Navigating Illicit Online Communities:

How Actionable Intelligence Helps Agencies Combat Cybercrime

MARKET TRENDS REPORT

govloop FLASHPOINT

Introduction

The internet consists of more than just searchable content. Search engines such as Google and Bing merely skim the surface of the internet and index what they find. The content that remains unindexed is part of the deep web, and further into the layers of the internet is the dark web, which consists of intentionally concealed content. In these hidden spaces, illicit communities flourish.

Today, cybercriminals are exploiting government data and personally identifiable information, and using that information across these threat-actor communities to engage in fraudulent and illegal activities — putting agencies at serious risk.

Agencies need to gather intelligence on these communities, which are havens for fraud, financially motivated cybercrime and money laundering, but it is difficult and dangerous to gather information on cybercriminals and others in these environments. Governments don't have the necessary tools, resources and capabilities to maneuver in these communities or to use their findings to proactively defend against cyberattacks.

The thin guise of anonymity in these spaces can sometimes allow law enforcement, military and intelligence personnel to conduct surveillance activities, identify malicious actors and undertake other operations to further protect national security. But without the necessary expertise and technology to automate secure and persistent data gathering within the far reaches of the internet, government agencies attempting to gather such information can actually create substantial risks for their employees.

So, how can agencies that need to penetrate these communities for cybersecurity move forward?

GovLoop partnered with Flashpoint, a leader in threat intelligence and an expert in accessing these illicit communities, to explore the capabilities open to agencies that are looking to gather intelligence to properly respond to threats.

In this report, we delve into the challenges and solutions agencies face in threat-actor communities. We also gain insights from Brian Brown, Vice President of Business Development at Flashpoint, about agencies partnering with the private sector to better understand illicit communities and respond to rising threats.

BY THE NUMBERS

5%

of the internet is about how much regular users see. This is the surface web.

Source: Congressional Research Service

550 billion

individual documents are housed in the deep web, as compared to the 1 billion contained within the surface web.

Source: The Journal of Electronic Publishing

"There are a number of areas in which the study and use of the Dark Web may provide benefits. This is true not only for citizens and businesses seeking online privacy, but also for certain government sectors — namely the law enforcement, military, and intelligence communities."

Source: Congressional Research Service

1.685 billion

websites exist on the surface web as of May 2019, according to Internet Live Stats. The deep web is an estimated 400 to 500 times larger than the surface web.

Source: The Journal of Electronic Publishing

$1.2 billion

is how much one illicit community was valued at before the FBI seized it in October 2013. The Justice Department obtained $48 million from the sale of 144,336 Bitcoins found in the computer of the community's founder.

Source: Justice Department, U.S. Attorney's Office, Southern District of New York

$500,000

is generated per day in the dark web's illicit marketplaces.

Source: Carnegie Mellon University

THE CHALLENGE
Exploitation of Government Data and Systems

Illicit communities pose significant risks to federal agencies and are known to support activities that directly undermine or interfere with government actions. These communities support fraud, cybercrime for financial gain, money laundering and other illegal activities that threaten national security.

Government agencies should work to gather intelligence to respond proactively to the communities' activities. But obtaining information on cybercriminals and others in such communities to prevent or anticipate attacks is challenging. Agencies can find themselves charting unfamiliar territory if they lack the expertise and technology to automate secure and persistent data gathering within these communities.

It can also be difficult for civilian agencies to get permission to build the infrastructure and manage the intelligence operations process that comes with doing this kind of work. Among the issues agencies must consider are the regulations or policies that govern how they go about gathering intelligence on illicit communities.

"Some of our best employees have come out of the government, and they're focused on these online communities from a different perspective," Brown said. "But in order to gain intelligence on illicit communities you have to really go through some very strict controls that the government overlays on top of their department and agencies."

Walking through those steps requires time and effort, and the challenge is finding a way to easily navigate within those illicit community spaces as a governmental entity.

Another challenge is building a staff with the correct perspectives to navigate illicit communities. A team with a wide view of these communities, with access to the right resources and with an expansive skillset to understand these groups, is a lot to ask from a specific department or agency. Although the Homeland Security Department (DHS) centralizes that responsibility, it has the added task of defending the entire .gov domain.

THE SOLUTION
Combat Illicit Threat Actors With Intelligence

With all that takes place in illicit communities, agencies without visibility into them face heightened risk. But as we've noted, access to information on cybercriminals and other threat actors in these communities is difficult and dangerous to obtain.

Without the necessary expertise and technology to automate secure and persistent data-gathering , agencies attempting to gather such information will require a significant investment of time and resources, and they'll risk exposing government professionals.

A better approach is risk intelligence accessed and analyzed by experts in penetrating these communities. This provides relevant context to organizations that typically lack the benefits of intelligence derived from illicit communities. Plus, using intelligence to respond to illicit activity will enable agencies to identify trends, and this level of intelligence empowers agencies to better investigate and defend against a variety of threats.

The recent arrest of a white supremacist in Pennsylvania who made dozens of online threats to minorities on the deep and dark web is an example of the efficiency of this approach. Flashpoint's intelligence and expertise gathering data from illicit communities was critical to the discovery the suspect's online presence and true identity, and ultimately brought the severity of the threat to law enforcement's attention.

To bridge the gap between the information needed to navigate an illicit community and the information

agencies have access to as outsiders of that community, agencies should tap into the private sector's capabilities.

The key, according to Brown, is establishing communication about the requirements to gather intelligence on these communities, both now and in the future.

