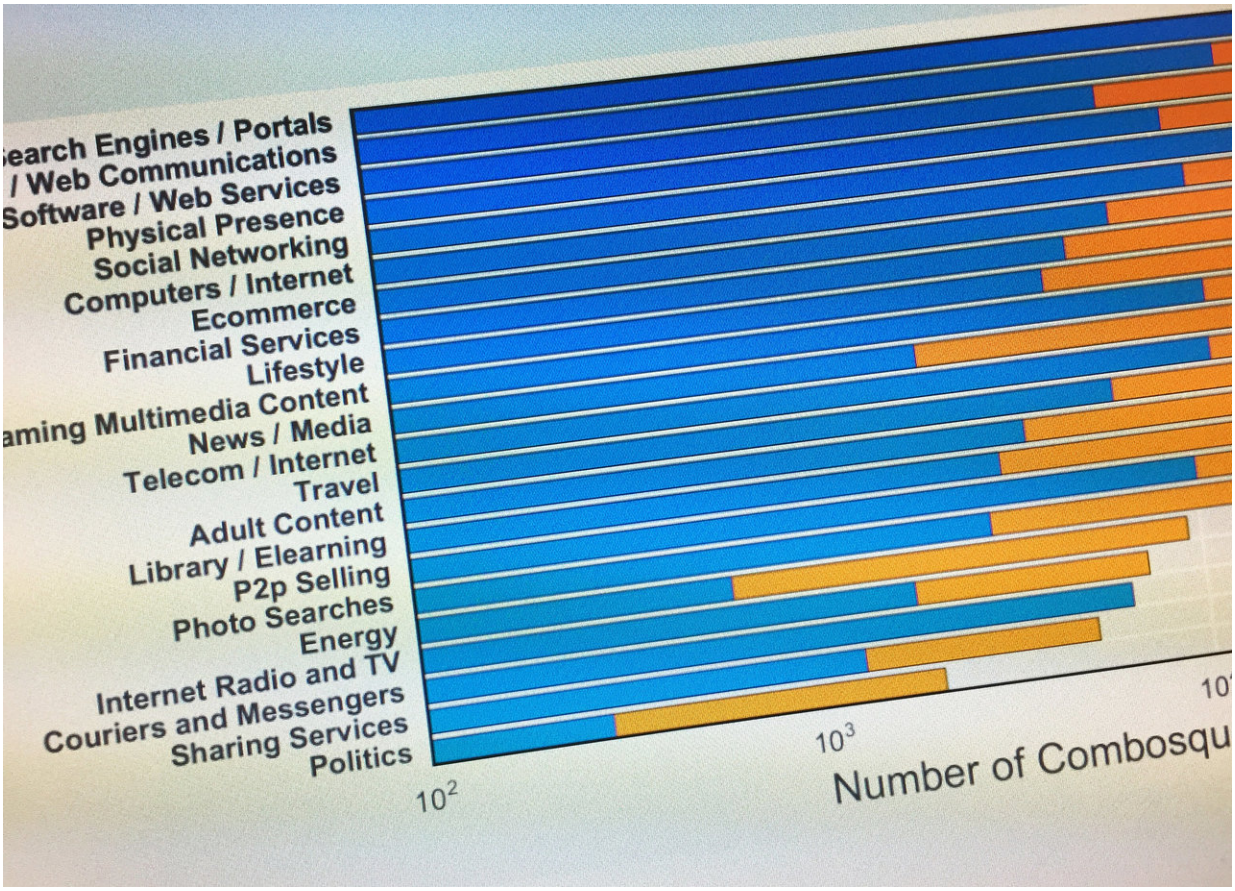
'Combosquatting' attack hides in plain sight to trick computer users

October 30 2017



This chart shows the number of combosquatted domains identified in each domain group studied. Credit: Georgia Tech

To guard against unknowingly visiting malicious websites, computer

users have been taught to double-check website URLs before they click on a link. But attackers are now taking advantage of that practice to trick users into visiting website domains that contain familiar trademarks—but with additional words that change the destination to an attack site.

For example, attackers might register www.familiarbankname-security [.]com or www.security-familiarbankname [.]com. Unwary users see the familiar bank name in the URL, but the additional hyphenated word means the destination is very different from what was expected. The result could be counterfeit merchandise, stolen credentials, a malware infection - or another computer conscripted into a botnet attack.

