LOOKINGGLASS

CASE STUDY

HOW A FEDERAL LAW ENFORCEMENT AGENCY TACKLES CYBER ATTRIBUTION

"We help organizations identify how a hacker got in, what vulnerability they exploited, and what mitigation needs to be put into place. But we also have to determine the real-life identity of that hacker and then prove beyond a reasonable doubt in a court of law that this person committed this crime…LookingGlass provides the data, in whatever format we need, that helps pinpoint and prioritize what and where we need to be looking to jumpstart our investigations. Without LookingGlass, some of our most effective operations would slow to a crawl or stop."

With a law enforcement mission, this federal agency finds and brings to justice national and international criminal enterprises that engage in activities such as money laundering, narcotics smuggling, human trafficking, illegal arms dealing, intellectual property theft, etc. Within this agency are teams that investigate cyber-enabled crimes. "Team NXS," which became a formal group in 2019, focuses on cyber crimes that involve unauthorized access, either to steal intellectual property, to exfiltrate sensitive, national security data, or to conduct other criminally motivated operations.

With such an extensive mission, Team NXS needed a cybersecurity partner that could help:

- identify indicators of compromise quickly and early to help prioritize cases and direct research efforts
- support local, national, and international investigations
- provide detailed technical data to support the difficult task of cyber attribution and to strengthen investigations with evidence that supported legal charges

This agency has been able to meet its mission objectives faster and with greater success by leveraging LookingGlass's actionable, tailored threat intelligence solution.

THE CHALLENGE: SORTING THROUGH THE BYTES FOR RELEVANT TIPS

Like many enterprises around the world, this federal agency grapples with finding and retaining skilled cybersecurity staff. To add to this challenge, the agency also has difficulty keeping their staff trained on evolving technologies and new tactics or techniques used by cyber criminals to evade investigators.

Where this agency differs from other enterprises, though, is their mission focus. Sitting at the intersection of law enforcement and cybersecurity adds a layer of complexity to the challenges facing the agency and Team NXS.

Many private enterprises do not have the resources to attribute a cyber attack to an individual but uncovering this is critical to Team NXS and their mission. For Team NXS, attribution – identifying the actor responsible for a cyber attack – is crucial to ensuring cyber criminals are held responsible for their crimes. Furthermore, any attribution needs to be grounded in clear technical detail and evidence that will stand up in a court of law.

Because Team NXS concentrates on cyber crimes that involve unauthorized access that results in intellectual property theft from U.S. companies, the exfiltration of national security information (e.g., hacking a defense contractor to steal planes for a military aircraft), or hacking financial entities to facilitate crime, it can often feel like there is both too much data and not enough. Team NXS needs to sort through troves of data and information to identify information that points to a cyber incident before they can begin researching and investigating. While the team has access to a variety of tools, several data feeds, and even information provided from other agencies, obtaining timely, actionable insights from the data can be challenging.

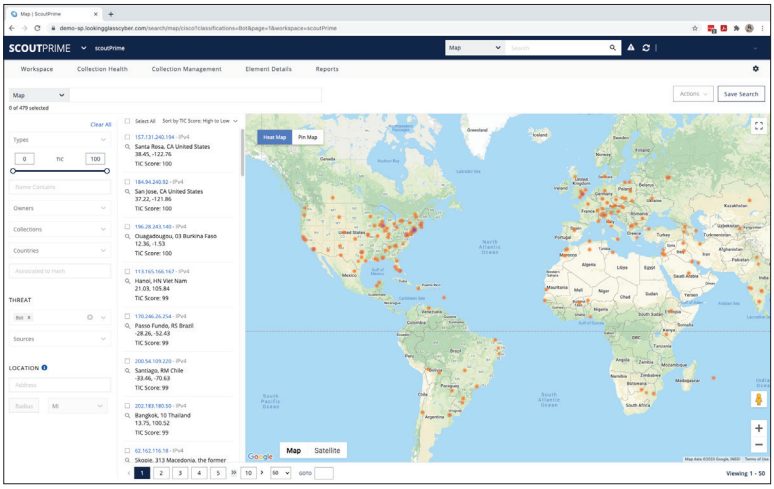
For example, Team NXS can get a tip from an agency or partner that they've seen activity on the dark web for access to a company's data or credentials, which indicates that either a breach has occurred or will occur in the near future. Team NXS begins its investigation with several potential paths to pursue, including engaging the malicious actor directly where possible. However, it is unlikely that said actor will simply state which organization they have breached even in direct interaction. Team NXS needs to identify the victim – to support detection, response and potentially recovery – and the malicious actor – along with the evidence that ties the malicious actor's digital persona to their real-life identity – in order to meet the agency's objectives. As with any criminal investigation, analysis of a plethora of information is required, but in the case of Team NXS, there is also significant digital information that must be sorted through, reviewed, and assessed and analyzed and mapped to the real world.

