)	[redacted].onion	100x Your Coins in 24 Hours - Officially Hidden Service Anonymous
(i)	[redacted].onion	Empire Market
(i)	[redacted].onion	Mr. Stealy's Drugs Store
(i)	[redacted].onion	Tor Finance Service
(i)	[redacted]ka4zkrtj…	1923Turk Hack Grup - 1923Turk
(i)	[redacted].onion	DarkMarket - Secure Black Market
(i)	[redacted].onion	
(i)	[redacted].onion	100x Your Coins in 24 Hours - Officially Hidden Service Anonymous
(i)	[redacted]fes6t24p…	100x Your Coins in 24 Hours - Officially Hidden Service Anonymous (Since 2015) 2019

Figure 2: A snapshot of discovery tool Fresh Onions, which allows users to find new dark web sites and communities

It can be difficult to search across the dark web, but there are a few popular crawlers that can be used to discover new sites. One of the more popular ones is Fresh Onions, but it often gets taken offline and has limited reach, so it may not be as reliable as Google.

Speaking of Google, the clear web can often be used to find entry points into dark web forums. Simply Googling "dark web websites" or "dark web forums" often returns clear web sites that offer .onion links to dark web pages. However, these are often well-known and well-established sites on the dark web, so you likely won't find anything brand new or highly exclusive.

Telegram, another channel that's growing in popularity among dark web users, can be used to find new hacker watering holes. Telegram is an instant messaging platform that has both open and invite-only groups. The invite-only groups typically have the best resources (with highly restricted access), but users often post new forums or markets on open channels. If you're active in Telegram and build your credibility, you can sometimes get invited to the more exclusive private groups.

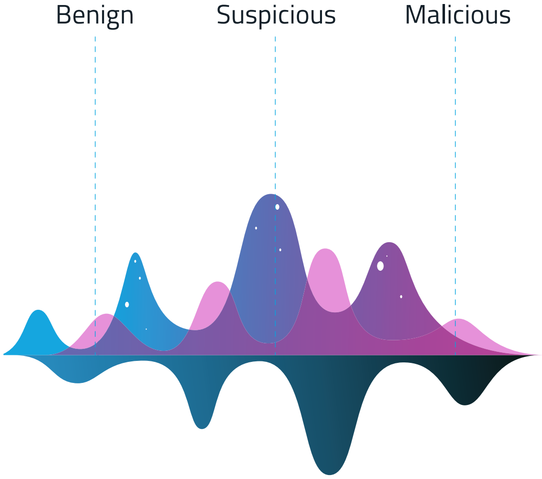
Overall, the best way to stay on top of new sources on the dark web is to embed yourself into the community. This takes both time and skill, as you'll need to blend in with other threat actors, and often will have to build your credibility as a "fellow threat actor" to be trusted. If done correctly, this is the best way to find new sources of intelligence as hackers like to share only with people who have been vetted. The stronger your dark web reputation, the more likely you'll get invited to exclusive groups and forums.

Generating Intelligence: Identifying Threats Targeting Your Organization

Now that you've identified your sources and established yourself as credible, you need to know what to look for. Much goes on across the dark web, and threat hunters are often tasked with trying to find the needle in the haystack. But when it's discovered, it can be incredibly valuable in helping you anticipate and mitigate threats before they're used against you.

