The What, Where & When for Effective Dark Web Threat Hunting

wipro | INTSIGHTS

Intoduction.

As the cyber-crime ecosystem evolves, cyberattacks are becoming more complex, creative, and tailored to the industries and organizations they target. To do this, attackers must research, prepare and seek out information on their targets prior to an attack. While each attack may differ, the general types of information an attacker is required to have to succeed remain similar. So, by setting up the right monitoring and investigative processes, it is possible for organizations to detect and gain context around an attacker's plan of attack before damage is done by tracking what they seek out.

Today, the cybersecurity community focuses a great deal on technical elements and indicators of malicious activity to detect threats - and has thus invested heavily in technologically driven solutions. However, at IntSights, we believe there is much to be gained from investigating the human factor behind attacks and that in doing so, it is possible to uncover actionable warning signs much earlier in the cyberattack chain than through technological means alone. That is why we continuously monitor the dark web, collecting millions of data points on hacker behavior to give our clients the best chance at detecting an attack before damage is done. When classifying each data point we gather, we always start with the same three questions:

1. **What malicious intent or activity was discovered?**
2. **Where and how was this information detected?**
3. **When in the planning process would this information be valuable?**

No matter the maturity level of your organization, when analyzing a new piece of intelligence, you should always start by asking yourself these three questions. They will enable you to better understand the scope and nature of detected threats, form a strategy to prioritize and monitor risk, and finally, if and how to allocate resources towards a response or intervention.

The Big Three: What, Where, When.

When it comes to identifying new sources of risk and potential indicators of attack, there are three guiding questions: What? Where? When? They may seem obvious, but from our experience working with clients across the globe, sometimes answering these questions can be quite challenging. Let's break them down:

What

Am I Protecting
- Asset Types
- Employee Groups
- Geographic Locations
- Customer Data
- Secret Projects or IP

Am I Defending Against
- TTPs
- Adversary Groups
- Insider Threats
- Customer Fraud

Where

Did this Info Come From
- Forums & Markets
- 3rd Party Data Leaks
- Mobile Messaging Apps
- Government Notification

Am I Defending Against
- TTPs
- Adversary Groups
- Insider Threats
- Customer Fraud

When

Was It Detected
- Reconnaissance
- Initial Compromise
- Early Foothold
- Lateral Movement
- Data Exfiltration

Is Action Required
- Immediately
- In the near term
- Longer term

What.

There are two big 'whats' every threat hunter needs to be able to answer:

1. **What are you most focused on protecting?**
2. **What types of attacks, techniques, or groups are targeting your industry?**

When answering these questions, avoid generic statements or groupings, and try to be specific. If you work at a large retailer for example, rather than protecting "company assets", try and focus on the two or three key targets that keep you up at night – perhaps POS and customer loyalty databases – and the techniques or groups focused on those asset types – perhaps ransomware and Russian organized crime. Being able to answer the two whats is essential to sourcing the right threat intelligence and analyzing what is truly actionable, as they define the basis from which relevance, actionability, and impact severity can be derived.

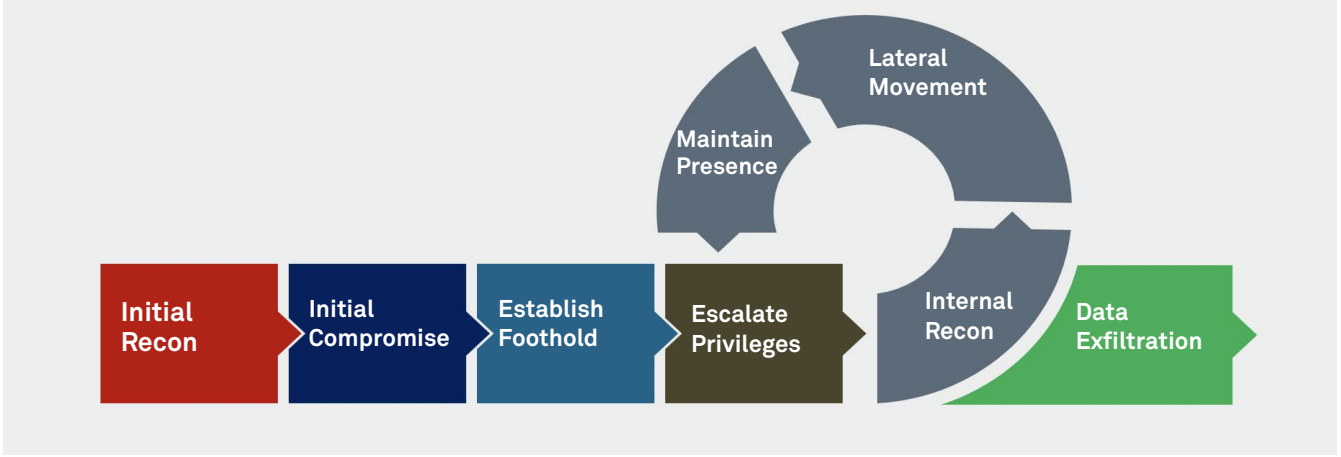
Where.

