Computer science researcher meets updated phishing attacks head on

June 11 2018, by Amy Loeffler

Enterprising hackers can spoof the email address of a trusted friend, co-worker, or business and send forged emails to victims. "These kinds of phishing attacks are especially dangerous," said Gang Wang, an assistant professor of computer science in Virginia Tech's College of Engineering. "Technology changes so quickly, and now a hacker can obtain your information easily." Credit: Virginia Tech

In this age of cyberattacks and data breaches, most email users are on the lookout for, and understand the potential risks of, messages and attachments coming from unfamiliar sources.

However, that vigilance alone might not be enough to keep you protected, according to new research from Virginia Tech that examines the growing sophistication of phishing attacks.

Along with savvier writing, now enterprising hackers can spoof the email address of a trusted friend, co-worker, or business and send forged emails to victims. With the right amount of social engineering, it's easy to obtain crucial and sensitive information from an unsuspecting recipient with a simple request.

"These kinds of phishing attacks are especially dangerous," said Gang Wang, an assistant professor of computer science in Virginia Tech's College of Engineering. "Technology changes so quickly, and now a hacker can obtain your information easily. This information can be used to commit cyberattacks that run the gamut from being mildly annoying, like having to deal with a checking account that has been hacked, to serious consequences of physical life and death if information, for example, to a hospital's computer mainframe is obtained."

One of Wang's research areas is currently focused on studying how to thwart these attacks. He will present a paper on his recent findings at the 27th Annual USENIX Security Symposium in Baltimore, Maryland, in August.

Phishing attacks have involved nearly half of the more than 2,000 confirmed security breaches reported by Verizon in the last two years. These breaches cause leakage of billions of records and cost millions of dollars to rectify depending on the industry affected and its geographic location.

Spoofing, where the attacker impersonates a trusted entity, is a critical step in executing phishing attacks. Today's email system has no mechanism to fully prevent spoofing.

"The SMTP system we are using today was designed without security in mind," said Wang. "That's something that has plagued the system since its inception."

Security measures were put into place to guard against spoofing attacks after the fact and rely on email providers to implement strategies using SMTP extensions, such as SPF (sender policy framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication), to authenticate the sender. Measurements conducted by the research team in 2018 indicate that among Alexa's top 1 million domains, 45 percent have SPF, 5 percent have DMARC, and even fewer are configured correctly or strictly.

For the study, the research teams' methodology was centered on setting up end-to-end spoofing experiments on popular email providers that are used by billions of users. They did this by setting up user accounts under the target email services as the email receiver and using an experimental server to send forged emails, with a fake sender address, to the receiver account.

The spoofed sender address is the key to the study as this is a critical part of the authentication process. If the spoofed domain has a valid SPF, DKIM, or DMARC record, then the receiver, in theory, is able to detect spoofing.

Spoofing can be done using existing contacts or the same email provider as the intended recipient.

To this end, researchers used five different types of email content for

the study: a blank email, a blank email with a benign URL, a blank email with a benign attachment, a benign email with actual content, and a phishing email with content that impersonates technical support to notify and rectify a security breach by being directed to a URL.

In total, the study used 35 popular email services, such as Gmail, iCloud, and Outlook. The researchers found that email providers tend to favor email delivery over security. When an email failed authentication, most email providers, including Gmail and iCloud, still delivered the email as long as the protocol of the spoofed domain was not to reject it.

The researchers also found that only six email services have displayed security indicators on forged emails, including Gmail, Protonmail, Naver, Mail.ru, 163.com, and 126.com. Only four email services consistently display security indicators on their mobile email apps. Human factors still remain a weak link in the end-to-end process, so the research team framed the study to understand users' email habits.

In Wang's study, the click-through rate for people who received the email with a security indicator was 17.9 percent. Without a security cue, the rate was 26.1 percent. Because not everyone who received a phishing email opened the email, the team also calculated the click-through rate on all users who opened the email, resulting in higher rates of 48.9 percent and 37.2 percent.

Recommendations from the study include adoption of SPF, DKIM, and DMARC to authenticate emails, and if an email is delivered to an inbox, email providers should place a security indicator, such as Google's red question mark on the email, to warn users of the potential risks.

The team also recommended consistency among email providers for different interfaces. Currently mobile users are exposed to higher level of risks due to the lack of security indicators. And finally, the study

recommended that misleading elements, such as a "profile photo" and email "history," be disabled on suspicious emails.

With so many emails being delivered on a daily basis, it's surprising that there aren't more successful phishing campaigns.

"It really only takes one email to cause a security breach," said Wang.

Provided by Virginia Tech

Citation: Computer science researcher meets updated phishing attacks head on (2018, June 11) retrieved 3 May 2024 from https://phys.org/news/2018-06-science-phishing.html