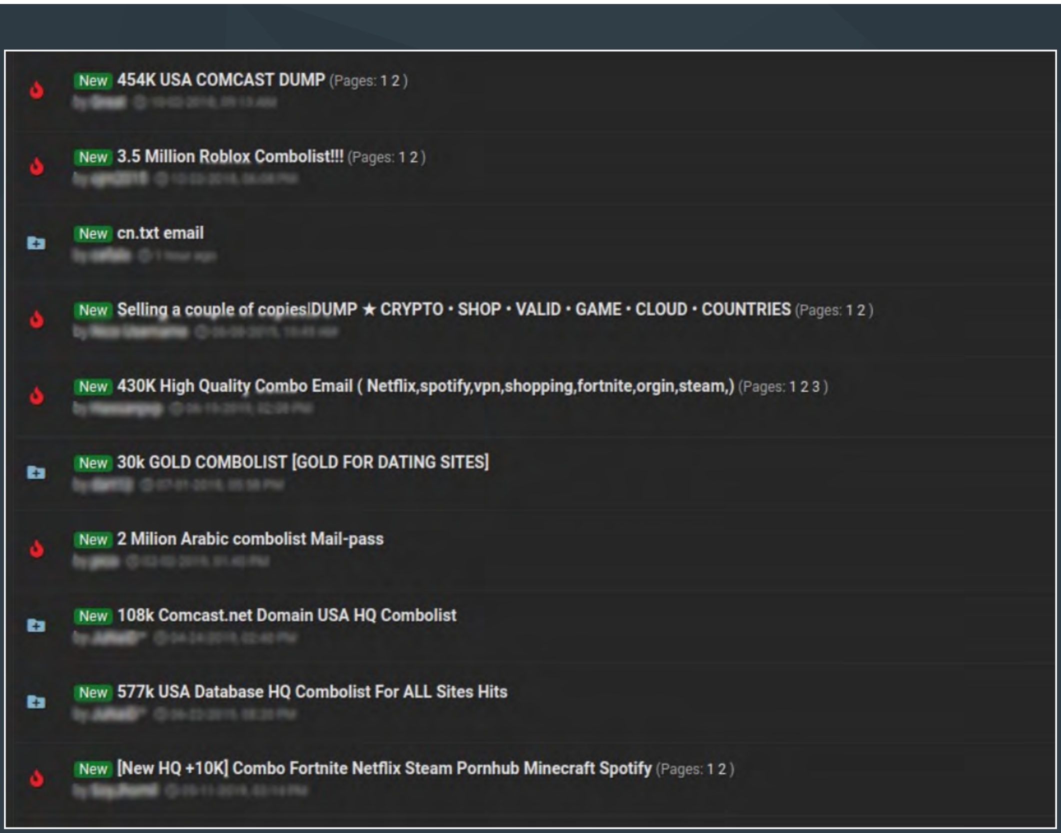
Identifying and Validating Threats

As you can imagine, finding threats on the dark web is not black and white. False claims are often made, data is constantly recycled, intent is not always clear, and validation is often needed to distinguish benign activity from suspicious or malicious campaigns. Think of it as a spectrum, with benign all the way to the left, suspicious in the middle, and malicious to the right. So, how do you assess whether a threat is far enough toward "malicious" to warrant action?



Threat hunters often need to piece together separate clues from different sources to understand the full context of a threat. This might involve purchasing or asking for samples of data for sale to validate sources and/or legitimacy. It's also important to track and record activity over time, as threats often evolve over the course of weeks or months. All of these variables play a part in determining the context and severity of a threat, so it's critical to have broad visibility and sufficient analysis skills to uncover threats in a sea of unrelated activity.

Ultimately, intelligence is only useful if you can act on it, so it's critical to find and validate threats that specifically relate to your organization.



New 454K USA COMCAST DUMP (Pages: 1 2)
[redacted]

New 3.5 Million Roblox Combolist!!! (Pages: 1 2)
[redacted]

New cn.txt email
[redacted]

New Selling a couple of copies|DUMP ★ CRYPTO • SHOP • VALID • GAME • CLOUD • COUNTRIES (Pages: 1 2)
[redacted]

New 430K High Quality Combo Email (Netflix,spotify,vpn,shopping,fortnite,orgin,steam,) (Pages: 1 2 3)
[redacted]

New 30k GOLD COMBOLIST [GOLD FOR DATING SITES]
[redacted]

New 2 Milion Arabic combolist Mail-pass
[redacted]

New 108k Comcast.net Domain USA HQ Combolist
[redacted]

New 577k USA Database HQ Combolist For ALL Sites Hits
[redacted]

New [New HQ +10K] Combo Fortnite Netflix Steam Pornhub Minecraft Spotify (Pages: 1 2)
[redacted]

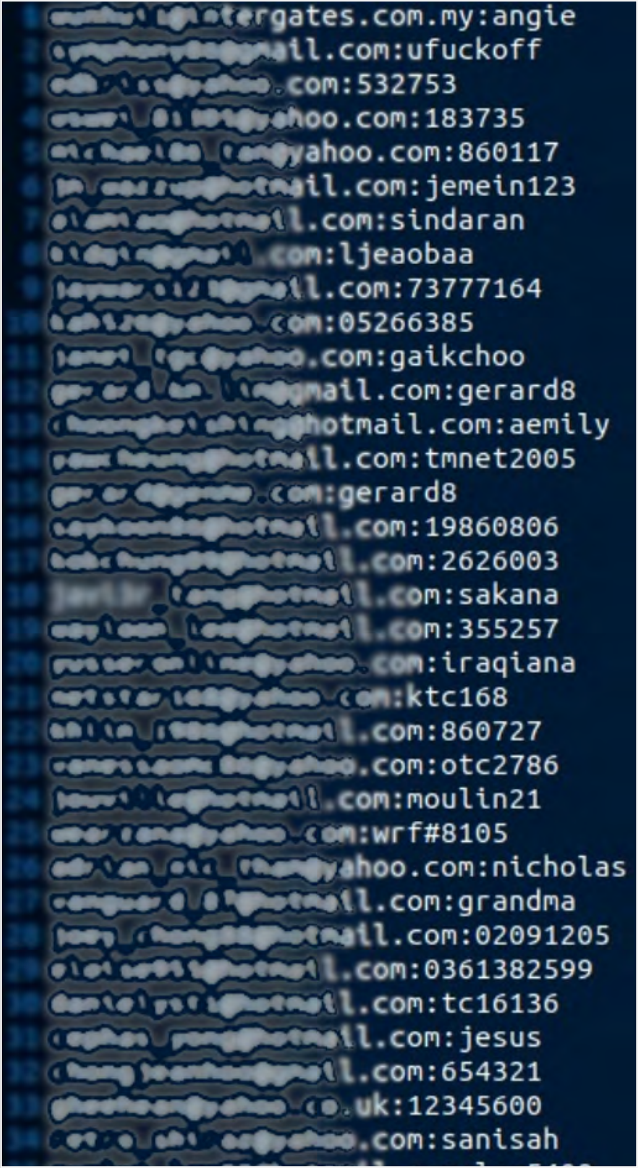
Figure 3: Claims of stolen goods and digital assets on a popular forum

Automating External Threat Intelligence

Continuous dark web monitoring is a time-intensive – and often overwhelming – task for even the largest teams of threat hunters and researchers. This is why many organizations are embracing external threat intelligence solutions that allow them to automate the monitoring and analysis process for dark web intelligence. This is often complemented with additional manual hunting and threat validation to significantly reduce the burden on security operations teams that are charged with rapidly responding to and mitigating cyberattacks.

The key to building an effective intelligence process is to connect it to your existing security initiatives. Take credential leakage, for example. Every organization needs to ensure its employee credentials are secured to avoid unauthorized access to company systems. Leaked credentials are one of the most common digital goods on the dark web, so companies must have clear processes established for how to identify and lock down compromised credentials while minimizing disruptions to employee productivity. Activities should include collecting new credential dumps, analyzing contents, validating credentials against your Active Directory, and orchestrating appropriate action to reset or lock down those credentials.

