THREAT-BASED DEFENSE

A Public Response to Emerging Exploits

Changing the State of HLS Cyber Capacity: Moving to Threat-based Active Defense

Leveraging new techniques to enhance
the collective cyber defenses of the United States

"To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself." - Sun Tzu

Introduction

The Public Response to Emerging Exploits (PROTeX) concept uses existing capabilities and capacity to focus on three central enablers for a more effective national cyber defense system:

- Connected networks: Shortcomings in cybersecurity present a national threat that affects government, private industry, academia, and individual citizens, potentially creating great mutual motivation for action. But to take advantage of strength in numbers, all of these parties must be connected in a common network – through not only a physical connection but also a social, human connection – to be able to share tools, techniques, and technology.
- Collaborative partnerships: Cybersecurity does not stem from control, but from partnerships. In a close-knit network, everyone has a role to play. Formal and informal public-private partnerships represent a critical tool in building national capacity to address common security challenges across .gov and .com networks.
- Collective action: To get ahead of our adversaries, the nation must join disparate activities into a coordinated campaign. By using common standards, sharing data, and working together to develop technical innovations, we can greatly improve the capabilities of both the parts and the whole of our connected network.

The first PROTeX paper presented the concept that DHS must shift from primarily Government-focused action to engagement with private organizations and citizens of the United States. The paper urged DHS to redefine the role it plays in helping to protect the cyber ecosystem. In particular, it focused on how DHS can use collaborative partnerships, either directly or indirectly, to achieve common goals. Subsequent papers in this series discuss various roles DHS can play and suggest a range of potential actions.

This paper examines one of several ways that DHS can leverage collaborative partnerships to execute collective action against threats facing systems across connected networks. We recommend that DHS capitalize on an innovative new concept — threat-based active defense — that a small number of organizations across the public-private spectrum have applied to achieve success by engaging the advanced persistent threat (APT) broadly.

Threat-based Active Defense

Today, isolated defenders crouch in their foxholes in a reactive posture awaiting the next assault, focusing on the nearest threat, and responding to the next attack. Because the adversary is distributed, organized, and persistent, our nation's defenders are at a disadvantage. We are suffering huge losses in national intellectual property and experiencing setbacks in our ability to deliver services to citizens and to conduct business. This primarily reactive posture has cultivated a sense of dependence on commercial vendors and government organizations and has paralyzed efforts by individuals and non-governmental organizations to recognize their organic potential.

But there is hope. A small subset of defenders have banded together to share tools, techniques, warnings, and experiences, and have significantly improved the defense of their networks, systems, and data. The success of this group derives from integrating three techniques: ***cyber intelligence analysis***, ***defensive engagement of the threat***, and ***focused sharing and collaboration***.

THREAT-BASED ACTIVE DEFENSE is not about directly preventing attacks. Defenders manage attacks by applying innovative tools across the attack lifecycle to learn about the opponent's goals and methods. By sharing this information with others, every defender benefits.

To appreciate the innovation represented by threat-based active defense it is useful to understand how the cyber ecosystem in the United States has addressed system and network defense in the past. Most defensive strategies in use today focus on limiting the effect of zero-day exploits by using commercial security products to block malicious sites, and by patching systems to correct exploitable vulnerabilities in installed software. This approach relies on security vendors to quickly detect new malware and attacks, generate and deploy new signatures, and eventually patch the vulnerability. In this way we attempt to minimize compromises and losses from traditional threats.

We have now realized that traditional methods do not offer adequate protection against the APT. The APT's focused approach and demonstrated adaptability reduce the effectiveness of established commercial discovery/signature generation processes. Furthermore, because commercial security products treat each attack as an individual event, they provide little help against an enduring threat. When the inevitable compromise does occur, the adversary's focus on establishing a long-term presence and then methodically pursuing strategic targets leads to big losses.

Motivated by this unacceptable level of loss, advanced defenders are developing improved methods. Across multiple organizations proven successes have emerged from both an integrated approach toward cyber intelligence analysis and the use of distinct innovative techniques – most notably attack lifecycle ("kill chain") analysis, specific sharing and collaboration, and defensive engagement of the threat.

