Expanding the scope of blocklisting to improve risk-based threat mitigation

Dave Piscitello, Interisle Group LLC

Traditional reputation or block listing is based on a review of criminal or malicious activity associated with URLs, IP addresses or domain names to make a high confidence {allow, block} decision at a granular level. One objective of this decision process is to achieve high confidence or near zero false positive results.

Nearly all cyber attacks today involve the use of the DNS to manifest cyber threats. The threat landscape is broad and evolves rapidly. Information that first responders have traditionally employed to achieve near zero false positives is no longer reliably available in near real time. These circumstances favor the attacker, who benefits from a longer attack window.

It is perhaps time to consider risk rather than reputation as the basis for {allow, block} decisions. Whereas blocklisting seeks near zero false positive identification of a threat, risk-based threat mitigation strategies assess threats, assess the likelihood that a threat can be manifested into an attack, determine a risk tolerance, and implement measures to mitigate threats that have a high probability of success.

In this session, we will examine ways where information can be published via the Domain Name System (DNS) and used in real time to assess the risks associated with the domain name delegation and registration life cycle.