Where can I find actionable intelligence? Having defined what you are protecting and what types of attacks you are most likely to encounter, this is the logical next question. Given the proliferation of both high quality and low quality threat intelligence sources, information on likely attack techniques or indications of an attack can be found in a lot of different places. For beginners, dark web forums are a great place to start. The forums, of which there are hundreds, are popular communities where hackers exchange ideas and even trade illegal merchandise. The type, topic and users on the forum varies - they can be malware analysis sites that have samples of malware that could be analyzed for attack indicators – or they could be mobile based chat groups with attackers seeking specific information related to your organization to better inform an upcoming attack.

For the less sophisticated, industry specific ISACs and threat intelligence firms, such as IntSights, can be a great resource for those without the resources or desire to go dark web hunting on their own. Understanding where, even at a broad level, hackers may be sharing or discussing information relevant to your organizational needs will dramatically narrow your scope of monitoring and enable you to get the most out of your limited resources.

When.

When in the attack chain does a particular threat occur? And when can it be detected? Understanding the answers to these questions can enable you to better gather the right qualitative indicators that appear earlier in the attack chain. These human driven factors often appear far earlier than technical indicators and can enable preventative action such as reporting and removing of fake domains before a phishing attack is executed. It is also possible sometimes to directly engage with an attacker, using avatars, to gain more information on the nature or severity of the threat.By focusing on these questions and developing systems to watch and alert as threats arise, you'll be able to peer earlier into the attacker supply chain and be positioned to act quickly and with the context needed to minimize damage or stop an attack entirely.



Classifying Threats - The IntSights Process

Having answered the big three (what, when, where), you should now have a solid understanding of what information is useful to begin collecting and gathering, and the focus can shift to data classification and filtering. As stated earlier, threat intelligence can come in many forms and being able to bucket and group this information into a framework that can be leveraged and acted upon is essential. At IntSights, we've spent a great deal of time thinking about this problem and use the answers gained from the big three to classify the cyber threat intelligence we gather into six main categories: Attack Indication, Data Leakage, Phishing, Brand Security, Exploitable Data and VIP.

Attack Indication: Attack indications are, as the name suggests, documented indications that an attack may be being planned, organized, actively executed, or recently occurred. These are typically soft indicators, such as online chatter between hackers or derived from a new item up for sale. While often not directly actionable, this information can provide critical insight into the types of threat actors targeting your organization, how they plan to exploit a vulnerability in your defenses to gain entry, or what types of information they are attempting to steal.

Data Leakage: Unfortunately, this is often a retroactive indicator suggesting an attack has occurred. Data leakage is the posting of confidential information online. This type of data can help incident response teams more quickly scope what type of data may have been stolen, the source of intrusion, and if caught quickly, prevent further damages.

