Executive Summary:  

[State of the Internet] / Security

Volume 5, Issue 5

Phishing — Baiting the Hook
Executive Summary

Phishing isn’t a new phenomenon. Since the early days of the Internet, nefarious actors have been impersonating people and businesses in order to first gain your trust, and then your personal information. Now that the Internet is more prevalent in our lives, attackers are getting savvier, making their phishing attacks more sophisticated so that we still fall for them – no matter how aware we are.

Phishing attacks require two things: a lure and a landing. This installment of the State of the Internet (SOTI) report covers these items and explores the lifecycle and development of these attacks. We’re also excited to feature Alex Pinto, Head of Security / DBIR Team Leader at Verizon Enterprise Service, as our guest author for this edition.

Pinto writes about data science and secrecy, and how sharing data can help the industry rise to the elevated level necessary to work to deter more sophisticated attacks:

“Over the years, I’ve heard many practitioners say that Information Security is a profession in its infancy. I believe that this anxiety about our profession boils down to a fear of the unknown, and a lack of data. We’re playing chess in the dark, unable to plan our next move, let alone see our endgame.”

In order to adapt to increasing defenses, phishing has evolved from being an email-based attack to one that now includes mobile devices and social media. This evolution is leveraging the world’s increasingly connected existence as a means of rapid propagation.

This report dives into virtually every aspect of phishing: from the basics of phishing as it has evolved over the years, to the development cycle used by phishing kit creators, and the growth of phishing as a service.

It seems that part of the evolution has led to the shortened life span of phishing kits. More than 60% of the phishing kits monitored by Akamai were active for only 20 days or less. Kits typically focus on consumer products, banking or finance, and gaming. Attackers build kits to focus on these markets, not only because of the wide pool of potential victims, but also because personal information from these verticals can lead to a hefty payday.

Aspects of compromised data could be financial records or other services such as streaming media, restaurant accounts, travel accounts, retail rewards accounts, and more. Each of these can be packaged and sold, sometimes as individual units. Other times, they can be sold in bulk based on geographic location.

According to Akamai data, the high-tech sector was the top target for phishing attacks. A number of high-profile technology organizations, along with businesses in the retail space, had several kit variants that targeted them during our observation period.

Akamai observed more than 2,064,053,300 unique domains commonly associated with malicious activity over a 60-day period. Of those domains, 89% had a life span of less than 24 hours, and 94% had a life span of less than three days.
Even as awareness of phishing attacks grow, criminals are still finding ways to fine-tune their phishing lures. Developers set out to design phishing kits as a near-perfect clone of the target’s website, because the criminals are hoping that a quick visual inspection is all a victim will need before entering credentials, personal information, or downloading a file.

How does Akamai protect itself against the threat of phishing, one of the most prevalent attacks any organization faces? For the first time, we are peeling back the layers to show readers how Akamai uses Akamai to protect itself. Since much of the data in this issue is drawn from our global logs and research, we thought it appropriate to share information about what we tell customers about our own experience. These systems represent a subset of our controls, with many additional systems in place to protect our enterprise.

It's important for security businesses to use their tools to protect themselves. Not only does it show confidence in their technology, but it also provides a case study on what types of challenges their customers might face. But no technology is perfect, which is why Akamai builds layers of overlapping controls to protect itself.

The latest SOTI report digs deeper into a few examples of how the phishing economy works, and how users and businesses can take steps to protect themselves against the ever-evolving threat of phishing. This style of attack is not one-size-fits-all, so users and businesses must continue to do due diligence to stay one step ahead of criminals looking to misuse their social trust.

To read the full report, head to Akamai State of the Internet/Security: Phishing – Baiting the Hook.