SEARCHLIGHT. CYBER

PROFILING A DARK WEB CRIMINAL

A USE CASE FOR GATHERING INTELLIGENCE ON A DARK WEB ALIAS

INTRODUCTION

The main reason that criminals use the dark web is for the anonymity that it provides. Dark web networks such as The Onion Router (Tor) mask where traffic is coming from, so that a user can not be identified based on their IP address.

The most sophisticated criminals work hard to maintain their operational security (OPSEC) on the dark web, taking care not to share any information that might lead to their identification by law enforcement or cybersecurity professionals. Of course, it is hard to avoid mistakes over time, and there are countless examples of criminals being unmasked by slip ups such as the use of email addresses or usernames that match clear web accounts (see our Suspect Identification[1] use case for more information on how criminals can be identified).

However, even in the case where a criminal's OPSEC is so good that they can't yet be unmasked, there is still a great deal of value that can be unlocked in gathering intelligence on their online persona.

WHILE THE DARK WEB MAY MASK A THREAT ACTOR'S IDENTITY, IT ALSO PROVIDES A GREAT DEAL OF INTELLIGENCE ON THEIR ACTIVITIES THAT CAN BE USED TO INFORM CYBERSECURITY DEFENSES AND ULTIMATELY PREVENT ATTACKS.

In the area of cybersecurity in particular, a cybercriminal's real name is almost certainly of less value to a defender than a clear understanding of details such as their favored tactics, techniques, and procedures, their associations with other cybercriminals, and their role in the cybercriminal ecosystem. While the dark web may mask a threat actor's identity, it also provides a great deal of intelligence on their activities that can be used to inform cybersecurity defenses and ultimately prevent attacks.

To demonstrate how this can be achieved, we have taken the example of a real dark web persona that goes by the alias "carnaval" to show how intelligence and cybersecurity professionals can build a profile using dark web intelligence.

[1] https://slcyber.io/whitepapers-reports/suspect-identification-gathering-evidence-from-the-dark-web/

A CYBERCRIMINAL OF INTEREST

To demonstrate how dark web intelligence can be used to build a profile of a cybercriminal, we have taken the real life example of “carnaval”, an actor we regularly observe interacting with Initial Access Broker posts on dark web forums.

This activity makes carnaval a “person of interest” because Initial Access Brokers are a type of cybercriminal that sell vulnerabilities in an organization onto other threat actors to exploit. They play a critical role in the cybercriminal ecosystem, where increasingly actors with specific skills own their own area of the attack “supply chain”. For example, we regularly observe cybercriminals involved with ransomware groups purchasing vulnerabilities from Initial Access Brokers, to conduct their attacks.

This activity usually takes place on dark web forums and often in the form of a rudimentary auction - with the Initial Access Broker listing a “start” price, “step” increments of bidding, and a “blitz” price to buy the access outright.

We have observed carnaval “bidding” on these posts, which indicates that they could be an active cybercriminal. Indeed, carnaval was recently identified by cybersecurity researchers[2] as a possible affiliate of the ransomware group LockBit.

Now we have identified our individual of interest, what can we learn about them using dark web intelligence?

[2] https://www.trendmicro.com/en_gb/research/24/d/operation-cronos-aftermath.html

PROFILING A THREAT ACTOR

When assessing a cybercriminal, typically we are trying to understand the following things:

THEIR CAPABILITIES

Establishing how skilled they are at hacking, the resources they have at their disposal, and their previous experience in conducting attacks, can help a security team determine the level of genuine threat an actor poses. Remember - like all online forums - there is an element of bravado on hacking forums. Cybercriminals are not above making false claims and overstating their ability, so this assessment is important for identifying which threat actors need to be monitored as a priority.

THEIR CREDIBILITY

Further assessment of the risk an actor poses can be undertaken based on their reputation within the cybercriminal community. For example, a cybercriminal with long-standing forum accounts, a lot of communication with other forum members, and generally positive interactions could be assessed to be more of a threat than an actor with no clear social "standing" in the hacking world. Many forums have ranking systems that can help security professionals to quickly establish an actor's credibility.

