Attack-Based Network Defense

Major William North

ABSTRACT

The Department of Defense Information Network–Army (DODIN-A) is one of the largest and most complex networks in the world, and commanders are struggling to determine the effectiveness of their defensive posture as threat actors constantly attack the unclassified and classified networks. To gain a shared understanding of threats across its Defensive Cyber Operations–Internal Defensive Measures (DCO-IDM) and the cybersecurity community, the Army must establish a catalog of known and unknown threat techniques. This catalog would provide a list of analyzed threat techniques and potential mitigation actions so that Army forces spend less time reacting to the results of exploitations and more time defeating malicious actors. The catalog would also provide the foundation to support persistent penetration testing to provide a mechanism to find overlooked weaknesses, and to train analysts with real-world vulnerabilities. With this methodology in place, an Attack-Based Defense would establish an objective and quantifiable way to assess the effectiveness of cyber forces, inform commanders on how to employ cyber forces, provide business metrics for where cyber forces can improve, and ensure a common incident response across the enterprise.

INTRODUCTION

Recently there have been several highly embarrassing and entirely preventable penetrations into the Department of Defense Information Network (DODIN) conducted by DoD personnel such as the Attack the Pentagon program and the Ms. PacMan operations.

MAJ William North has served in the U.S. Army as a network engineer for 14 years. His last assignment was serving as the Network Defense Chief for U.S. Army Cyber. Before that, he served as a network engineer for the 335th Signal Command (Theater) (Provisional). He was honored with Meritorious Service Medals for his contributions to cyber and network operations. He is a distinguished graduate of the Intermediate Learning Education course and is currently a Ph.D. student at the University of Illinois at Urbana-Champaign.

Even though the tests were aimed at sections of the DODIN that do not affect the Army, one inevitably deduces that the defense of the DODIN and, by extension, the DODIN-A have room for significant improvement. A nation-state actor takes fewer than twenty minutes on average to start moving laterally after an initial compromise[1] and the time between vulnerability disclosure and weaponization is nine days on average,[2] the Army must take steps to improve network defense strategy and operations.

Army Regulation 10-87 tasks US Army Cyber Command with providing cyber support to combatant commanders and serving as the Cyber Security Service Provider (CSSP) for the DODIN-A.[3] The full spectrum of cyber operations includes cyber-attack, exploit, defense, and security. The CSSP requirements are to identify, protect, detect, respond, and recover. Of these mission sets, the cyber operations security and defense with the CSSP pillars provide the broad guidance for the Army to conduct defensive cyberspace operations.[4] In the Army, the principal Defensive Cyberspace Operations–Internal Defensive Measures (DCO-IDM) lead is the Cyber Protection Brigade with its service-assigned teams, and the principal for DODIN operations is the Network Enterprise and Technology Command (NETCOM). As noted in draft Army Field Manual 3-12, "Cyberspace defense actions conducted during DCO-IDM overlap with cyberspace security actions performed during DODIN operations."[5] Therefore, effective defense of the DODIN-A requires a continuum of effort between these principal units.

Unfortunately, the Army does not have the organizational structure and collective processes to knit these separate units together. The defense community does not have a common communications platform and utilizes a vast array of toolsets that have led to drastically different tactics, techniques, and procedures in different units. This muddled and confusing strategy frustrates efforts to develop a focused community and

limits the ability of defensive forces to respond to threats in an accurate and timely manner. Therefore, the Army must adopt a coordinated methodology supported by objective measures of performance (MOP), supported by key performance parameters (KPP), which assures commanders that the DODIN-A is properly defended against adversary activity and provides commanders situational awareness to make timely and accurate decisions.

FOUNDATIONAL ASSUMPTIONS

Asset Management

One underlying requirement for the Attack-Based Defense to work is that defensive personnel must have an accurate picture of the network they are defending – in other words, the foundation is hardware and software asset management. This ensures network operators have access to authorized devices and software and can detect unauthorized and unmanaged devices and software. Without understanding what is and is not on the network, defensive forces spend more time trying to understand terrain than in mitigating incidents on the network. Furthermore, having a standard asset management solution provides a box around expected behavior which enables analysts to determine anomalous behavior more quickly.

