What's Behind The Surge In Phishing Sites?

By Tyler Moffitt

The diversification of attacks

Since first being described in a 1987 paper, phishing attacks have diversified considerably. While it was once reliably email-based with a broad scope, it now entails malware phishing, clone phishing, spear phishing, smishing, and many more specialized forms. Inevitably, these strains of attack require landing pages and form fields in for users to input the information to be stolen, helping to fuel the rise in active phishing sites.

Spear phishing—a highly targeted form of phishing requiring cybercriminals study their subject to craft more a realistic lure—has turned out to be a lucrative sub-technique. This has likely contributed to more cybercriminals adopting the technique over mass-target emails pointing to a single source. More on profitability later.

Opportunism

After years of studying phishing data, it's clear that the number of active phishing sites rises predictably during certain times of the year. Large online shopping holidays like Prime Day and Cyber Monday inevitably precipitate a spike in phishing attacks. In another example, webpages spoofing Apple quadrupled near the company's March product release date, then leveled off.

Uncertainty also tends to fuel a rise in phishing sites.

"Not only do we always see a spike in phishing attacks around the holidays," says Moffitt, "It also always happens in times of crisis. Throughout the COVID-19 outbreak we've followed a spike in phishing attacks in Italy and smishing scams promising to deliver your stimulus check if you click. Natural disasters also tend to bring these types of attacks out of the woodwork."

The year 2019 was not without its wildfires, cyclones, and typhoons, but it'd be safe to suspect the number of phishing sites will grow again next year.

Short codes and HTTPs represent more phishing opportunities for cyber criminals. Malicious content is now often hosted on good. Short codes also have the unintended consequence of masking a link's destination URLs. Both these phenomena make it more difficult to identify a phishing attack.

"All of sudden these mental checks that everyone was told to use to sniff out phishing attacks, like double-checking URLs, no longer hold," says Moffitt.

Profitability

Let's face it, this is the big one. The rise in popularity of shared drives makes it more likely that any single phishing success will yield troves of valuable data. Compromising a corporate Dropbox account could easily warrant a six-figure ransom, or more, given the looming threat of GDPR and CCPA compliance violations.

"A few years ago, most of the targets were financial targets like PayPal and Chase," according to Moffitt. "But now they are tech targets. Sites like Facebook, Google, Microsoft, and Apple. Because shared drives offer a better return on investment."

Even for private individuals, shared drives are more bang for the buck. Credentials which can easily lead to identity theft can be sold on the dark web and, given the rampant rates of password re-use in the U.S., these can be cross-checked against other sites until the compromise spirals.

Finally, phishing is profitable as an initial entry point. Once a cybercriminal has accessed a business email account, for instance, he or she is able to case the joint until the most valuable next move has been determined.

"It's a really lucrative first step," says Moffitt.

Don't take the bait

Installing up-to-date antivirus software is an essential first step in protecting yourself from phishing attacks. Continual education is equally as important.