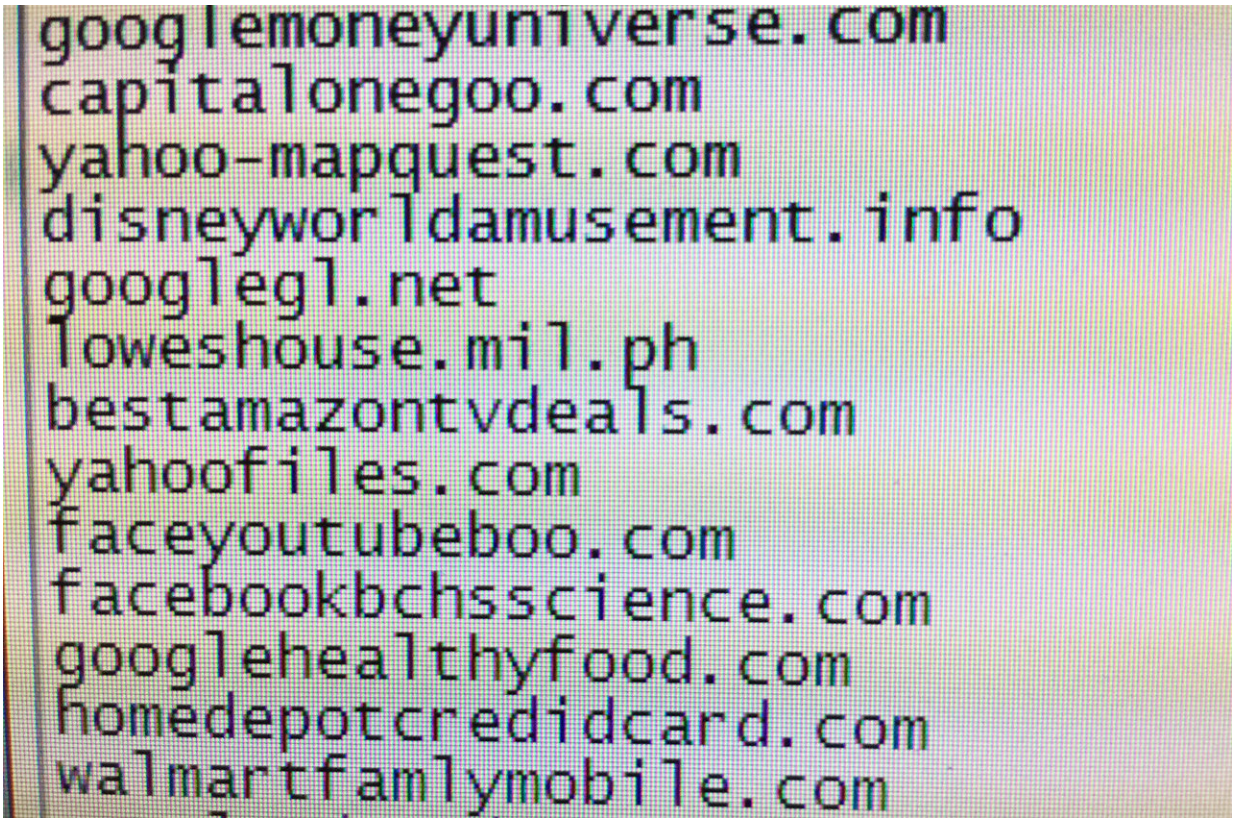
The attack strategy, known as combosquatting, is a growing threat, with millions of such domains set up for malicious purposes, according to a new study scheduled to be presented October 31 at the 2017 ACM Conference on Computer and Communications Security (CCS).

"This is a tactic that the adversaries are using more and more because they have seen that it works," said Manos Antonakakis, an assistant professor in the School of Electrical and Computer Engineering at the Georgia Institute of Technology. "This attack is hiding in plain sight, but many people aren't computer-savvy enough to notice the difference in the URLs containing familiar trademarked names."

Researchers from Georgia Tech and Stony Brook University conducted the study, which is believed to be the first large-scale, empirical study of combosquatting. The work was supported by U.S. Department of Defense agencies, the National Science Foundation and the U.S. Department of Commerce.

Combosquatting differs from its better-known relative, typosquatting, in which adversaries register variations of URLs that users are likely to

type incorrectly. Combosquatting domains don't depend on victims making typing errors, but instead provide malicious links embedded in emails, web advertising or the results of web searches. Combosquatting attackers often combine the trademarked name with a term designed to convey a sense of urgency to encourage victims to click on what appears at first glance to be a legitimate link.



Selection of combosquatting domains identified during the study. The domain names include a trademarked name, plus an additional word or words. Credit: Georgia Tech

"We have seen combosquatting used in virtually every kind of cyberattack that we know of, from drive-by downloads to phishing

attacks by nation-states," said Panagiotis Kintis, a Georgia Tech graduate research assistant who is the first author of the study. "These attacks can even fool security people who may be looking at network traffic for malicious activity. When they see a familiar trademark, they may feel a false sense of comfort with it."

For their study, the researchers began with the 500 most popular trademarked domain names in the United States, and excluded certain combinations made up of common words. They separated the domains into 20 categories, then added two additional domains: one for for politics - the study was done before the 2016 election - and another for energy.

