Disrupting the Attack Surface

Overview

The design principles for disrupting the attack surface create a more difficult environment for the adversary, provide defenders with the ability to observe and analyze adversary actions, and prevents the adversary from advancing through their lifecycle. This document describes how to apply the *adaptive response, deception, dynamic positioning, non-persistence, realignment,* and unpredictability[1] resiliency techniques.

Applying *Adaptive Response* to Impede Adversary Activities

Adaptive Response – Implementing nimble cyber courses of action to manage risks – can impede the spread of destructive malware in an enterprise information infrastructure and limit the damage that it does. There are two approaches that may be applied:

- Dynamic Resource Allocation: Change the allocation of resources to tasks or functions without terminating critical functions or processes.
- Adaptive Management: Change how defensive mechanisms are used based on changes in the operational environment, as well as changes in the threat environment.

Priorities for Immediate Action with *Adaptive Response*

The top priorities for *Adaptive Response* are:

- Reallocate resources to specific tasks or functions to manage risks without terminating functions or processes.
  - Identify which resources are available for reallocation without degrading, or at least minimizing the degradation of, the core mission or business functions. This activity requires planning (i.e., before an attack is known to have occurred).
  - Determine the processes for reallocation of resources, including what will be impacted and how to manage those impacts. As in the previous activity, this requires planning before an attack, as well as automation so that the planned changes can occur quickly once the adversary activity is noted
  - Ensure that the planned Cyber Courses of Action (CCoAs) take into account that some functions available under normal circumstances will not be available in adverse conditions due to reallocation.
- Change how defensive mechanisms are used based on changes in the operational environment, as well as changes in the threat environment.
  - Reduce alert trigger threshold resulting in a lower false negative rate but a higher false alarm rate during identified times of increased adversary threat levels.
  - Tighten controls to reduce unauthorized activities – this may make things more difficult for legitimate users as well.
  - Modify the use of defensive tools (e.g., scripting engines that can be run against endpoints) so that they are used in a more assertive and proactive manner to fight through an attack.
  - Change policies for network inspection – this requires more time, planning and resources and may require exemptions from normal organizational policy (e.g., breaking encryption for packet inspection, closing outbound packets, or limiting TOR or SSH in certain environments).

[1] All italicized words are defined in the *Cyber Resiliency Terms and Concepts* document.

Applying *Deception* to Redirect and Impede Adversary Activities

Deception – misleading, confusing, or hiding critical assets from, the adversary – can redirect adversary activities into deception environments thereby impeding the attack flow, slowing down the attack lifecycle, and enabling defenders to study and expose the adversary activity. There are two approaches that may be applied:

- Dissimulation/Disinformation: provide deliberately misleading information to adversaries.
- Misdirection/Simulation: Maintain deception resources or environments and direct adversary activities there.

Priorities for Immediate Action with *Deception*

The top priorities for *Deception* are:

- Establish, maintain, and direct adversaries to deception environments causing adversaries to unintentionally divulge information about the nature of their attack in a safe setting.
    - Hire and train staff who are able to create and maintain realistic deception environments.
    - Identify common adversary targets and attack vectors (e.g., email) and employ technology such as detonation chambers to detect zero day and signature-less email attacks.
    - Create honeypots/honeynets to deceive the adversary.
        - Monitor this environment and analyze adversary activity to observe what the adversary's actions are likely to be in the real environment.
        - Ensure that the deception environment is realistic enough to keep the adversary there.
        - Deception environments are rarely maintained indefinitely, therefore determine factors that indicate when it is no longer cost effective to maintain a particular deception.
    - Consider incorporating *Dynamic Positioning* and *Unpredictability* into the environment to provide a realistic feel.
- Provide deliberately false information to mislead and possibly track adversaries.
    - Identify which information types are the most likely targets for an adversary to attack.
    - Create honey tokens (e.g., false information that mimics the most likely targets like default system administrator accounts). Monitor what happens to this information (who accesses it, whether it is downloaded and where it ends up outside of the business' environment).
    - Maintain the information so that it looks like it is real and being used. There are some resources in the data loss prevention space. Care should be taken with this approach as the faked data could become a liability.

Applying *Dynamic Positioning* to Limit Adversary Impacts

Dynamic Positioning – distributing and dynamically relocating functionality or assets – can limit the spread of destructive malware in an enterprise information infrastructure and aid in removing the malware from the infrastructure. There are four approaches that may be applied:

- Functional Relocation of Sensors: Relocate sensors, or reallocate responsibility for specific sensing tasks, to look for indicators of adversary activity, and to watch for adversary activity during recovery and evolution.
- Functional Relocation of Cyber Assets: Change the location of assets that provide functionality (e.g., services, applications) or information (e.g., data stores), either by moving the assets or by transferring functional responsibility.
- Asset Mobility: Physically relocate physical assets (e.g., platform or vehicles, mobile computing devices).
- Distributed functionality: Distribute functionality (e.g., processing, storage, and communications) across multiple components.

