CACI
EVER VIGILANT

ARTICLE

DARKBLUE INTELLIGENCE SUITE

Removing Risk

Investigating data on the dark web

CACI's DarkBlue Intelligence Suite provides secure and safe access to intelligence on the dark web

In February 2024, hackers released data about Russia's purchase of thousands of Iranian drones. The details were the stuff of a spy novella, including payments of literal tons of gold to shell companies, drone performance specs, bulk discounts, and even a brochure for the drone factory.

For intelligence officials, the data was a virtual treasure, but the dangers of retrieving it were very real. The information lived on the dark web, an unregulated and hidden part of the internet accessible only via special software, unique configurations, or authorizations.

"One major risk is malware. It's first and foremost, and probably even second and third," said CACI's Thomas Groendal of the potential risks to dark web investigators. "The presence of malware is endemic throughout leaked data sets. The data may also be illegal. It may be confidential. There could be all kinds of reasons that just grabbing that data and saving it to your machine is a terrible idea."

SAFELY FINDING THE RIGHT DATA ON THE DARK WEB

The DarkBlue® Intelligence Suite was developed to help revolutionize open-source intelligence (OSINT), or the gathering and analyzing of openly available data to produce actionable information.

For an OSINT analyst, the dark web as a resource can be as dangerous as it is invaluable. In addition to malware and illegal images, there is the potential that a target may discover the identity of the investigator or their organization via IP or browser information, putting their mission or themselves at risk.

Want to learn more about the DarkBlue Intelligence Suite?

Request a free trial at caci.com/darkblue/trial

In addition, dark web data is usually unstructured and complex in form. For example, files from the same leak might be a mix of CSVs, CAD files, 90-page image-laden PDFs, spreadsheets, and more.

"The lack of interoperability between different types of data just makes it harder and harder to have an algorithm go out and find your insights and clues for you," Groendal said. "Trying to navigate that kind of data is just messy and laborious, so DarkBlue was built to handle that problem. We have a giant collection of hay, and we differentiate ourselves as the magnet that helps pull the needles up."

DarkBlue is a SaaS platform that provides analysts with the contextual clues that unlock de-anonymization of bad actors, such as uncovering identities behind bad actor monikers and the ability to collect valuable data found in the live environment that makes it easier to spot connections and patterns. The platform also provides access to the data without presenting harmful or illegal images from the dark web. Via its intuitive interface and native search capabilities, OSINT analysts can safely navigate and fully exploit open, deep, and dark web data.

DarkBlue works in conjunction with DarkPursuit®, a software solution within the suite that eliminates exposure to malware or identification by targets by providing users with a browser-based single session virtual machine. This allows investigators, analysts, and operators to anonymously access information from TOR, I2P, and Hyphanet sites where they can visit dark web marketplaces or collect content and technical selectors in one click for further exploitation in DarkBlue.

Users also benefit from CACI's Technical Collections Team, which unearths, sorts, and provides carefully curated mission-focused data. For example, the team has downloaded the entire data set of a recent Russian drone leak and has made it available for simplified search and viewing within the DarkBlue suite.

VIRTUAL SOFTWARE THAT MAKES A REAL DIFFERENCE

It is difficult to talk about the dark web without acknowledging it as place where the worst of the worst tend to operate. That's why CACI has partnered with human rights organizations such as the Anti-Human Trafficking Intelligence Initiative, the Innocent Lives Foundation, and The Asservo Project, and with other top technology companies such as AWS to ensure dark web investigators have secure and effective tools.

"The customers who are the most passionate about DarkBlue are those fighting child sexual abuse materials, fighting opioid trafficking, and other trafficking activities on the dark web," Groendal said. "We provide a very specific service to those people and for those mission sets. It's safety and de-anonymization of bad actors in a single solution."

Another growing user base of these solutions are special operations forces (SOF). Virtual access to the dark web allows them to prep for missions on a simpler and larger scale than in the past. For example, there traditionally may be only one machine available to a SOF user allowed to access the dark web, but a dozen people on a team. That's not a problem with a virtual machine because they can just boot up another terminal.

ABOUT CACI

At CACI International Inc (NYSE: CACI), our 24,000 talented and dynamic employees are ever vigilant in delivering distinctive expertise and differentiated technology to meet our customers' greatest challenges in national security and government modernization. We are a company of good character, relentless innovation, and long-standing excellence. Our culture drives our success and earns us recognition as a Fortune World's Most Admired Company. CACI is a member of the Fortune 1000 Largest Companies, the Russell 1000 Index, and the S&P MidCap 400 Index. For more information, visit us at caci.com.