Investigator Interview: Clearing the Path to Enforcement

Kelly Taaffe, **Senior Writer**
August 23, 2017

MarkMonitor's own investigative research specialist, Joshua Hopping, dives into a new generation of brand protection that equips firms with intelligence powerful enough to rip entire networks of cybercrime "out by their roots."

Hopping leverages an advanced form of "High-Value Targeting" (HVT), which zeroes in and takes down the most egregious infringers in bulk. While the methods he uses are newer to the brand protection industry — they are the "bread and butter" of this 13-year MarkMonitor veteran's work. And it's a critical component to taking action against a variety of cyber-criminals — from those peddling imposter baby formula to the fraudsters selling pirated entertainment and software, not to mention the shadowy actors behind the rising incidents of phishing and trademark infringement.

"We go deeper than just identifying that the abuse is happening," Hopping said. "We find out who's behind it."

To arrive there, he integrates captured data points such as phone numbers, emails, servers, names, images, and fragments of text as well as other sources such as shipments. With that analysis he is able to verify key links between varied marketplace listings and websites that might reveal operations masterminded by a common actor — indicating an HVT is involved behind the scenes. Clients are then provided with a complete report including visuals, analytics and charts to aid them in taking next steps. This actionable intelligence can be used to dismantle and/or disrupt the infringing actions of a network.

"It's not just the data," he said. "There's analysis and commentary behind it … You get that visual story of how things are connected."

This level of detail, he said, is more the industry exception than the norm. A typical enforcement strategy stops at mitigation efforts, such as sending out a cease and desist letter or delisting counterfeit goods. The comprehensive strategy enabled by MarkMonitor proved successful in 2016 when the company helped take down more than 230 websites during a coordinated operation for Europol known as "In Our Sites Seven" (IOS VII), a campaign that will take place again this year. MarkMonitor also assisted luxury brand Belstaff in targeting 3,000 websites selling fakes, some 800 of which were managed by one individual in China. Belstaff was later awarded $42 million in damages.

"What fascinates me is being able to make those connections, finding out who these people are," he said.

It's a well-known fact that criminals often hide behind an intermediary proxy service. Today, however, many fraudsters have amped up their strategies, using stolen identities to populate the Whois records of fraudulent domains — even using fictitious computer-generated names and addresses created by specialized software.

But for Hopping, one slip-up can be all it takes to blow their cover.

"He made one mistake on one address, and we connected it back," he said of one offender. "You see it and you think, 'I got 'em. This is where it's at.'"

Hopping, who is a member of the ASIS International, said he sees even more potential for a focus on the big fish in the near future. Patent-pending, MarkMonitor technology, for example, would use big data analytics and machine learning to further improve simultaneous detection of High-Value Targets across digital channels, from marketplaces and e-commerce to websites, social media and more. In fact, he's helping lead the initiative at MarkMonitor.

Learn more about MarkMonitor Investigative Services today by calling 800-745-9229 (U.S.) or +1-415-278-8479 (global).