International Law Enforcement Steps Up Battle Against 'Darknet' IP Theft

17/11/2016 BY BRUCE GAIN FOR INTELLECTUAL PROPERTY WATCH — LEAVE A COMMENT

Share this Story:

A recent multinational crackdown on illegal activity in the anonymous channels of the so-called Darknet resulting in multiple arrests around the world was intended to thwart rampant online intellectual property theft. But how much the dragnet will help to thwart cybercrime in the future remains in question.

"Operation Hyperion," consisting of law enforcement agencies from the United States, Australia, Canada, New Zealand, the United Kingdom, and the European Union's Europol, is what the group said is a first step in prosecuting those who break laws while hiding their identities with software such as Tor on the Darknet.

The law enforcement agencies' dragnet in October mainly involved counterfeit pharmaceuticals and data, but also led to arrests of perpetrators brokering chemical toxins, stolen credit card information, and even services used for murders for hire and money laundering.

"What this shows is that international law enforcement has the ability to stop the flow of illicit and counterfeit goods on the Darknet. The Darknet does provide levels of protection against bad people trying to do bad things, but there are law enforcement efforts underway to go after these people," Danielle Bennett, a spokesperson for the US Immigration and Customs Enforcement (ICE) branch of the Department of Homeland Security (DHS), told *Intellectual Property Watch*. "We are going also going behind the

websites that service as the forums but are also going after the buyers and sellers themselves, which represent an important piece of the trade."

ICE officials noted how Tor software can be used for legitimate purposes, such as masking communications among users in "authoritarian countries," but has also increasingly served as a way to anonymously purchase illegal goods and services over the Darknet.

However, the degree to which the law enforcement crackdown will mitigate further attacks and intellectual property cyber theft remains murky at best. By definition, the Darknet, and more specifically, the use of Tor software to protect those seeking to sell and distribute stolen intellectual property-related information covers a vast international underworld of illicit commerce that is difficult to quantify.

For attacks against firms or organisations that have intellectual property information that is digitized, such as proprietary computer code and algorithms, for example, attackers have become more sophisticated – and stealthier. It just takes one single successful penetration of a network among thousands that are often made per day against lucrative targets to find its way onto servers where information is stored. Attackers often are able to find backdoors to networks when a user opens a seemingly innocuous link on a website or a file sent as part of a phishing scheme that is in fact a malware program. The malware then proceeds to infiltrate the network, initially without the IT administrator's knowledge. Oftentimes, a backdoor hacker penetrates a network and proliferates behind the firewall for several months or even years before it is used to steal data.

In this way, intellectual property and identity theft is more difficult to track than stolen goods are, Mike Morris, CTO for root9B, told *Intellectual Property Watch*.

"[Cyber attacks and Darknet channels] are more difficult to track because sophisticated attackers have a vast network of redirection points before they ever launch an attack against their networks. They are able to tunnel their traffic through multiple hop points usually in a number of countries," Morris said. "After the theft of this data, they can use a separate set of hop points to access a large array of providers hosting Darknet sites. If they are sophisticated enough, this is a network of nearly endless hop points coupled with anonymous personalities and transactions."

Law enforcement bodies are also unable to prosecute data thieves who steal intellectual property-related data using the Darknet who are sponsored by the foreign governments in the countries in which they operate. Many of these virtually untouchable "threat actors" operate out of nations such as China, Russia and Taiwan, James Scott, co-founder and senior fellow of ICIT told *Intellectual Property Watch*.

"Without extradition agreements and the assistance of local law enforcement in those regions, the taskforce can do little more to arrest sellers than launch social engineering attacks to lure them out of the country," Scott said. "Without cooperation, the task force can still target some of the markets and forums where intellectual property is exchanged and it can arrest buyers in an attempt to deter sales – although neither effort would result in the same impact as arresting the sellers because in many cases, the seller is also the threat actor with the capability to steal the data in the first place."

Intellectual property laws can also vary significantly between countries. This is because some attackers are not necessarily committing intellectual property theft over the Darknet depending on the laws in place in their host countries. There can also be difficulties between law enforcement alliances between countries that have different intellectual property legislation.

"The fact this is said to be a multinational law enforcement effort causes a slight issue in terms of bringing justice for intellectual property theft. Particularly, the collaborated effort is made up of countries where there is a broad agreement about the illegality of a potentially criminal activity," Morris said. "In the countries that are said to be collaborating, it would seem that there are not widely agreed upon intellectual property laws. Making the determination of an intercepting entity to determine what is deemed to be IP and what is not."

Meanwhile, organisations are increasingly required to invest heavily in the services security firms offer for protection against attacks and remain ahead of the technology curve against data thieves operating on the Darknet. They often must be able to take action by relying on "bleeding-edge cybersecurity solutions," Scott said. These include artificial intelligence (AI) threat detection, user behavioural analytics (UBA), user activity monitoring (UAM), and data loss and spillage prevention (DLSP), Scott said.

Firms can also protect their intellectual property on the Darknet by investing in cybersecurity awareness and training and by teaching personnel to practice cyber-

hygiene best practices, Scott said. “Preventing social engineering attacks, such as spear-phishing, watering-hole attacks, and drive-by-downloads, and mitigating insider threat, will significantly reduce the likelihood of incidents that result in the loss of intellectual property,” Scott said. “Firms who are alerted to the exchange of their intellectual property or the exchange of access to their systems, user accounts, etcetera, on Deep Web forums or markets, should take immediate incident response actions that include contacting appropriate law enforcement, mitigating the impact of the loss, and preventing the source of the compromised data from filtrating other property.”

Bruce Gain may be reached at info@ip-watch.ch.

FILED UNDER: COPYRIGHT POLICY, ENGLISH, INFORMATION AND COMMUNICATIONS TECHNOLOGY/ BROADCASTING, IP POLICIES, LANGUAGE, NORTH AMERICA, OTHER INTERNATIONAL ORGS, PATENTS/DESIGNS/TRADE SECRETS, REGIONAL POLICY, SUBSCRIBERS, THEMES, TRADEMARKS/GEOGRAPHICAL INDICATIONS/DOMAINS, VENUES