THEIR GOALS AND MOTIVES

While most cybercriminals operating on the dark web fall under the bracket of "financially motivated", there are nuances within that category. For example, we increasingly observe financially motivated attacks being targeted at organizations in nations that have an opposing political view. Goals also differ between cybercriminals, with some looking to launch the attack themselves while others (like Initial Access Brokers) hold a role in the cybercriminal supply chain.

IDENTIFYING CRITERIA

Capturing information such as emails, usernames, cryptocurrency addresses, and details such as Telegram account handles, Tox addresses, and PGP keys not only increases the likelihood of law enforcement unmasking the individual but can also help cybersecurity professionals to identify other accounts the actor has. Cybercriminals often operate across multiple sites, sometimes with different usernames. Linking these dark web profiles enables a more accurate assessment of the threat.

Understanding these key points will enable a security team to assess the level of threat an actor poses to an organization and - from there - make decisions around the best next steps. Ultimately, that is the aim of threat intelligence: to make the best possible decisions given the situation and information at hand.

PROFILING CARNAVAL

Our dark web intelligence platform has accumulated the following information on the cybercriminal known by the alias “carnaval”. This initial intelligence gets us some way to building a profile on carnaval, in line with the criteria outlined on **Page 3**. For example, even the actor’s presence on the XSS and Exploit forums is suggestive of a certain amount of credibility within the cybercriminal community. Their Tox account also helps us to create a link between different dark web sites, increasing the likelihood that it is the same individual operating in different forums.

ACTIVE SINCE

The actor carnaval appears to have initially started their activity on the hacking forum Exploit and then transitioned over to XSS, with no activity seen on Exploit since September 2023 (**Figure 1**). Exploit and XSS are infamous hacking forums that have been active for nearly two decades. Users of these forums tend to see themselves as more “professional” than cybercriminals in other, non-Russian hacking forums.

