ACTING BAD FOR GOOD

IS IT POSSIBLE TO ACT LIKE A CYBERCRIMINAL FOR GOOD? RAMÓN VICENS, CTO AT CYBER THREAT INTELLIGENCE COMPANY BLUELIV DISCUSSES FIGHTING CRIME ON THE DARK WEB, THE INTERNET THAT HAS BEEN INTENTIONALLY CONCEALED

A common visualisation used for the Internet is an iceberg. The indexed surface web is less than 10 per cent of what is visible, but 90 per cent is non-indexed and known as the deep web. A small subset of the deep web includes hidden information and services: namley the Dark Web.

It's a common misconception that the Dark Web, or darknet, is purely for illicit activity. After its creation by the US military in the mid-90s, public users jumped at the concept, seeing the darknet as a platform to freely share information, software and services without fear of censorship.

The darknet has several advantages, including anonymous marketplaces, hidden forums, and a lack of state-based governance. The New York Times, for example, publishes on the darknet to reach readers whose governments might prohibit access, while TOR has reportedly been used by activists to undermine regimes in North Africa.

CYBERCRIME RESOURCE

This same freedom also enables criminal underground actors to operate in something approaching a safe space. The illegal information and services that can be found there are limited to specific internet users - those who gain access via TOR, I2P, invitation-only closed forums or Telegram groups, and of course, those with enough technical skill to force their way in.

Once in, you'll then find threat actors marketing their services and seeking recommendations and reviews in the same way as legitimate sellers. Their goods can be bundled together or sold as kits, lowering the barrier to entry for cybercriminals. For example, a less-sophisticated hacker can purchase their own stealer malware, perhaps including a user's manual or 24/7 customer support. From here they can deploy it to harvest credentials from a target then sell them on to a buyer in a different marketplace.

Given the darknet's structure, criminals often join forums to find the really juicy stuff. In many cases you have to contribute to these forums in order not to get banned. In others, you need to be invited or even be recommended through a trusted relationship to gain access. Here for example, illicit trade of very high-quality credentials is conducted through personal relationships and private messages, rather than sold openly.

KNOW YOUR ENEMY

The darknet is tough, but not impossible, to penetrate. There are public TOR indexers but these can't reach closed forums or other networks like I2P, Freenet or zeronet. There are also cybersecurity modules provided by threat intelligence companies, which crawl through the darknet, index the content and then provide a search engine to those who purchase their services. Forums meanwhile might need to be penetrated by deploying same method used by real-world criminals organisations - going in undercover and conducting espionage.

Using these methods is like putting a spy in the enemy's camp: listening in on conversations to prevent attacks before they happen, hunting for malware that can exploit unpatched vulnerabilities, discovering new TTPs (tactics, techniques and procedures) that could impact an organisation, or searching for compromised credentials and other confidential information.

Despite these tools, the question remains whether you can actually fight crime effectively on the darknet, or like so many real-world security forces, simply try to keep illicit activity from spilling over into the public domain.

The best way to fight cybercrime on the darknet is to operate in much the same way as the bad guys. As they build communities to exchange information and TTPs, so must we. In May, Europol launched a dedicated team to "find sustainable solutions and a common coordinated approach to respond to criminality on the dark web." Threat Intelligence involves actor tracking and sharing IOCs (indicators of compromise) and malware distribution information, all enabling private sector entities to collaborate better amongst themselves and with law enforcement: ultimately, we're on the same side. NC