Data Management Strategy

The other underlying requirement is that analysts must capture the appropriate logs from all relevant data sources. Provided a minimum-security baseline (described below), network operators have a guide as to which data points are important, for how long data need to be stored, and how quickly those data points need to be ingested. This drives a robust data management strategy that incorporates the way an analyst formats and culls data, the development of the data fabric to facilitate the transport of data, and backbone infrastructure to support this data flow. Without protected and complete logging records, defensive forces are blind to the details of an attack and follow-on actions taken by the adversary.

Threats

To develop an objective and quantifiable approach to defense, the Army must start with understanding known and unknown threat techniques. For example, when defending against known threat techniques, cyber defenders should be able to tell the commander: how a threat technique works, where the risks lie in defending against that technique, how best to increase the security posture in response to that technique, how the Army will defend against that technique, and the potential impact on mission execution. For unknown threat techniques, defenders should be able to provide to the commander: potential avenues of approach for that technique and recommendations on how to increase the DODIN-A's security posture against that technique. For known threat techniques and potential unknown threat techniques, defenders need to be able to evaluate their effectiveness to monitor, detect, and respond to these threat techniques.

In defending the network, one cannot assume that 95 percent patching is good enough as a cyber adversary needs only to find one weak link to bypass the cybersecurity wall, take advantage of unmitigated vulnerabilities, and easily pivot from the initial entry point into the heart of the network. Therefore, a threat to any portion of the network is a threat to any other part of the network. We must analyze every threat technique from x_1 to x_n.

To understand the x_1 known threat technique (in the Attack-Based Defense Model, this is the base phase), an analyst must answer the following questions:

- Of what vulnerability is the x_1 threat technique taking advantage?
- What characteristics and attributes identify x_1?
- What is the behavior of x_1?
- What data can an analyst collect to detect the indicators and behavior of x_1?
- What does an analyst do when presented with a correlated event indicating a compromise?
- What is the triage priority of this event?
- Who else needs to know this information?

Further, an analyst must also consider all other known threat techniques and consider if there is overlap with x_1. For example, consider x_2 known threat technique:

- Is it possible that the vulnerability, indicators, and/or behavior overlap with x_1?
- If so, does an analyst need to collect the data once or twice?
- Is there correlating information between x_1 and x_2?

The answers to these questions inform defensive forces how to detect, understand, and monitor threat techniques. An analyst will consolidate this threat technique dictionary into a single document to which all defensive forces have access for shared understanding. This document, known as the Minimum-Security Baseline (MSB), provides a catalog from which threat techniques are monitored, analyzed, and mitigated.

However, having an MSB does not guarantee that analysts will respond correctly once an analyst detects a threat technique. Persistent penetration testing (PPT) provides a way to regularly assess the completeness of the MSB and the ability of defensive forces to respond in an accurate and timely fashion to known and unknown threat techniques. PPT enables a continuous feedback loop in which red teams assess defensive forces against the MSB and identify areas for improvement, providing a mechanism to fold those recommendations back into the MSB that red teams validate in another assessment. This methodology supports a running estimate of known threat techniques against which defensive forces can and cannot defend;

indicates where to reinforce the network's defensive posture; allows red teams to test response time and actions of analysts; provides validated analytics, questions, rules, and signatures for detection; provides a playbook for response actions; and offers a continuous feedback loop that fuses DODIN operations, DCO-IDM, and threat intelligence.

When considering y_n unknown threat techniques, DCO-IDM forces are at a significant disadvantage. These types of threats include insider threat events, social engineering, and zero-day threats derived from intelligence sources. Although they are initially at a disadvantage, this method creates the ability to quickly push a y_n threat technique from being unknown into an x_n known threat technique through a deliberate and sustainable process. Additionally, it outlines a framework that enables DCO-IDM forces to hunt for adversaries on the network while providing a mechanism to ensure an analyst incorporates the selectors into the MSB.

