Literature Survey
Web Phishing Detection

Phishing attacks target holes in systems that exist because of the involvement of humans. Users are the weakest link in the security chain since many cyberattacks are spread via methods that take advantage of flaws in end users. Since there is no single, effective way to address all of the weaknesses in phishing, numerous strategies are frequently used to counteract particular attacks. Many of the recently proposed phishing mitigation strategies are surveyed. In order to show how phishing detection strategies fit into the broader mitigation process, a high-level overview of the many types of phishing mitigation approaches is also offered, including: detection, offensive defense, rectification, and prevention.

Phishing is a social engineering assault that seeks to take advantage of flaws in system operations that are the result of system users. For instance, a system may be technically safe enough to prevent password theft, but uninformed end users may reveal their passwords if an attacker requests that they change them via a specific Hypertext Transfer Protocol (HTTP) connection, endangering the system's overall security. Additionally, attackers may utilize technical flaws (such as DNS cache poisoning) to create even more convincing social engineering communications (i.e. use of legitimate, but spoofed, domain names can be far more persuasive than using different domain names). Due to this, phishing attacks are a multi-layered problem, and both technological and human-level issues must be addressed for an effective mitigation strategy.

(A) History

The term "phishing" was first used in 1996 as a result of social engineering attacks by online con artists against America On-line (AOL) accounts, claims APWG. The word "phishing" is derived from the verb "to fish," where "fishers" refers to attackers who utilise socially engineered communications as bait (e.g. steal personal information of victims). Though the theft of personal information is used here as an example, it should be highlighted that attackers are not constrained by that.

(B) Phishing Motives

Weider D states that the main reasons for phishing attempts, from the viewpoint of the attacker, are:

•Financial gain: Phishers can profit financially from the use of stolen banking credentials.

•Identity hiding: phishers may sell stolen identities to other people who may be criminals looking for ways to disguise their identities and activities rather than using the identities themselves (e.g. purchase of goods).

•Identity hiding: phishers may sell stolen identities to other people who may be criminals looking for ways to disguise their identities and activities rather than using the identities themselves (e.g. purchase of goods).

•Fame and notoriety: Phishers may target victims in an effort to gain attention from their peers.

(C) Importance

According to APWG, phishing attacks were in a raised till August, 2009 when the all-time high of 40,621 unique 3 phishing reports were submitted to APWG. The total number of submitted unique phishing websites that were associated with the 40,621 submitted reports in August, 2009 was 56,362.As justified by APWG, the drop in phishing campaign reports in the years 2010 and 2011 compared to that of the year 2009 was due to the disappearance of the Avalanche Gang Which, according to APWG's 2nd half of 2010 report,was responsible for 66.6% of world-wide phishing attacks in the 2nd half of 2009 [7]. In the 1st half of the year 2011,the total number of phishing reports submitted to APWG.

Reference

Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones