The Changing Face of Phishing

By Ken Dunham – ISSA member, Boise, USA chapter

For many 2003 was the awakening of a new type of fraud, *phishing*. Five years later, in 2008, significant changes have occurred in the phishing fraud arena, and these will be impacting changes in phishing over the next five years. One of the key challenges of proactive cybersecurity efforts is to predict where the next threat focus will be by bad actors as they respond to new countermeasures in the wild. This article briefly reviews phishing and malcode threats starting in 2003 forward and then identifies three key future phishing threats that will likely mature over the next five years: endpoint phishing, phishcode, and vishing attacks.

In 2003 most phishing pages were rather simple to create, deploy, and trick users into entering sensitive information on a remote website. During this same period a few malcode threats emerged that were related. One code, MiMail, included a PayPal-spoofed window to steal full details from the victim. In 2003 this was a very forward-thinking and advanced threat, seemingly all too common five years later.

Over the next few years as the phishing market matured, a variety of changes took place. Tricks with iFrame windows, overlays, images, vulnerabilities, and especially URI obfuscation were all too common. In other cases phishing involved abuse of services like Google Adwords abuse in 2005, spoofing legitimate retailers to redirect shoppers to a phishing site.

Phishing soon became well-integrated into the spam market with groups like Rock Phish. This led to the development of image-based spam and similar techniques from organized criminal groups with the capabilities to quickly develop and implement their own countermeasures.

By 2006 codes like MetaPhisher had already performed sophisticated man-in-the-middle (MITM) manipulation of financial transactions for dozens of banks globally, including a local phishing attack against UK banks. This is a much more powerful vector of attack that is very difficult to both identify and mitigate compared to traditional phishing vectors.

By 2008 phishing malcode exist that monitor URIs and obtain injection scripts from a remote command and control server in real time, injecting additional frames or modified content into the browser as the user visits a financial organization or similar website. This endpoint phishing is very difficult to mitigate as it is performed dynamically on the host instead of a remote website.

Phishcode attacks, where phishing pages are used to exploit and/or trick the user into installing malicious code, now exist, revealing a tighter convergence between malcode and phishing fraud operations. When the end point is compromised and controlled, the bad actor has more power and survivability for extended fraud operations compared to more traditional vectors.

Vishing, which combines phone and phishing techniques, is a more sophisticated form of phishing but is highly scalable, efficient, and automatable. Bad actors can send out traditional spam emails directing users to call a number to "verify their card" or similar such socially engineered messages. Credit card data (or other sensitive information) entered by victims is sent to the bad actor's computer, parsed, and exported to the bad actor's email in real time. More dangerously, vishers may also use or abuse outbound broadcast services to call thousands of individuals within a specific geolocation, play a recorded message, and have them interact with a remote VoIP server that sends data submitted by victims to the visher, again in real time. While the visher takes a break from vishing, victims are busy interacting with a calling service and VoIP server, entering sensitive data being sent to the visher's server and affiliated email account(s). A vishing attack can start and stop within just a few hours for 50,000 users or more, easily resulting in thousands of victims. This new vector is also very difficult to mitigate because of its speed and abuse of VoIP services. Vishing is a prime opportunity for phishers as they shape shift to counter current security efforts in the wild.

About the Author

Ken Dunham has more than a decade of experience on the front lines of information security. As Director of Global Response for iSIGHT Partners, he oversees all global cyberthreat response and malcode research operations. He frequently briefs upper levels of federal and private-sector cybersecurity authorities on emerging threats, and regularly interfaces with vulnerability and geopolitical experts to assemble comprehensive malicious code intelligence and to inform the media of significant cyber threats. He can be reached at kend@kendunham.org.