CASE STUDY

STATE GOVERNMENT DEPARTMENT IN THE UNITED STATES

LAW ENFORCEMENT

CHALLENGES

- RESOURCE-HEAVY, MANUAL INVESTIGATIONS
- NO WAY TO SAFELY ACCESS TOR
- VISIBILITY OF DARK WEB MARKETS AND SITES

SOLUTION

DARK WEB INVESTIGATION PLATFORM

> Increasingly other teams are coming to us for our ability and expertise in conducting dark web investigations. In those situations we can tell them that we have a tool that could help and work in collaboration with them to overcome their challenges.

LIEUTENANT
US STATE GOVERNMENT DEPARTMENT

DARK WEB CRIME BECOMES HIGH PRIORITY FOR CYBER INVESTIGATION UNIT

A Cyber Investigation Unit looked to procure a dark web investigation tool following a directive from the chain of command to increase its capabilities for tackling crime originating on the dark web. The Department was already actively investigating on the dark web using human intelligence officers to gain access to dark web marketplaces and forums and gather evidence. However, this approach was very manual and resource intensive, which created challenges in undertaking multiple investigations on the dark web at scale. Additionally, if a post was deleted from the dark web before the Cyber Investigation Unit were able to capture the evidence, they had no way to collect the archived data from the criminal sources.

The Cyber Investigation Unit had a wide remit for supporting state law enforcement across a broad range of cybercrime cases including online fraud, illicit cryptocurrency use, child protection investigations, drug and human trafficking. This meant they were looking for a solution that would give it a holistic view of dark web crime, enable it to identify specific crimes relevant to the state, and ultimately simplify dark web investigations.

A Lieutenant from the department explained: “We have an objective set by command to pursue more investigations on the dark web to ensure that there is no safe haven for cybercriminality within our jurisdiction. We knew from our own experience that dark web investigations are complicated and that we required a more sophisticated tool for gathering intelligence from the dark web.”

UNCOVERING CRIMINALITY ON THE DARK WEB

With Searchlight Cyber, the Cyber Investigation Unit is now able to interrogate more than 15 years of dark web data that has been collected and archived in the platform and is continuously updated as new activity takes place on dark web forums, marketplaces, and sites. This provides the Unit with a far greater overview of the dark web than it would have ever been able to achieve with its human sources and also better tools for searching and querying data, allowing it to more easily identify crimes and suspects in the state.

The successful use of Searchlight has even seen other departments approach the Cyber Investigation Unit for support when their investigations stray into the realms of the dark web. The tool has been especially helpful when searching for information on a suspect, such as known email or cryptocurrency addresses, which can help to identify more accounts and begin to build a body of evidence against criminals.

The Lieutenant elaborated: "Increasingly other teams are coming to us for our ability and expertise in conducting dark web investigations. In those situations we can tell them that we have a tool that could help and work in collaboration with them to overcome their challenges."

> "In the course of our investigations we have to access the dark web directly, in order to gather evidence or to understand the context behind a post. Before using Searchlight this was a complex process that required us to take extensive measures to do it in a way that was safe for our officers and infrastructure.

SAFELY BRINGING DARK WEB CRIMINALS TO JUSTICE

According to the Cyber Investigation Unit, the most valuable feature of Searchlight for them is the "Stealth Browser". This is a virtual machine that is spun up within the Searchlight platform in a sandboxed environment, giving investigators safe and instant access to a dark web site.

The state department had previously been accessing the dark web for investigations using Tails OS, which had been loaded onto a USB. Accessing the dark web this way was complicated for investigators and still contained some risk of downloading malware onto devices or investigators being identified by dark web criminals. By comparison, Stealth Browser allows the Unit's investigators to access the dark web quicker and with the reassurance that their infrastructure is protected.

The Lieutenant explained: "Sometimes in the course of our investigations we have to access the dark web directly, in order to gather evidence or to understand the context behind a post. Before using Searchlight this was a complex process that required us to take extensive measures to do it in a way that was safe for our officers and infrastructure. The ability to quickly do this via Searchlight using the Stealth Browser is a huge benefit both in terms of resources and peace of mind."

SEARCHLIGHT. CYBER

CONTACT US SALES@SLCYBER.IO // SLCYBER.IO

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
+44 (0)345 862 2925

USA HEADQUARTERS
44 Merrimac Street,
Newburyport, MA 01950
+1 (202) 684 7516