All of the pieces of a puzzle are important when agencies are trying to identify the risks to their organizations by looking at things that have happened or could happen, and then putting the right controls in place from staff, solutions and policy perspectives.

Flashpoint's ability to collect critical data on adversaries from surface web sources such as blogs, chat services platforms, and message boards, as well as illicit underground communities makes it a trusted partner. As that partner, Flashpoint supports federal and civilian agencies with finished intelligence, cyber observables, and technical indicators to help them better understand their risks and the intent of threat actors while also bolstering their defenses.

BEST PRACTICES

Effectively Using Intelligence About Illicit Communities

1. Evaluate the issues that you hope to address

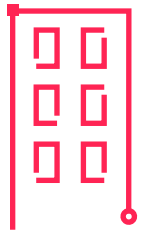
Illicit communities are expansive and difficult to navigate. To maximize efficiency and minimize unwanted costs, the needs of your agency should come first. Identify and evaluate what you want to solve before you pour time and resources into gathering intelligence around it. Then, you can build on acquiring capabilities to expand on your targeted interest.

2. Be flexible and able to analyze new datasets and problem requirements

Intelligence is in high demand, but with high demand comes high requirements. Flexibility is key to making sure that new intelligence can be analyzed well and used to respond proactively to new incidents or counter current threats.

3. Collaborate with other agencies on solutions

Communication is key to countering coordinated illicit activity. Agencies should find a space, such as the Flashpoint collaboration community, in which they can work together on similar issues or common problems. Collaborating to build on previous solutions could result in innovation and growth of operations and procedures across agencies to combat illicit activity.



4. Partner with private industry to get a holistic overview of methods to gather intelligence

Partnering with the private sector can greatly widen the scope of capabilities that agencies have to gather intelligence and learn more about illicit actors. Agencies should understand the abilities of the company they're partnering with. That's why Flashpoint ensures that teams comprise the right people to fulfill the requirements or policies of the department or agency.

USE CASE
Fighting Fraud and Supply-Chain Risks

As long as stolen data is in demand, there will always be criminals ready to supply and satisfy that demand. Flashpoint experts have seen how this demand has hatched all kinds of fraud schemes among illicit online communities.

Fraudsters trade illegal goods and take advantage of anonymization. When a new technique is developed or proves especially effective, threat actors talk about and share details among themselves. Having insights into these conversations is critical.

In one instance, Flashpoint analysts monitoring Locky ransomware uncovered a spam campaign during the 2016 holiday season. Locky, which was distributed via phishing emails disguised as payment invoices, was previously linked to infections causing massive economic and reputation damage at numerous organizations. Flashpoint responded immediately by notifying potential victims in the public sector of the ongoing campaign and provided relevant indicators of compromise, including samples of the text of a phishing email, offering organizations the understanding they needed to appropriately bolster security measures, implement appropriate user-access controls, and educate employees on phishing awareness.

Governments need access to this relevant data, and Flashpoint can provide it. For example, illicit communities have discussed identifying and then executing fraud against the Internal Revenue Service. These communities have ranged from standard criminal groups to highly sophisticated cybercriminal communities. Organizations without visibility into these closed-access regions of the internet face heightened risk. This is why Flashpoint offers threat intelligence, or the right data at the right time with the right context, to help agencies understand and mitigate risks.

Fraud isn't the only issue agencies must defend against. The public-sector supply chain and current procurement standards invite complexity and create a potentially vast, exploitable attack surface. The reason is government's software and hardware supply chains are complex and globally sourced entanglements of code and components from third-party manufacturers and service providers.

Any comprehensive evaluation of vendors supplying the public sector should include a discussion and audit of each supplier, plus intelligence related to known adversaries, threats and vulnerabilities to the supply chain.

HOW FLASHPOINT HELPS

The Flashpoint Intelligence Platform provides users with an archive of finished intelligence reports — data from illicit forums, marketplaces, chat services, blogs, paste sites, technical data, card shops and vulnerabilities — in a single, finished intelligence experience. The platform scales Flashpoint's internal team of specialized, multilingual intelligence analysts.

Whether users are intelligence experts or new to business risk intelligence, Flashpoint's platform and services deliver relevant intelligence that empowers them to make more informed decisions and to mitigate risk in any part of their organizations.

"Everything that we do at Flashpoint is all in conjunction with the normal terms of service, and we interact in these spaces the way that the actors would interact," Brown said. "We are able to very, very quickly bring that unique perspective, a perspective that is not only steeped in what civilian agencies care about, but also what global enterprises care about."

Read more at: www.flashpoint-intel.com

Conclusion

Solutions that dive beneath the surface of the web are often difficult to obtain because of the nature of the communities that they involve. However, acquiring the right services to counter threats is necessary for a robust cyber strategy.

Ultimately, efforts to gather intelligence on illicit communities leads to better decisions across agencies. If your agency wants to prioritize understanding and gaining insight into illicit communities, partnering with experts might be the answer. This could allow for a holistic picture based on reliable intelligence and help your agency anticipate or identify threats housed in illicit spaces.

ABOUT FLASHPOINT

Flashpoint delivers Business Risk Intelligence (BRI) that empowers organizations worldwide to combat threats and adversaries. Fueled by a combination of sophisticated technology, advanced data collections, and human-powered analysis, Flashpoint tailors its offerings to customer requirements. The result is meaningful intelligence that enables large enterprises and the public sector to bolster cybersecurity, confront fraud, combat insider threats, enhance physical security, and address vendor risk and supply chain integrity.

Learn more at www.flashpoint-intel.com.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop