New tool detects malicious websites before they cause harm

by Josephine Wolff for the Office of Engineering Communications
Oct. 27, 2016 2:30 p.m.

Nick Feamster

Photo courtesy of the Department of Computer Science

Malicious websites promoting scams, distributing malware and collecting phished credentials pervade the web. As quickly as we block or blacklist them, criminals set up new domain names to support their activities. Now a research team including Princeton University **computer science** (http://www.cs.princeton.edu/) professor **Nick Feamster** (http://www.cs.princeton.edu/~feamster/) and recently graduated Ph.D. student Shuang Hao has developed a technique to make it more difficult to register new domains for nefarious purposes.

In a **paper** (http://www.icir.org/vern/papers/predator-ccs16.pdf) presented at the 2016 ACM Conference on Computer and Communications Security on Oct. 27, the researchers describe a system called PREDATOR that distinguishes between legitimate and malicious purchasers of new websites. In doing so, the system yields important insights into how those two groups behave differently online even before the malicious users have done anything obviously bad or harmful. These early signs of likely evil-doers help security professionals take preemptive measures, instead of waiting for a security threat to surface.

“The intuition has always been that the way that malicious actors use online resources somehow differs fundamentally from the way legitimate actors use them,” Feamster explained. “We were looking for those signals: what is it about a domain name that makes it automatically identifiable as a bad domain name?”

Feamster, the acting director of Princeton’s **Center for Information Technology Policy** (http://citp.princeton.edu/), will be participating in the upcoming fourth **Princeton-Fung Global Forum** (http://fungforum.princeton.edu/), which is focused on cybersecurity. The event will be held March 20-21, 2017, in Berlin.

Once a website begins to be used for malicious purposes — when it’s linked to in spam email campaigns, for instance, or when it installs malicious code on visitors’ machines — then defenders can flag it as bad and start blocking it. But by then, the site has already been used for the very kinds of behavior that we want to prevent. PREDATOR, which stands for Proactive Recognition and Elimination of Domain Abuse at Time-Of-Registration, gets ahead of the curve.

The researchers’ techniques rely on the assumption that malicious users will exhibit registration behavior that differs from those of normal users, such as buying and registering lots of domains at once to take advantage of bulk discounts, so that they can quickly and cheaply adapt when their sites are noticed and blacklisted. Additionally, criminals will often register multiple sites using slight variations on names: changing words like “home” and “homes” or switching word orders in phrases.

By identifying such patterns, Feamster and his collaborators were able to start sifting through the more than 80,000 new domains registered every day to preemptively identify which ones were most likely to be used for harm.

Testing their results against known blacklisted websites, they found that PREDATOR detected 70 percent of malicious websites based solely on information known at the time those domains were first registered. The false positive rate of the PREDATOR system, or rate of legitimate sites that were incorrectly identified as malicious by the tool, was only 0.35 percent.

Being able to detect malicious sites at the moment of registration, before they're being used, can have multiple security benefits, Feamster said. Those sites can be blocked sooner, making it difficult to use them to cause as much harm — or, indeed, any harm at all if the operators are not permitted to purchase them. "PREDATOR can achieve early detection, often days or weeks before existing blacklists, which generally cannot detect domain abuse until an attack is already underway," the authors write in their paper. "The key advantage is to respond promptly for defense and limit the window during which miscreants might profitably use a domain."

Additionally, existing blocking tools, which rely on detecting malicious activity from websites and then blocking them, allow criminals to continue purchasing new websites. Cutting off the operators of malicious websites at the moment of registration prevents this perpetual cat-and-mouse dynamic. This more permanent form of protection against online threats is a rarity in the field of computer security, where adversaries often evade new lines of defense easily, the researchers said.

For the PREDATOR system to help everyday internet users, it will have to be used by existing domain blacklist services, like Spamhaus, that maintain lists of blocked websites, or by registrars, like GoDaddy.com, that sell new domain names.

"Part of what we envision is if a registrar is trying to make a decision about whether to register a domain name, then if PREDATOR suggests that domain name might be used for malicious ends, the registrar can at least wait and do more due diligence before it moves forward," Feamster said.

Although the registrars still must manually review domain registration attempts, PREDATOR offers them an effective tool to predict potential abuse. "Prior to work like this, I don't think a registrar would have very easy go-to method for even figuring out if the domains they registered would turn out to be malicious," Feamster said.

In addition to Feamster, the authors include: Shuang Hao, now at the University of California-Santa Barbara; Alex Kantchelian and Vern Paxson, University of California-Berkeley; and Brad Miller, Google. The work was supported in part by the **National Science Foundation** (https://www.nsf.gov/) and Google.

Related Stories

Researchers discover new steps in the escalating cat-and-mouse game of internet censorship

READ MORE (/news/2016/04/15/researchers-discover-new-steps-escalating-cat-and-mouse-game-internet-censorship)

Cybercrime stopper: An undergraduate's project protects against internet theft

READ MORE (/news/2018/01/19/cybercrime-stopper-undergraduates-project-protects-against-internet-theft)

OIT temporarily blocking survey website due to phishing email

READ MORE (/news/2012/04/13/oit-temporarily-blocking-survey-website-due-phishing-email)

Princeton-Fung Global Forum asks if liberty can survive the digital age

READ MORE (/news/2017/04/13/princeton-fung-global-forum-asks-if-liberty-can-survive-digital-age)

Researchers reveal 'extremely serious' vulnerabilities in e-voting machines

READ MORE (/news/2006/09/13/researchers-reveal-extremely-serious-vulnerabilities-e-voting-machines-0)

Princeton researchers envision a more secure Internet

READ MORE (/news/2008/02/15/princeton-researchers-envision-more-secure-internet)

PRINCETON UNIVERSITY