InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

11/2/2016
03:50 PM

Kelly Jackson Higgins
News
Connect Directly

Catching Online Scammers, Dealers & Drug Dealers With DNS

Researchers at Black Hat Europe this week will demonstrate a streamlined technique for spotting and identifying illicit narcotics, counterfeiters, and other scammer websites and operations.

Takedowns of malicious or fraudulent websites is a temporary fix for online fraud and crime, mainly because the bad guys then just put up another website domain they have waiting in the wings.

Researchers at Black Hat Europe in London tomorrow will demonstrate a new technique they developed that uses Domain Name Service (DNS) analysis to more efficiently spot illegal websites and online criminal operations. Andrew Lewman, chief revenue officer at Farsight Security, and Stevan Keraudy, CTO of CybelAngel, teamed up with an approach that detects, analyzes, and clusters illegal websites to better root out domain abuse.

"It's new research and taking a network science approach to identify online criminal networks," Lewman says.

The method employs visualization and analysis of DNS requests to identify common threads that tie sketchy websites together, according to the researchers, who will detail their findings in the "Narcos, Counterfeiters, and Scammers: An Approach to Visualize Illegal Markets" presentation at Black Hat. They plan to show how they filtered thousands of counterfeiting websites via DNS cache-miss requests, and then drilled down to several hundred domain names that were tied to one illicit organization.

"The main problem is criminals have a lot of resources. They don't just create one website, they create thousands of them at one time and only put one online" at a time, Keraudy says. "As soon as

they're spotted or taken down, they just look at one of those thousands of websites waiting in line and put one online. They are very organized," he says.

Thus the one-by-one website takedown approach by authorities is a time-consuming and ultimately, losing, battle.

Internet pioneer and DNS expert Paul Vixie has previously called for a "cooling-off period" for new Internet domain names to help thwart domain abuse. Vixie argues that there's no legitimate rationale for a new Internet domain name to go live less than a minute after it's registered. That pattern is often a red flag for malicious activity, an issue that the generation of inexpensive and quick-to-deploy domain names has spawned.

Vixie's concept of putting new domain names on hold for just a few minutes or hours is a practice that could deter malicious activity. "If they still exist then and are not taken down … and are not in a reputation system [blacklist], that means there's probably nothing wrong with them," Vixie, who is CEO of Farsight Security, said in an interview with Dark Reading last year.

Human-Readable

Lewman and Keraudy used Farsight's Passive DNS service, which gathers DNS response data in real-time, and CybelAngel's Web-crawling technology and data analysis algorithms, to allow the researchers to spot counterfeiters' domain names when those sites go live. "We converted passive DNS to visualization related to" a commonly counterfeited brand, for example, Keraudy says.

It's basically a way to convert that data into human-readable and easily understood intelligence about the bad sites and their operations.

"You get clustered visualization of those websites, so you can clearly visualize those [illicit] organizations," he says.

A company whose brand is being abused, such as a luxury handbag company, would then get specific details and information on that illegal organization, so they then can take legal action.

"We have a crawler on the suspicious websites with the goal of extracting as much information as possible, such as phone number, email, Whois" and other information, Keraudy says.

But even this more advanced method of rooting out domain abuse isn't likely to stop online scamming altogether.

"It will always be a cat-and-mouse game," Keraudy says.

Related Content:

- Vixie Proposes 'Cooling-Off Period' For New Domains To Deter Cybercrime
- DDoS And The Internet's Liability Problem
- Domain Abuse Sinks ‘Anchors Of Trust’
- 7 Regional Hotbeds For Cybersecurity Innovation

Kelly Jackson Higgins is Executive Editor at DarkReading.com. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise ... View Full Bio

- Outsmart Ransomware Attacks with the Right Protection Strategy
- DarkReading Virtual Event: Re-Thinking IT Security Strategy

MORE WEBCASTS

White Papers

- Darktrace Discoveries: Global Threat Case Studies 2016
- You Will Be Breached

MORE WHITE PAPERS

Reports

- [Dark Reading] 2016 Security Salary Survey
- [Gartner Report] The 5 Models of Security Operation Centers

MORE REPORTS