THE SOLUTION: CRACKING CASES WITH ACTIONABLE THREAT INTELLIGENCE

In 2019, Team NXS heard about LookingGlass's solutions from a federal agency partner that is also focused on cybersecurity incidents.

LookingGlass offers contextualized, correlated threat intelligence overlaid upon a dynamic map of the world's internet infrastructure to provide an analysis and visualization of logical (IP routing), physical (geo-location) and transit medium (fiber, satellite) information. The flexibility of LookingGlass's platform means organizations can use it as a foundational platform to serve a full spectrum of cybersecurity missions and operations.

Some users begin with LookingGlass intelligence because it surfaces interesting indicators and helps prioritize investigations or analysis. Other clients leverage LookingGlass to operationalize threat intelligence—providing risk mitigation, asset tracking, and situational awareness by giving them an adversary's view of their network infrastructure from the public internet. And still other users turn to LookingGlass after an incident occurs to provide more context, explore if a vulnerability was part of the attack or incident, and validate various pieces of information from the incident.



Furthermore, LookingGlass clients have access to analysts with decades of experience in information security and intelligence gathering. Clients can turn to the LookingGlass analyst team with a single question or a full inquiry; leveraging LookingGlass tools, data feeds, and the largest repository of cyber threat intelligence and threat actor information in the world, including more than 20 years of data assembled from the surface, deep, and dark web, LookingGlass analysts can source and provide unique intelligence.

MEETING MISSION OUTCOMES: BRINGING CYBER CRIMINALS TO JUSTICE

Initially, Team NXS used LookingGlass intelligence for incident response, specifically to help identify U.S.-based companies that may have been breached. In an early collaboration, Team NXS was investigating a potential data breach at a financial services company, but they were not sure which organization this was. The size of the sector meant a much larger swath of potential companies to contact in trying to identify the victim, which meant days wasted on outreach for identification and longer lead times before response and recovery efforts could begin.

Team NXS turned to LookingGlass for help identifying the victim. Within a matter of days, LookingGlass provided Team NXS with a full network footprint map of potential companies, that included DNS history and Shodan tags to identify vulnerable hosts. Additionally, LookingGlass analysts identified potential actors through research in underground forums and by pinpointing information in LookingGlass's proprietary cyber threat intelligence and actor repository. Team NXS was able to use this intelligence to help quickly identify the victim, reach out, and support incident response.

Supporting incident response activities, especially efforts to quickly identify a set of companies that could be victims of a cyber crime, continues to be a critical component of the collaboration between LookingGlass and Team NXS.

More recently, Team NXS turned to LookingGlass to help finetune its preventive efforts—to proactively identify cyber crime or fraud indicators and shutting down the digital avenues for malicious actors to conduct their attacks.

In particular, with COVID-19, malicious actors have increasingly used the pandemic to commit crimes. For Team NXS, this means stopping criminals from standing up fake charity websites to conduct fraudulent fundraising and fake medical supply websites to sell counterfeit medicines or "remedies" for COVID-19, among a host of other activities.

At the start of these operations, Team NXS spent significant time manually reviewing, copying, and pasting potential websites and newly registered domains from their initial source into a more usable format and tool that allowed the team to identify which sites to investigate first.

With LookingGlass, the team now receives this information in whatever format they need, enabling them to ingest it easily into their tools for analysis and prioritization. Ultimately, this has helped to increase Team NXS's productivity and reduce days of manual work in culling through tips to prioritize the most critical ones for further investigation.

The COVID-19 operations have been a massive success for Team NXS. In total, as of October 2020, **more than 65,000 domains have been sourced by LookingGlass** and analyzed by Team NXS in their efforts to identify cyber criminals and stem cyber crime during the pandemic. This has impacted **more than $18 million in fraudulent transactions and recovered funds and led to more than 180 criminal arrests.**

+18 Million
fraudulent transactions and recovered funds

+65,000
domains have been sourced by LookingGlass

+180
criminal arrests in October 2020

ABOUT LOOKINGGLASS

LookingGlass develops cybersecurity solutions that empower organizations to meet their missions with tailored, actionable threat intelligence. For more than a decade, the most advanced organizations in the world have trusted LookingGlass to help them protect financial systems, ensure telecommunications are cyber-resilient, and safeguard national security interests.

Rooted in operationalizing threat intelligence, LookingGlass solutions help reduce the time to detect and respond to incidents, enable cyber investigations, optimize threat hunt operations, and improve analyst productivity and efficiency. By linking the risks and vulnerabilities from an organization's external attack surface to customized threat actor models, LookingGlass provides a more accurate view of cyber risk and enables systematic definition and deployment of mitigations to defend against the threats that matter.

Find out how we can help your organization at **www.LookingGlassCyber.com**