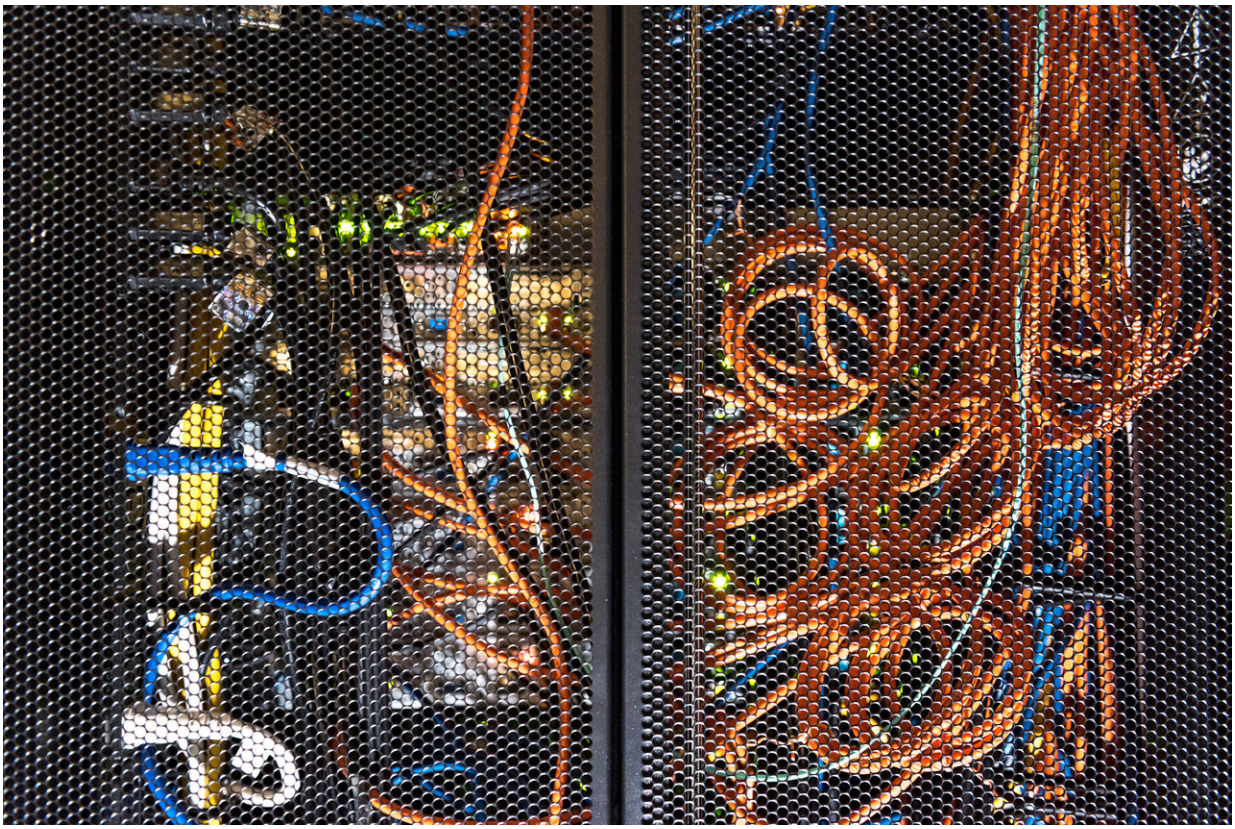
With the resulting 268 trademark-containing URLs, they set out to find domain names that incorporated the trademarked name with additional words added at the start or end. They searched through six years of active and passive domain name system (DNS) requests - more than 468 billion records - provided by one of the largest internet service providers in North America.

"The result was mind-blowing," said Kintis. "We found orders of magnitude more combosquatting domains than typosquatting domains, for instance. The space for combosquatting is almost infinite because attackers can register as many domains as they want with any variation that they want. In some cases, registering a domain can cost less than a dollar."

In the six-year data set, the researchers found 2.7 million combosquatting domains for the 268 popular trademarks alone, and the combosquatting domains were 100 times more prevalent than typosquatting domains. The combosquatting attacks appear to be challenging to combat, with nearly 60 percent of the abusive domains in operation for more than 1,000 days - almost three years. And the number

of combosquatting domains registered grew every year between 2011 and 2016.

Among the malicious domains, the researchers discovered some that had previously been registered by legitimate companies which had combined words with their trademarks. For some reason, those companies permitted the registrations to lapse, allowing the trademark-containing domain names - which once led to legitimate sites - to be taken over by combosquatting attackers.



Attackers are taking advantage of 'combosquatting,' which sends computer users to domains that contain familiar trademarked names -- but are actually attack sites. Credit: Georgia Tech

In many cases, malicious domains were re-registered multiple times after they had expired, suggesting an improvement in "internet hygiene" may be needed to address this threat.

"Imagine what happens in a city when the garbage isn't picked up regularly," Antonakakis said. "The garbage builds up and you have diseases develop. Nobody collects the garbage domains on the internet, because it's nobody's job. But there should be an organization that would collect these malicious domains so they cannot be re-used to infect people."

More stringent anti-fraud screening of persons registering domains would also help, he added. "We don't want to prevent legitimate users from getting onto the internet, but there are warning signs of potential fraud that registrars could detect."

What can be done by ordinary computer users and the organizations where they work?

"Users unfortunately have to be better educated than they are now," Antonakakis said. "Organizations can provide training in the on-boarding process that takes place for new employees, and they can protect their network perimeters to prevent users from being exposed to known combosquatting domains. More needs to be done to address this growing cybersecurity problem."

More information: Panagiotis Kintis, et al., "Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse," 2017 ACM Conference on Computer and Communications Security, arxiv.org/abs/1708.08519

Provided by Georgia Institute of Technology