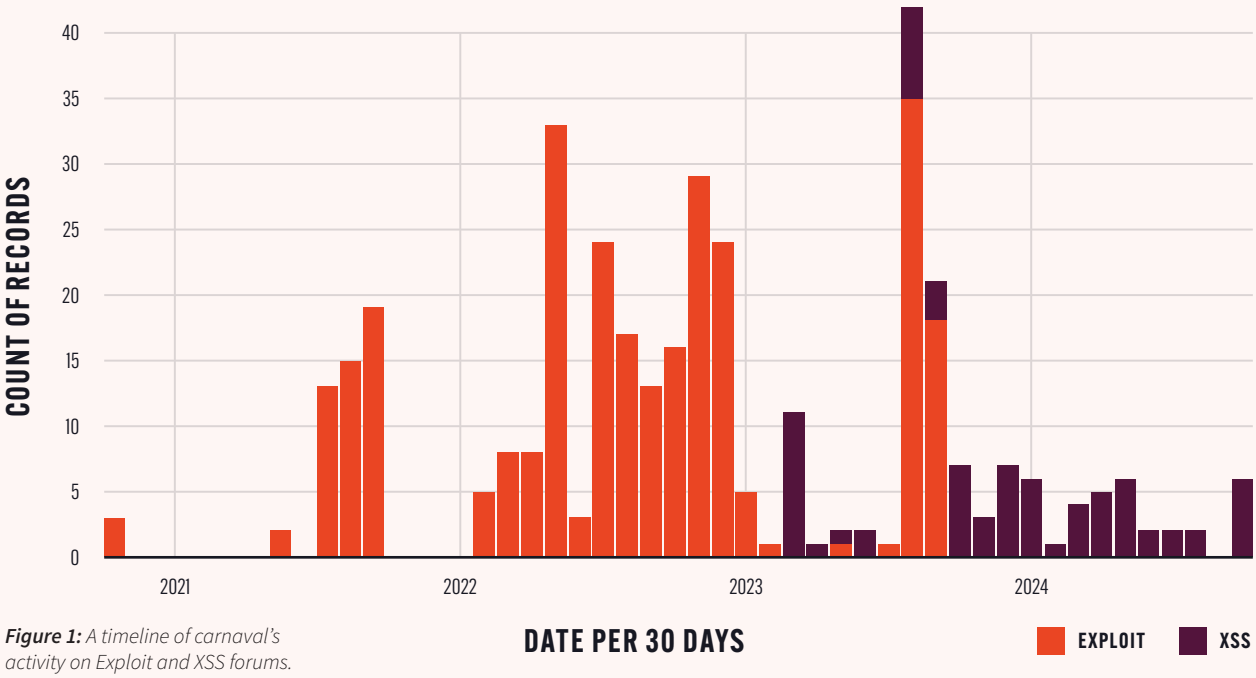

Figure 1: *A timeline of carnaval’s activity on Exploit and XSS forums.*

ACTIVE ON

As well as Exploit and XSS, we assess with low confidence that carnaval also has a presence on another Russian hacking forum, AntiChat. There are only two posts attributed to carnaval on this site, which makes it difficult to come to a reliable judgment, although there is a shared identifier that suggests it is the same actor (see “Identifiers” below).

IDENTIFIERS

The same TOX address was used by the actor carnaval across their Exploit, XSS, and AntiChat accounts, suggesting that it is the same person on all three sites. TOX is a messaging service offering end-to-end encryption, which makes it a popular communication tool for cybercriminals.

LANGUAGES

More than two-thirds of carnaval’s posts are in Russian, which indicates that this is their first language. This is consistent with the use of Exploit, XSS, and AntiChat, which are all forums that primarily use the Russian language.

LEARNING FROM THREAT ACTOR CONVERSATIONS

Once cybersecurity professionals have established where the actor is active, far more intelligence can then be produced by reviewing the conversations carnaval has had on the dark web and actions that they have taken.

CUSTOMER OF INITIAL ACCESS BROKERS

Searching for "carnaval" and the auction terms discussed on **Page 2** in our dark web platform returns dozens of results for Initial Access Broker posts that carnaval has bid on. **Figure 2** is a typical example, where carnaval has paid the "blitz" price - i.e. bought the access outright - in an auction for remote desktop protocol (RDP) access related to an organization in the US.

