Technology CyberSecurity

Security experts reveal secret to catching online scammers and counterfeiters

From fashion brands to illegal drugs - how Passive DNS could help stop crooks.

By Jason Murdock

November 4, 2016 15:40 GMT

The illicit sale of counterfeit goods and narcotics is not limited to the Dark Web and enterprising criminals are increasingly using the clear-web as a platform for their business. From fashion items to prescription drugs, cheap and easy to set-up websites only bolster this thriving industry.

To counter the problem, Andrew Lewman, chief revenue officer (CRO) at Farsight Security and Stevan Keraudy, chief technology officer (CTO) at CybelAngel, have designed a way of identifying and stopping these criminals using a technique based around real-time DNS analysis.

Taking to the stage at Black Hat Europe 2016, attended by **IBTimes UK**, the researchers demonstrated how Passive DNS – a collection of domain names and IP addresses – can be mixed with advanced "web crawling" to create a visualisation of sellers and counterfeiters.

"No-one really cares about DNS [Domain Name System] anymore unless you are into domain generation algorithms and botnets. But nearly every transaction starts with a DNS lookup," explained Lewman.

"You want to find an IP address or Google? It goes back and forth through DNS. If you can watch the initial [DNS] requests you can start to figure out where the first request came from and who has been looking up things over time."

The researcher said that there is a greater need for real-time analysis as the techniques used by cybercriminals are evolving rapidly.

"We have all seen spearphishing campaigns come and go in less than an hour," he said. "They looking for [then] shut the whole thing down."

The main challenge, the researchers explained to a packed room of attendees, is that criminals operating online now have a lot of resources at their disposal for very little effort. These sellers never create just one website – they create thousands.

"The old school way of targeting counterfeiters is to take down the websites one by one," Keraudy said. "It's very costly, taking a website required legal action and can cost a lot of time and money and it's very inefficient because counterfeiters are very well organised.

"They have thousands of websites waiting in line and as soon as you take one of them down they put another one back online within an hour. So it's a lost battle."

Optimising the takedown

In the talk, titled "Narcos, Counterfeiters, and Scammers: An Approach to Visualize Illegal Markets", Keraudy said the main aim of the tool is to "identify sellers and counterfeiters and how to put them into human readable visualisation in order to optimise the takedown efforts."

"We subscribe to Farsight's Passive DNS and we filter it using keywords," he explained. Using a selection of "brand specific" (Rolex, Channel, Dior) and "generic" search terms, the tool is able to analyse the trove of DNS records and locate potentially illegal activity, the researcher said.

Once the websites are identified – CybelAngel's web crawling technology comes into play by automatically scanning the homepage, links, pictures and body of the website "to collect as much information" and identify if the website is active.

It does "Whois" lookups, geolocation searches and "everything that can ID the website," Keraudy said, adding that Google Analytics IDs are also important. He noted: "Counterfeiters are businessmen and when you do business you want to do marketing, and when you do marketing, you use Google Analytics."

The crawlers can also automatically detect if there is a payment system on the website. The tool will "go through the system and put in some fake data" to follow the process up until the point of purchase. "We do not go through with the payment," Keraudy stressed.

The visualisation tools then make "clusters" of each website and – in a spider web fashion – creates a representation of each website and how they are linked. "We group the websites that belong to the same actor – the same organisation," he said. "You can target directly a whole organisation and not only just a website."

He added: "The clusters represent organisations that run thousands of websites selling illegal goods. Because we also have a traffic estimator we know which clusters to target first. We know which ones drive the most traffic so probably the most revenue. What you want to do is target the centre."

According to Lewman, who was previously a chief executive within the Tor Project, the technique can also prove to be useful for combating Dark Web sellers. He said it "works well" on these markets as "they are often run by the same criminal organisations that run the clear net markets."

The researchers said that – currently – the tool is being targeted towards enterprises over law enforcement. Keraudy told IBTimes UK: "We work with the corporates and they send it to their legal departments to work with law enforcement."

But that's not to say DNS analysis is limited to the business world. "Farsight does work with law enforcement and they use our database to look up past activity – to look up who owned an IP or who hosted what on an IP over time," Lewman acknowledged.