External threat intelligence supports numerous security initiatives. Mapping out the mitigation process is one fundamental way to gain value from your intelligence program.



```
[redacted]tergates.com.my:angie
[redacted]il.com:ufuckoff
[redacted].com:532753
[redacted]hoo.com:183735
[redacted]yahoo.com:860117
[redacted]il.com:jemein123
[redacted]l.com:sindaran
[redacted]om:ljeaobaa
[redacted]l.com:73777164
[redacted]om:05266385
[redacted].com:gaikchoo
[redacted]mail.com:gerard8
[redacted]hotmail.com:aemily
[redacted]l.com:tmnet2005
[redacted]om:gerard8
[redacted].com:19860806
[redacted].com:2626003
[redacted].com:sakana
[redacted].com:355257
[redacted]om:iraqiana
[redacted]m:ktc168
[redacted].com:860727
[redacted].com:otc2786
[redacted].com:moulin21
[redacted]m:wrf#8105
[redacted]ahoo.com:nicholas
[redacted]il.com:grandma
[redacted]il.com:02091205
[redacted].com:0361382599
[redacted]l.com:tc16136
[redacted]il.com:jesus
[redacted].com:654321
[redacted].uk:12345600
[redacted].com:sanisah
```

Figure 4: Example of a large-scale credential leak containing email addresses and passwords

Taking It to the Next Level: Using HUMINT to Bolster Threat Hunting

When cybersecurity teams extend their visibility beyond their perimeters, they often look across the clear, deep, and dark web for indications that they are at risk or may be attacked. There are many tactical elements – like automating the process for discovering leaked credentials – that build a foundation for effective dark web monitoring. But there are more advanced tactics that can be used to go deeper to uncover the threat actors and motives behind attacks.

This practice is called HUMINT – or Human Intelligence – and it involves gathering intelligence through interpersonal contact and engagement, rather than by technical processes, feed ingestion, or automated monitoring. It's typically a manual process, requiring a very specific set of skills and knowledge to remain undercover and not raise suspicion.

It's the high-tech equivalent of what an undercover FBI agent does, spending months or years working to infiltrate a criminal organization. It's painstaking and nerve-racking work, and can be a dangerous activity for an individual, regardless of experience and skill. Here are some key use cases for establishing sources and conducting HUMINT gathering:

> **Post-Attack Investigation:** Hackers will often make claims or take credit for attacks online. If the attack mentions your company or, perhaps, another in your industry, it may be worth contacting the threat actor to investigate how the attack was launched, what entry points were used, and which tools were deployed. This intelligence can be used to stop further damage and/or protect against a similar attack.
>
> **Extortion Attack Damage Assessment:** If your company is being extorted, you might want to verify what data has been stolen as well as its value. This information can be used to assess the potential impact of a breach.
>
> **New Attack Vector Discovery:** As a part of the threat hunting process, HUMINT can be used to discover new scamming methods, new exploits, and other hacker TTPs that may be used against you. Threat intelligence solutions can provide you with a lot of this intelligence, but supplementing it with your own HUMINT gathering can help you gain an even deeper understanding of current threats.

Because sources and avatars take time to develop, you shouldn't wait until after one of the above scenarios happens to begin collecting HUMINT. You need to start developing your HUMINT process now so that you have the credibility and sources in place if you find yourself in one of these situations. If you reach out to threat actors as a new avatar right after a recent security incident, they will immediately be suspicious of your motives.

HUMINT

Download our white paper to learn more about HUMINT gathering.

DOWNLOAD YOUR COPY

Threat hunting is a risky endeavor for security teams, but the intelligence gathered can give you a significant advantage in protecting your organization. Remember, this is a delicate practice that should be performed only by experienced professionals. The last thing you want to do is be exposed and immediately and simultaneously put your personal life and organization at risk.

What can IntSights do to help?

IntSights provides a comprehensive external intelligence solution that enables organizations to identify and neutralize threats across the clear, deep, and dark web. Using our unique cyber reconnaissance capabilities and multi-dimensional threat analysis, we deliver validated, actionable intelligence and orchestrated mitigation to help you proactively protect your organization. Our platform seamlessly integrates with existing security solutions to eliminate operational vulnerabilities, secure data, and protect resources.

Our commitment to marrying automated external threat intelligence with expert threat hunting by our dedicated analyst team empowers security teams to take control of the environment beyond their perimeters and Defend Forward.

The dark web poses a risk to all organizations, but it also presents an opportunity. Start using dark web activity to inform a proactive security strategy, and gain an advantage over your adversaries.

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the open, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: https://www.intsights.com.