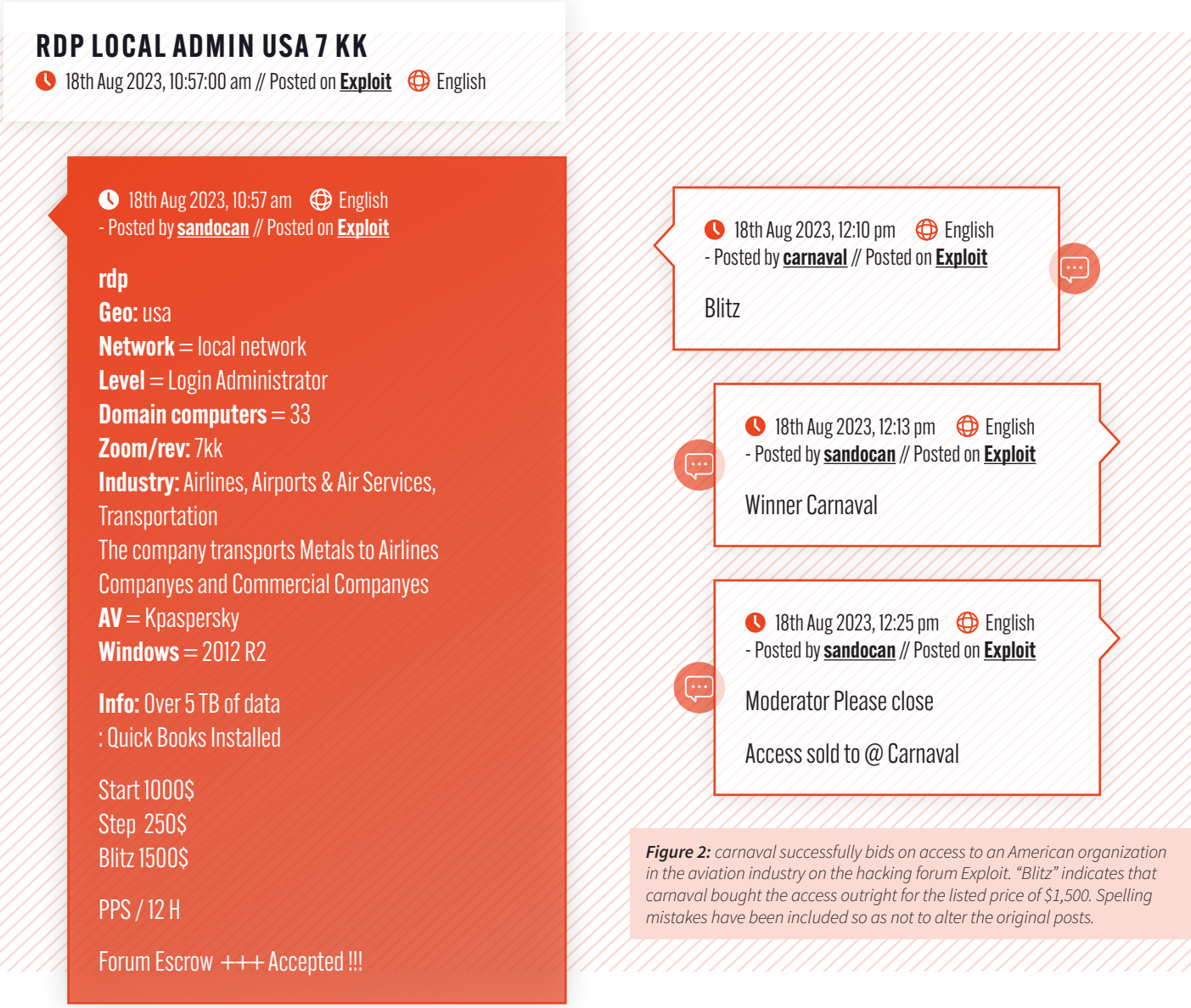

Figure 2: *carnaval successfully bids on access to an American organization in the aviation industry on the hacking forum Exploit. "Blitz" indicates that carnaval bought the access outright for the listed price of $1,500. Spelling mistakes have been included so as not to alter the original posts.*

By monitoring these posts, a security team can gather intelligence on the types of organizations that carnaval targets, the types of access the actor typically bids for, and exactly how much the actor is willing to pay for the access. These trends become particularly clear across multiple posts.

PROACTIVELY ADVERTISING FOR INITIAL ACCESS

A closer investigation of carnaval's forum activity shows that the actor does not just reactively bid for access but also actively advertises the fact that they are looking to buy access into certain organizations. These posts shed even more light on carnaval - including their victimology, the types of access they are interested in, and their reputation within the cybercriminal community.

Figure 3 is an example of such a post on the XSS hacking forum, with just some of the subsequent responses and comments from other forum users to demonstrate the intelligence that can be extracted by monitoring these posts.

I WILL BUY CORPORATE ACCESS

27th Feb 2023, 11:52:52 am // Posted on **XSS** Russian

27th Feb 2023, 11:52 am Originally posted in Russian - Posted by **carnaval** // Posted on **XSS**

Hello everyone!

I will purchase or take into work (50% to 50%) corporate access. I will consider any adequate GEO. I will consider purchasing with Local Admin, Domain User. Organizations without revenue, hospitals, critical infrastructure, where there is a danger to human life and health, do not offer. Revenue from $ 5kk. Cost from $ 500. There will never be payment in advance. Keep this in mind. Only after verification.

TOX: [redacted]

carnaval's original advert, posted in February 2023, establishes the criteria the actor is looking for in their victims. Interestingly, the actor claims that they are not interested in attacking hospitals, critical infrastructure or causing any "danger to human life".

This speaks to the nuances in "goals and motivations" we mentioned on **Page 3**. The indication here is that carnaval is a cybercriminal motivated by financial gain, not a desire for disruption.