ATTACK-BASED DEFENSE

This approach to threat techniques provides the structural foundation of the Attack-Based Defense method. It contrasts with the current way the Army approaches cyber defense, which is more akin to bumping into things to determine that something is amiss. To implement this Attack-Based Defense method, the Army should utilize the following three-tiered process:

Base Tier

The base tier is the threat assessment phase, and the main objective of this phase is to identify and characterize threats and package this information into the MSB. This phase underpins the Attack-Based Defense and requires technically and tactically sound analysts grouped into a DevOps Support Cell (DSC). The DSC's job is to translate the offensive cyber mindset to the Army's defensive posture. DSC analysts must possess skills that include scripting, security information and event management systems, offensive cyber operations, endpoint detection and response, and operating system logging. Due to the challenging variety of skill sets required, the cost to employ these individuals, and the need to develop an enterprise MSB, the DSC should reside at the highest organizational level possible. Additionally, leadership should insulate the DSC from day-to-day operations to ensure the team develops and disseminates high-quality content to DCO-IDM forces.

A key tool in the base phase is a testing environment. To create an MSB efficiently and effectively, the DSC will need to analyze threat techniques and run malicious code against an emulated Army network. The lab will provide analysts an environment that will not break the production environment and a sandboxed location in which to train against known threat techniques. Beyond traditional defensive operations, this lab will also provide numerous advantages to the Army, such as a collaborative environment that fosters progress and innovation of TTPs through research and development, a shared environment for new applications testing and evaluating new Commercial Off the Shelf (COTS) software on an open network that does not associate the process with the Army for operational security, an environment

that simulates actual base or enclave-level architecture unconstrained by DODIN-A security policy, and an avenue for Cooperative Research and Development Agreements (CRADA) which will improve ties with vendors for newest versions of software and faster technical support. In general, leadership should consider the lab as an internal resource in which all interested users can come to test new content, whether hardware or software, before recommending its installation or purchase.

The output of the base phase is an MSB that includes a catalog outlining what a threat technique does, the indicators and behaviors associated with that threat technique, a triage priority assignment, and the defensive techniques that should be employed against that technique. The MSB is tool and network agnostic so that an analyst can apply it to any network and provides the foundation for the Attack-Based Defense.

2nd Tier

The second tier applies the MSB to the tools used by defense analysts. This requires a dedicated red team and a defense analyst cell to deploy real-world threat techniques and to determine the effectiveness of the response with the tools available. During this phase, the MSB integration team develops the KPPs and MOPs that drive the defense response against a known threat technique. Sample KPPs are the time to detection, time to response, and the ability to assess x_n threat technique as x_n correctly. During the creation of the KPPs and MOPs, analysts should attempt multiple threat techniques simultaneously so that the aggregate DCO-IDM responses are in line with the individual KPPs and MOPs. If the response is sufficient, an analyst will pass that portion of the MSB, its tool-specific implementation, and the KPPs and MOPs to the third tier. If the response for x threat technique is insufficient, an analyst sends the threat technique response playbook back to the DSC for further analysis and refinement.

3rd Tier

The third tier takes the output of the second tier to create a shared understanding for the cyber defense community, enabling analysts to understand what an event means and how to respond by referencing the MSB. Essentially, this tier provides defensive forces a clear understanding of what the threat technique is and how to mitigate it (from the MSB), its expected response time (from the KPPs), and an objective way to measure performance. Further, it provides a foundation for red teams to conduct persistent penetration testing which easily and clearly provides the commander with a way to measure the effectiveness of his or her defensive forces and proactively find unknown threat techniques.

IMPROVING ON EFFECTIVENESS

Considering how well the defense community performs is difficult because there is not a standard set of tasks with adequate measures of effectiveness to conduct an assessment. Additionally, the defense community currently lacks a standard way to communicate about threat

technique response and how to convey to leadership the risk associated with an incident. Though there are several efforts throughout DoD to standardize policy and broad tasks,[6] the Army has not adopted these efforts in a comprehensive strategy. Without such a framework, leaders cannot determine if the Army is effectively spending its limited resources for cyber defense.

Further, the lack of measures of effectiveness exacerbates the shortcomings of current effectiveness assessments, which amount to proving a negative. When the network is running without incident or, more likely, incidents are contained below the need for leadership involvement, leaders are easily lulled into complacency. However, when an incident does occur, leaders face a significant impact on operations during response actions. This whiplash between background noise and significant impact provides a false image of the work being accomplished behind the scenes. To overcome this, analysts need to show leadership dashboards with relevant and clear information that strikes a balance between hiding complexity and highlighting critical information that leads commanders to take both proactive and reactive actions.

Such dashboards are incredibly difficult to make without having clearly defined the tasks for cyber defense and a standard way of referring to threat techniques which I advocate through the MSB. Without it, the Army will continue to struggle to communicate effectiveness to leaders both proactively and reactively. Therefore, though the creation of the MSB requires significant investment and commitment, it is a necessary first step in unifying the community's efforts and being able to show concrete metrics that leaders use to understand how effective defensive forces are utilizing the holistic Attack-Based Defense approach.

OBJECTIVES OF AN ATTACK-BASED DEFENSE

The Attack-Based Defense provides a methodical approach to cyber defense. Without such an approach, the Army will continue to have an unorganized and haphazard approach to adversaries in the DODIN-A. The main objective of Attack-Based Defense is to provide a way to measure the effectiveness of defensive forces against known threat techniques through an MSB and a process to turn unknown threat techniques into known threat techniques quickly. The MSB provides the foundation for PPT, which emulates the threat technique and enables the feedback loop where unknown threat techniques turn into known techniques. Finally, an Attack-Based Defense provides an objective and quantifiable way to assess the effectiveness of defensive forces, inform commanders how to employ defensive forces, provide data on where the Army's defensive forces can improve their effectiveness, and ensure a common MSB across the enterprise.

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. "First-Ever Adversary Ranking in 2019 Global Threat Report Highlights the Importance of Speed," Crowdstrike, accessed April 16, 2020, https://www.crowdstrike.com/blog/first-ever-adversary-ranking-in-2019-global-threat-report-highlights-the-importance-of-speed.
2. "Think Fast: Time Between Disclosure, Patch Release and Vulnerability Exploitation — Intelligence for Vulnerability Management, Part Two," FireEye, accessed April 16, 2020, https://www.fireeye.com/blog/threat-research/2020/04/time-between-disclosure-patch-release-and-vulnerability-exploitation.html.
3. U.S. Department of the Army, 2017, *Army Commands, Army Service Component Commands, and Direct Reporting Units: Army regulation 10-87*, paragraph 14-2.b.(2). "ARCYBER - Plans, executes, directs, and synchronizes assigned and authorized Joint and Service DODIN operations and defensive CO across the Army's portions of the DODIN and, when directed, on other DODIN and non-DODIN networks;" paragraph 14-2.b.(8) "Serves as the Army's principal Cybersecurity Service Provider (formerly Computer Network Defense-Service Provider)."
4. U.S. Department of the Army, 2020, draft, *Cyberspace Operations and Electronic Warfare: Field Manual 3-12*, paragraph 2-5. "Cyberspace actions used to defend blue cyberspace are actions employed through cybersecurity and defensive cyberspace operations-internal defensive measures (DCO-IDM)."
5. Ibid., paragraphs 2-17.
6. Examples of methodologies are the Department of Defense Cybersecurity Services Evaluators Scoring Metric, and the United States Cyber Command Risk Assessment Methodology.