PhishEye: Live Monitoring of Sandboxed Phishing Kits

http://www.eurecom.fr/fr/publication/4991/download/sec-publi-4991.pdf

Phishing is a form of online identity theft that deceives unaware users into disclosing their confidential information. While significant effort has been devoted to the mitigation of phishing attacks, much less is known about the entire life-cycle of these attacks in the wild, which constitutes, however, a main step toward devising comprehensive anti-phishing techniques. In this paper, we present a novel approach to sandbox live phishing kits that completely protects the privacy of victims. By using this technique, we perform a comprehensive real-world assessment of phishing attacks, their mechanisms, and the behavior of the criminals, their victims, and the security community involved in the process -- based on data collected over a period of five months.

Our infrastructure allowed us to draw the first comprehensive picture of a phishing attack, from the time in which the attacker installs and tests the phishing pages on a compromised host, until the last interaction with real victims and with security researchers. Our study presents accurate measurements of the duration and effectiveness of this popular threat, and discusses many new and interesting aspects we observed by monitoring hundreds of phishing campaigns.