Of course, carnaval's reticence to conduct attacks that could impact "human life" does not necessarily come from a place of altruism. Many financially motivated cybercriminals avoid these targets simply because of the perception that it will bring unwanted attention from law enforcement.

Figure 3: *A post from carnaval on the XSS forum in February 2023 titled "I will buy corporate access", followed by a selection of the responses. We have redacted the actor's TOX address.*

3rd Mar 2023, 05:35 am Originally posted in Russian
- Posted by **blessthefall** // Posted on **XSS**

I worked with a person at a neighboring site, I can only leave a positive review!

22nd Mar 2023, 09:23 am Originally posted in English
- Posted by **SGL** // Posted on **XSS**

Worked with him in the past on exploit.
Serious person.

30th Mar 2023, 00:28 am Originally posted in Russian
- Posted by **RocketRacoon** // Posted on **XSS**

Great buyer!

27th Apr 2023, 08:32 am Originally posted in Russian
- Posted by **amoralventures** // Posted on **XSS**

Everything is great! The man knows his business and doesn't mess around.

Several XSS users respond to the advert over the next month (in both English and Russian) claiming to have worked with carnaval before and leaving positive reviews. This strongly implies that carnaval is seen to have high credibility among their peers.

More can be learned about the actor's reputation by taking a broader look at their hacking forum profiles and interactions. On XSS, the actor has a +44 reputation score, as well as a recorded history of six successful deals, and a 0.1 BTC forum deposit (which is a down-payment that is forfeited if the actor commits a scam). This supports the hypothesis that the actor has a high level of credibility on the XSS forum.

However, carnaval's Exploit account, which they had been using until September 2023, is a murkier picture. On Exploit, carnaval had a +28 reputation and a 0.035575 BTC deposit but also has scamming reports against them.

In each of these disputes, carnaval is accused of indicating that they would like to buy access but then not paying the seller. The records show that carnaval settled each of these disputes, paying out the seller before receiving a harsher reprimand from the moderator of the forum. It is possible that a negative reputation for not paying for initial access drove carnaval to switch from the Exploit forum to XSS.

1st Dec 2023, 10:33 am Originally posted in Russian
- Posted by **carnaval** // Posted on **XSS**

We will buy expensive or take at % Local Admin, Domain User, Domain Admin. Only domain infrastructure.
Only USA, CA, Australia, New Zealand, EU.

20th Sep 2024, 08:54 pm Originally posted in Russian
- Posted by **carnaval** // Posted on **XSS**

We will buy expensive or take good access even with Sentinel at the discussed percentage - it doesn't matter. Only USA, Canada or greater Europe (Software agreements). We don't take anything else.

carnaval posts again several times on the same thread over the next year, often clarifying their interests. For example, in these posts the actor narrows down the geographies that they are interested in and that they are willing to buy access to organizations "even with Sentinel", which could be a reference to the cybersecurity products SentinelOne or Microsoft Sentinel.

Once again, this intelligence provides a clearer sense of the actor's "goals and motivations". While carnaval is primarily motivated by financial gain, their targets are clearly within geographies on the opposite geopolitical spectrum to Russia. This is most likely driven by the fact that Russian authorities are less likely to prosecute cybercriminals targeting organizations in these countries.

22nd Sep 2024, 02:11 am Originally posted in English - Posted by **Infernolord** // Posted on **XSS**

Are you interested in the rights and interests of Chinese companies? I have a lot of Chinese permissions

24th Sep 2024, 11:14 am Originally posted in English - Posted by **RocketRacoon** // Posted on **XSS**

not interested

True to their word, there does appear to be markets that carnaval is not interested in pursuing. In this exchange on the thread, the actor turns down access to an organization in China.

26th Oct 2024, 06:07 pm Originally posted in English - Posted by **Cr4** // Posted on **XSS**

We have access to a leading Moroccan car manufacture company.

Revenue last year 500m$+

1. Level: DA
2. How many hosts: Too many (heavy bloodhound)
3. Type of access: We have a proxy on the internal network (full access), we can get you RDP or Anydesk
4. AV: Windows Defender
5. Price: $10,000+

Some Initial Access Brokers post their adverts onto the thread, in the hope that carnaval will purchase them.