Threat-based active defense does not *prevent* attack. Instead, it maximizes the knowledge gained from individual,

often disparate attacks and related events, and uses that knowledge to reduce the likelihood of success of future attacks.

The remainder of this paper describes the evolved approach to cyber intelligence analysis, the unparalleled opportunities afforded by defensive engagement of the adversary, and the newly discovered benefits of information sharing and collaboration.

Cyber Intelligence Analysis

Advanced cyber defenders are climbing out of their foxholes by adapting lessons learned from other enduring contests: by applying the mindset of an intelligence analyst to think differently and more comprehensively about the problem. The "cyber intelligence" approach shares many characteristics of traditional intelligence analysis. Figure 1 shows the key activities of the classic intelligence Observe-Orient-Decide-Act loop (the "OODA loop"): collecting and correlating a broad range of technical and environmental data, and then developing and testing hypotheses about adversary capabilities and intentions. Like traditional intelligence analysis, cyber intelligence seeks to provide actionable information to friendly forces. Cyber intelligence analysts strive to develop durable signatures and detect zero-day attacks, better positioning cyber defenders to quickly eliminate the intrusions that do occur.

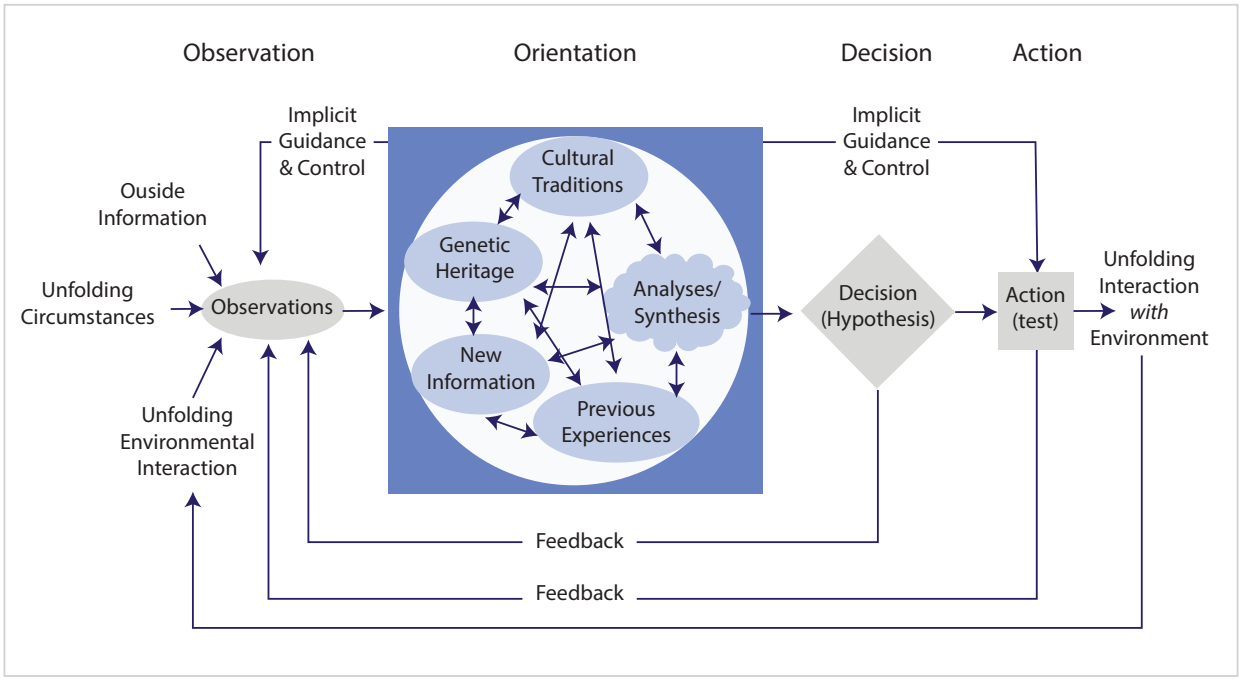


Figure 1. John Boyd's Classic OODA Loop[1]