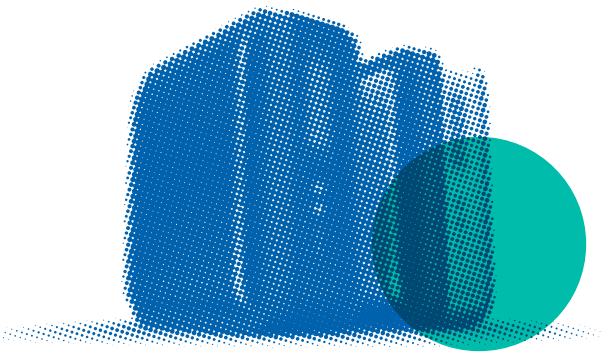
Phishing: This branch of social engineering has become a favorite of hackers of late due to its relative ease to set-up and high success rate. Cyber criminals use domains similar to company domains or spoof legitimate accounts aimed at getting employees or customers to volunteer sensitive information.

In recent years, dark web vendors have popped up offering customized turnkey phishing solutions targeting well-known brands – making it even easier for hackers to launch these types of attacks at scale.

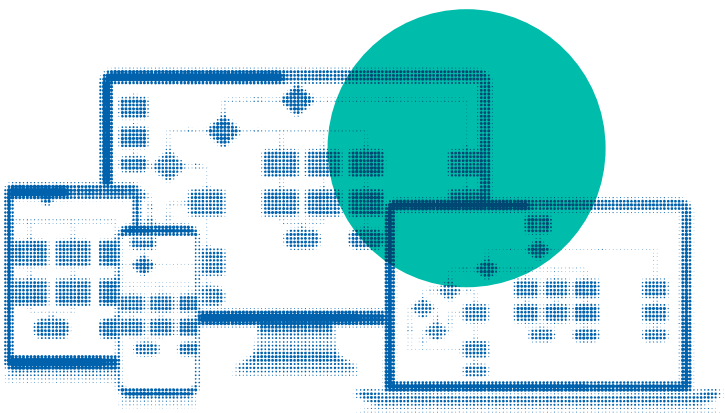
Brand Security: Brand security and Phishing often overlap, but brand security is a broader term designed to encompass the misuse of a corporate or organizational brand. This can include phishing emails and spoof websites, misleading social media ads, fake app listings, digital messages, fake employee profiles or accounts and misrepresentation forums.

Exploitable Data: Exploitable data relates to vulnerabilities and holes in existing enterprise defenses. Unlike Data Leakage which focuses on the data itself, Exploitable Data relates more closely to exposure and vulnerability gaps that could enable a bad actor to access or steal sensitive information. Threat intelligence examples of this could include chatter on stolen credentials, unpatched systems, expired signatures, unencrypted data, and network vulnerabilities.

VIP: This catch-all category refers specifically to threats related to key figures in an organization that are, for obvious reasons, prime targets for a campaign. They could be high profile individuals, employees with access to sensitive data or employee groups at higher risk of targeting due to some other factor.



Type	What	Where	When	IntSight Approach
Attack Identification	•Announced intention •Domain specific malware •Target lists •Stolen goods •Insider recruitment •Scam pages •Accounts for sale	•Forums •Malware repositories •Black markets •Paste sites •IM platforms •IRC chats	All stages	We use avatars to contact the threat actor and try to either gain a sample of the data that is offered for sale or extract more information from them. Then we can understand where the data came from and try to understand the scope of the attack and the capabilities of the attacker.
Data Leakage	•Confidential information •Leaked credentials •Email	•Paste sites •Company website •Data breaches •Insider leaks	After initial compromise	Varies based on type of leak, but we will investigate source of leak, change passwords and encourage user awareness training and dark web monitoring.
Phishing	•Social engineering via original domains or domains similar to corporate domains •Employee or customer targeted emails	•Whois services •Spam report sites •Internal IT •Customer support •FBI	Initial recon, compromise, and privilege escalation	Block suspicious domains from communicating with email gateways and firewalls. Remediate domains by contacting registrar and host service provider. Encourage user awareness training.
Brand Security	•Social engineering via unauthorized use of brands aimed at high employees or customers •Fake account profiles •Fake corporate apps	•Social media •Fake spoof sites •App stores	Preparation stage (before the attack, very early stage or ongoing attack)	Warn employees not to communicate with suspicious profiles or download suspicious apps. Request fake apps be removed from app stores.
Exploitable Data	•Unpatched vulnerabilities •Open ports •Unencrypted login pages •Internal pages accessible via IP •Exposed	•Corp/partner sites •Vulnerable software •Bug bounty programs •Dark web forums •Zero days exploits	After initial compromise	Investigate vulnerable points or open ports, ensure all relevant software updates are downloaded and patched. Review and secure web and service login pages.
VIP	•Top executives •Board members, •R&D team members •Legal	•Email •Social media •Credential theft	All stages	Tighter IT controls and improved user awareness training.