All of this detail from one hacking forum thread can enable an organization to build a profile that helps them determine if carnaval is a cybercriminal that they should be monitoring - for example, if they match the description of the Moroccan car manufacturing company posted at the end of the thread.

Just as importantly - in a world where resources are scarce and security teams have to make choices on prioritizing threats - it can also help organizations to rule out carnaval as a significant risk to them. For example, organizations in critical infrastructure or outside of western Europe and the US could de-prioritize carnaval as a threat.

SUMMARY

The small sample of dark web intelligence we have provided here demonstrates how a cybersecurity team can begin to build a profile of a cybercriminal they are concerned about. We now know of carnaval:

THEIR CAPABILITIES

carnaval's interaction with Initial Access Broker posts suggest that they are experienced in exploiting RDP access. This, combined with open source intelligence that they are associated with the ransomware group LockBit, indicates a potential point of ingress that organizations should be monitoring.

THEIR CREDIBILITY

carnaval clearly has an established reputation among the cybercriminal communities on the XSS and Exploit hacking forums (even if this is partly down to a bad track record of not paying for the access they have acquired) suggesting that the actor is an active threat.

THEIR GOALS AND MOTIVES

Organizations in the USA, Canada, Australia, and Europe are in the firing line of carnaval, unless they operate in the healthcare and critical infrastructure sectors. The actor is financially motivated and selects targets based on turnover, so should be a particular focus of organizations with a higher revenue.

IDENTIFYING CRITERIA

While carnaval has a high level of OPSEC, not exposing clear web information such as email addresses or accounts, their use of TOX has allowed us to confidently link their accounts across multiple forums, providing more information to build a comprehensive profile of the actor.

USING SEARCHLIGHT CYBER TO PROFILE DARK WEB CRIMINALS

Our dark web investigation platform gives analysts access to the most comprehensive dark web dataset on the market. It continuously captures data from the dark web and makes it easy to interrogate it in all the ways the dark web isn't, allowing cybersecurity professionals and law enforcement to gather intelligence and take actions against cybercriminal activity.

DARK WEB SEARCH

Search through more than 15 years of dark web data for intelligence on forums, marketplaces, hidden sites, communications, threat actors, illegal goods and more. Searchlight Cyber uses proprietary software to index more sites than any other solution on the market. Our data collection is continuously updated as new sites, posts, and profiles appear and this information is kept forever, even if the original item is deleted from the dark web.

DARK WEB PROFILES

Searchlight Cyber automatically builds profiles for dark web actors, allowing analysts to find associated profiles on other dark web sites, assess links to other groups, and monitor dark web conversations. Data points such as identifying criteria are automatically parsed by the platform, providing invaluable context on actors and allowing cybersecurity professionals and law enforcement to pivot on key artifacts.

CASE MANAGEMENT

Searchlight Cyber's case management system allows analysts to collate intelligence and useful information on a particular persona or group in files within the platform. Once a case has been created, it can be augmented with automated alerts that trigger whenever new intelligence comes to light. This allows cybersecurity professionals to continue with their day-to-day activity, safe in the knowledge that they will be aware if there is any update on a person of interest.

STEALTH BROWSER

Safely access dark web sites through a secure virtual browser hosted within the Searchlight Cyber platform. The Stealth Browser allows analysts and investigators to view content on the dark web networks Tor or I2P with one click, providing them with quick access to gather intelligence at the source. At the same time, it protects the user's machine from malware, allowing them to visit the dark web without putting themselves or their infrastructure at risk.

RANSOMWARE SEARCH AND INSIGHTS

The profiles of the administrators and members of ransomware groups are automatically collated in the Searchlight Cyber platform. Track and investigate the dark web activity of the most active ransomware groups through our continuously updated dashboard. Ransomware Search and Insights automatically collates intelligence on more than 60 ransomware groups' communications, members, and victims, arming security teams with the latest insights.

SEARCHLIGHT CYBER

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
200 Massachusetts
Avenue Northwest,
Washington, DC 20001
United States