[1]http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf

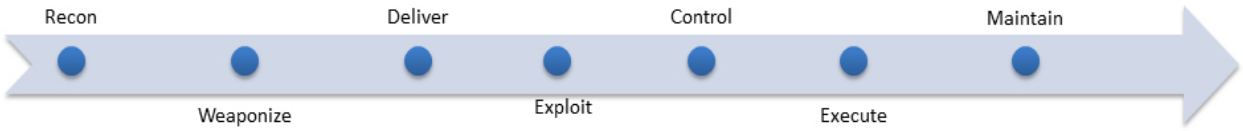
Many of the activities necessary for cyber intelligence are straightforward corollaries of their traditional counterparts, including data collection, correlation, attribution, and hypothesis formation regarding adversary strategy and tactics. Advanced defenders today:

- Collect and archive attack artifacts,
- Track environmental influences, including politics, technology developments, vulnerabilities, and exploits,
- Create databases of incidents and tactics, including targeting data and loss assessments,
- Use the data collected to generate hypotheses about adversaries, their intentions, and their TTPs, and
- Draw on all of the above to shape and prioritize defenses and react to incidents.

In addition, cyber intelligence analysts have developed techniques to address the unique aspects of the cyber threat, beginning with the development of the attack lifecycle as the fundamental model.

Attack Lifecycle ("Kill Chain") Analysis

As defenders collect and analyze data using the cyber intelligence approach, they find it very useful to organize ideas by modeling their understanding of the attack process. The "kill chain" framework, first articulated by Lockheed Martin[2], represents the stages in the development and deployment of an attack.



The kill chain depicts the phases of a cyber attack:

- Phase 1 Recon—develop a target
- Phase 2 Weaponize—the attack is readied for execution 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
- Phase 7 Maintain—long-term access is achieved

Understanding the attack lifecycle and using it as a framework to organize data and even influence analysis means explicitly considering the activities and artifacts of each stage, and how they influence all the other stages. Thinking across the lifecycle sometimes yields insights that a more narrow analysis will miss. In particular, performing analysis this way helps defenders use some of the APT's characteristics to defensive advantage.

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

One example of the leverage provided by attack lifecycle analysis comes from the domain of malware analysis. Traditional analysis examines intrusion artifacts (malware) and identifies detection signatures for a specific exploit. Those signatures are fragile because a trivial alteration (or re-weaponization) of an exploit can modify it enough to avoid detection. Lifecycle analysis of captured malware instead focuses on the weaponization phase, searching for artifacts that transcend the superficial modifications adversaries use to avoid antivirus systems. Discovering such artifacts generates significantly broader and more durable detection signatures, as well as a demonstrated ability to detect new attacks (based on the same weaponization process) the first time that particular version of the malware is seen.

Attack lifecycle analysis comprises a broad array of techniques, including:

- Data collection. Using a simple repository – even a list of unconnected facts – to record malware samples, relationships between samples, event timing, and origin or destination information, yields a dataset that can be searched, pivoted, and correlated with other information to generate new facts or relationships. These datasets can also be used for retrospective analysis and damage assessment.

- Open source[3] situational awareness. Monitoring, tracking, and evaluating world events; discovering vulnerabilities in networks, systems, and application software; determining the lifecycle of exploits in the wild; and studying reported information about criminal campaigns enable cyber intelligence analysts to remain aware of baseline (non-APT) cyber activity, opportunities for the APT to exploit newly announced vulnerabilities, and the potential influence of political, cultural, and religious events on cyber threat activity.

- Targeting analysis. Tracking network and system users over time and monitoring the level of cyber threat activity targeted against users yields insight into how adversaries discover and build up profiles about work programs and individuals.

- Malware reverse engineering. Analyzing the functionality of malicious software both statically and dynamically yields digital evidence of the cyber action—the low-level data associated with an attack. Reverse engineering employs a range of techniques, including
    - Detonation
    - Encryption analysis
    - Payload packaging analysis
    - Payload content analysis
    - C2 protocol analysis

[3]Open source intelligence refers to intelligence collected from publicly available sources.

- Higher order correlation. Combining observed events into sequences and patterns, linking actions to actors, and crafting patterns and targets into campaigns confers additional potential predictive power on cyber intelligence analysts and cyber defenders.