Case Study - The IntSight Process

Having detailed how IntSights gathers and classifies threat intelligence, let's step back and take a look at how this all comes together to make a meaningful impact on an organization's security by examining how a leading North American retailer used threat intelligence gathered by IntSights' to clamp down on gift card fraud.

At the time of this attack, hackers had focused in on gift card theft due to their lower profile and less stringent security oversight when compared to credit cards. They had been racking up large financial gains as consumers, retailers and providers had not fully awoken to the risks involved or losses being generated. While monitoring dark web chatter on behalf of this retailer, IntSights discovered that unknown to the company, their gift cards were being systematically produced and later sold on the black market.

Leveraging IntSights' platform, the retailers' security team was able to rapidly alert the company, and provide them valuable context to the incident - including attack identification, brand security and exploitable data examples - and suggest recommended remediation actions through the IntSights dashboard.

As a result, IntSights was able to raise the company's awareness to a growing and unknown source of fraud. The company was then able to use this information to justify the creation of an ongoing monitoring program, the implementation of better security measures in store gift cards and reduce the amount of black market activities using store gift cards.

IntSights Intelligence Dashboard visualizes and categorizes threats by type and severity from across the clear, deep and dark web.

Reimagining Security with Threat Intelligence

As you've seen, there is a great deal that can be gained by focusing on the human element of cybersecurity. Leveraging dark web threat intelligence can provide tips or context to a potential attack weeks or months before the use of technical indicators alone. As you look ahead and begin to apply the lessons learned in this paper, here are a few closing tips to remember:

Threat intelligence is more than IOCs: While many organizations focus on technical indicators, there is great value to be gained from qualitative and non-technical indicators of attack. Take a moment to step back and make sure you are considering how all forms of intelligence can advance your goals.

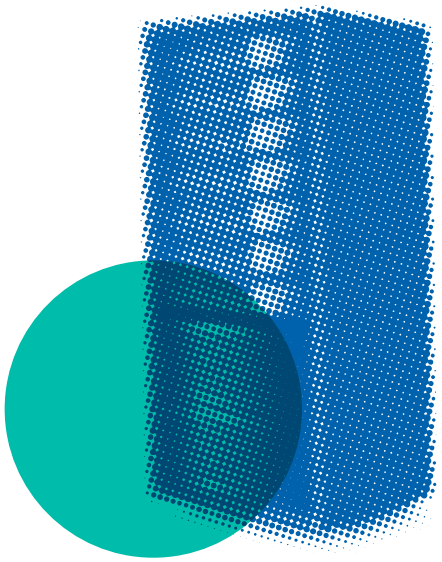
Get clarity on the big three – What, When, and Where: Every decision made related to sourcing or responding to threat intelligence should tie back to the answers gained from these questions. Being unclear or not fully understanding the answers to these questions can lead to gathering the wrong information or responding to the wrong threats.

Know what is actionable to you: There are many forms of threat intelligence and some will be more valuable to you than others. Use the big three questions to help focus on gathering only the intelligence and data types that are actionable to you.

Classify, then analyze: Having a solid classification process is critical to deciphering threat intelligence. Attempting to analyze raw data without context is a slow and painful process.

Make sure you have the right tools: Before jumping head first into the world of threat hunting, make sure that you and your team are equipped for success. Enterprise threat intelligence and mitigation platforms such as IntSight's can help by automating much of the gathering and analysis of threat intelligence and even aid in remediation to dramatically shorten your time to value. If you decide to walk alone on the dark web - don't forget to take basic precautions to ensure your operational safety - use VPN proxies, operate inside VMs, and develop unique non-identifiable avatars. No amount of intelligence is worth compromising your organization's operational security.

This article is contributed by IntSights



Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

IND/TBS/MAY-DEC 2020