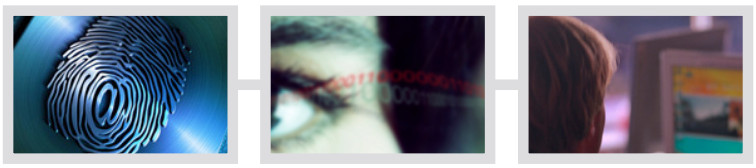
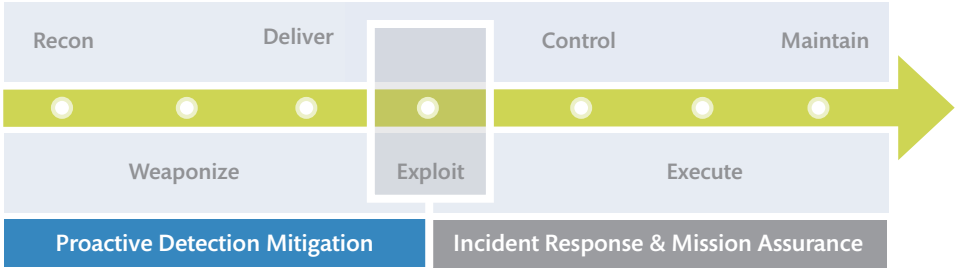
THREAT-BASED DEFENSE



Active Defense Strategy for Cyber

Introduction

Cyber attacks from advanced actors appear to be growing in scope and increasing in frequency. These attacks are successful because current defensive strategies are not well suited to mitigating prolonged and determined attackers leveraging advanced techniques. Most organizations continue to focus on preventing zero-day exploits by relying on commercial security products such as patching and blocking bad domain names and IP addresses. While these approaches are effective against some types of threats, they fail to stop advanced attacks and provide no knowledge of what an adversary does once the network is penetrated. A more effective framework for thinking about cyber defense called the cyber kill-chain, originally created by Lockheed Martin[1], is presented below.



The kill-chain depicts the phases of a cyber attack: *Phase 1 Recon*—the adversary develops a target; *Phase 2 Weaponize*—the attack is put in a form to be executed on the victim's computer/network; *Phase 3 Deliver*—the means by which the vulnerability is weaponized; *Phase 4 Exploit*—the initial attack on target is executed; *Phase 5 Control*—mechanisms are employed to manage the initial victims; *Phase 6 Execute*—leveraging numerous techniques, the adversary executes the plan; and *Phase 7 Maintain*—long-term access is achieved. The early steps of the kill-chain, *left of exploit,* represent an opportunity to proactively detect and mitigate threats before the adversary establishes a foothold. To the *right of exploit,* incident detection/response can be exercised along with assurance of mission-critical assets. To best leverage the opportunity for active defense, it is necessary to perform a retrospective analysis of threat characteristics across the entire kill-chain and correlate the results to produce tell-tale indicators.

MITRE

[1] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

© July 2012. The MITRE Corporation. All rights reserved. Approved for Public Release. Case Number 12-3352. Distribution Unlimited.

By understanding an adversary's kill-chain, the defenders have more opportunity to discover and respond to an attack. The following strategies for defense can be employed:

Recon: mine and analyze open resources to provide indicators and warning of intrusion attempts;
Weaponize: analyze artifacts to create high fidelity signatures to detect malicious activity;
Deliver: understand adversaries' tools and techniques for delivering messages to intercept them early;
Exploit: leverage anti-exploitation and exploit detection techniques to find zero-day attempts;
Control: employ robust intrusion detection signatures and tools to detect newly installed implants;
Execute: instrument and configure internal networks to detect existing internal compromises;
Maintain: deploy advanced host analysis to detect hidden implants and abnormal activity.

Active defense that leverages the adversary's kill-chain requires detailed cyber intelligence. This intelligence is best created through information sharing with peer organizations. Only by understanding adversaries' behavior against a range of targets over a period of time can defenders generate a robust set of adversary tactics, techniques and procedures (TTPs). By sharing information on TTPs, defenders gain valuable insights into an attacker's overall campaign plans and strategies. This, in turn, improves the defenders' ability to predict attacker behavior and create more dynamic defenses. However, scaling the sharing process across multiple organizations requires the parties involved to develop and/or use common security standards (such as MAEC[2]) and to employ trust models that enable genuine collaboration. A federation of sharing communities, each with its own "circle of trust" among its members using common security standards, will enable the most effective active defense strategy.

[2] http://makingsecuritymeasurable.mitre.org/docs/maec-intro-handout.pdf