Collectively, innovations in attack lifecycle analysis result in more durable signatures, the ability to correlate individual events and elements of these events to sustained campaigns, and improved threat models.

Defensive Engagement of the Threat

Engagement with the adversary is critical. Half of the kill chain happens after an exploit succeeds, and knowing what adversaries will do once they have gained a foothold on a system is an intelligence bonanza. In a properly controlled situation, cyber defenders can capture tools and observe techniques the adversary uses to compromise additional systems, establish reliable command and control links, and arrange for persistence. Cyber defenders can also observe what adversaries do after successful intrusion, including how they search for data, what data they search for, and how they exfiltrate data. This wealth of useful information, when analyzed, can produce new detection signatures as well as improved threat models and attribution, greater understanding of the adversary agenda, insight into how and why the adversary targets particular organizations or individuals, and more.

Only in rare cases can organizations defer remediation of an actual compromise in order to observe tactics and develop intelligence about the adversary. Typically the risks involved—significant data loss or other failures to contain the adversary—are unacceptable, and organizations understandably insist on immediate remediation, despite the missed intelligence opportunity.

A solution that works well today is to establish a synthetic environment that permits observation of the adversary and also allows risks to be managed. These adversary engagement environments range in complexity from single laptops to dedicated networks with servers, networking gear, and other enterprise-grade components. Organizations divert attacks into the adversary engagement environment, and allow them to proceed under observation.

Adversary engagement in this style has collected significant data about tools, as well as information that has been turned into actionable intelligence and has guided the defenses of organizations that engage in the practice. Given a sufficiently well-crafted engagement environment, adversary engagements have spanned weeks, even months, not only increasing the direct yield, but also diverting the adversary's time and attention from real targets.

Information Sharing and Collaboration as a Force Multiplier

Information sharing and collaboration has been a recommended best practice for over a decade. Adopting threat-based active defense as a strategy enables top-tier defenders to work together in new ways, and this enhanced collaboration constitutes another critical element that facilitates current successes. Defenders have expanded upon the traditional exchange of signatures and indicators through:

- *More direct exchange – participating in multilateral sharing organizations to address some of the weaknesses inherent in relying on vendors. In particular, when communities form around common interests, the relevance of the targeting, TTPs, and adversary threat intelligence improves greatly, and the operational tempo increases to match the needs of the participants.*

- *More building blocks – including tools, intrusion artifacts, packet data, observed tactics and procedures. Low-level data and the tools to process it can boost analysis in the receiving organizations, allowing them to both pursue unique interests and add to the creative analytic collective resource.*

- *More finished[4] intelligence – including successful defensive tactics, hypotheses about campaigns, actors, predictions and warnings, leveraging analysis for the benefit of all.*

Routine rapid exchange of these types of information has a force multiplier impact on the ecosystem. All members of information sharing partnerships benefit from the experiences and responses of all other members. Members serve as both demanding consumers and active producers of intelligence. Contributing even a single innovative tool or intrusion artifact can improve the awareness and security of all members.

[4]When information has been reviewed and correlated with data from other available sources, it is called finished intelligence.

Summary

By revisiting traditional beliefs about cyber defense and changing the "rules of the game," a small but growing number of cyber defenders are practicing threat-based active defense and gaining ground against the advanced persistent threat. Their strategy includes adopting a cyber intelligence approach based on the classic "OODA loop" and adapting it to the cyber attack lifecycle to benefit the defender. They have also created adversary engagement environments to lure and hold cyber attackers while observing and gathering information on threat tactics. As a result, adversaries are expending more time and resources for less return.

By extending traditional partnerships to share tools, techniques, warnings, and experiences, and sharpening the focus of information sharing and collaboration, these cyber defenders have achieved significantly improved results in minimizing compromise and loss from cyber threats. This approach enables meaningful common defense without sacrificing the individuality of the participants. The 'force multiplier' effect of sharing the full range of cyber intelligence and threat indicators will continue to grow as the practice of threat-based active defense expands across the cyber ecosystem. Our adversary's strength lies in numbers; our approach to engaging them should leverage our own numbers and our collective capabilities.

MITRE