Priorities for Immediate Action with *Dynamic Positioning*

The top priorities for *Dynamic Positioning* are

- Physically or logically relocate assets and functionality making it harder for an adversary to successfully target them, and increasing chances that the adversary's actions will be detected.
  - Change logical locations of services and applications on an aperiodic or irregular basis.
  - Change logical location of data stores on an aperiodic or irregular basis.
  - Physically relocate critical physical assets using mobile vehicles or computing devices, while maintaining appropriate protections.
  - Distribute functionality (processing, storing and communications) across multiple components.
- Physically or logically relocate defensive mitigations (including sensors) making the defensive landscape more challenging for adversary to traverse.
  - Change location (physically or logically) of sensors –this can be used to increase the level of monitoring in areas of concern but may leave some areas unmonitored. This also makes it harder and less likely for the adversary to identify defense mechanism and critical assets.

Applying *Non-Persistence* to Limit Adversary Impacts

Non-Persistence – Generating and retaining resources as needed or for a limited time – can limit the spread of destructive malware in an enterprise information infrastructure because the resources are terminated and reinitiated as needed. There are three approaches that may be applied:

- Non-Persistent Information: Refresh information periodically, or generate information on demand, and delete it when no longer needed.
- Non-Persistent Services: Refresh services periodically, or generate services on demand and terminate services after completion of a request.
- Non-Persistent Connectivity: Establish connections on demand, and terminate connections after completion of a request or after a period of non-use.

Priorities for Immediate Action with *Non-Persistence*

The top priorities for *Non-Persistence* are:

- Refresh services to eliminate adversary foothold.
  - Determine which information and services can be reinitialized/deleted and under what circumstances.
  - Use virtualization to refresh information and services drawing upon gold copies maintained in a secure environment.
- Refresh connections to minimize adversary's ability to gain or extend foothold.
  - Determine which connections can be reinitialized and when they can be eliminated to reduce exposure to attack.

Applying *Realignment* to Impede Adversary Actions

Realignment – aligning cyber resources with core aspects of mission and business functions – can impede the adversary's ability to spread destructive malware in an enterprise information infrastructure. There are four approaches that may be applied:

- Purposing: Ensure cyber resources are used consistent with critical mission purposes.

- Offloading/Outsourcing: Offload supportive but non-essential functions to a service provider that is better able to support the functions.
- Restriction: Remove or disable unneeded risky functionality or connectivity, or add mechanisms to reduce the risk.
- Replacement: Replace risky implementations with less risky implementations.

Priorities for Immediate Action with *Realignment*

The top priorities for *realignment* are:

- Offload supportive but non-essential functions to a service provider that is better able to support the functions.
    - Identify non-essential functions and service providers that can better support those functions.
    - Determine what separation from the service providers is needed for security reasons and what access they require to provide the service.
    - Provide only that access which is required, keeping in mind that shared resources (physical or logical) may be corrupted by an adversary or vulnerability and provide unauthorized access to these service providers. This is key to preventing an increase in the attack surface.
- Reduce the attack surface by removing, replacing or disabling risky implementations.
    - Remove or disable unneeded risky functionality or connectivity, or add mechanisms to reduce the risk.
    - Replace risky implementations with less-risky implementations.
    - Replace services with slightly tweaked services (i.e., introduce “special sauce”) to impede functionality of malware. These tweaks can also be used for substantiated integrity.

Applying *Unpredictability* to Impede Adversary Impacts

Unpredictability – making changes randomly or unpredictability – can impede the adversary’s ability to spread destructive malware in an enterprise information infrastructure. This technique does not stand on its own, rather it multiplies the impact of many other techniques (e.g., *deception, non-persistence* and *dynamic positioning*). There are two approaches that may be applied:

- Temporal Unpredictability: Change behavior or state at times that are determined randomly or by complex functions.
- Contextual Unpredictability: Change behavior or state in ways that are determined randomly or by complex functions.

Priorities for Immediate Action with *Unpredictability*

The top priorities for *Unpredictability* are:

- Change behavior or state at times or in ways that the adversary cannot readily determine, thus increasing the likelihood that the adversary will misread the defensive landscape impeding the success of their planned activities.
    - Identify places where randomness will not impede the mission (e.g., compiling code with some randomization, varying the time for patching or backing up systems, randomizing the specific address where data is stored, changing passwords or crypto keys at random intervals).
    - Test changes both for everyday use and for CCoAs used in adverse circumstances to ensure mission/business functions.

Preparing for the Future

As the attack surface increases due to the advent of the Internet of Things, and cloud computing, the need to disrupt and prevent attacks, and potentially reduce the attack surface also increases. The potential to adaptively respond to the adversary also increases because there are an increasing number of tools and techniques available to implement the techniques discussed in this document. However, it is important to test these tools and ensure they are mature enough for the environment in which they are deployed, since immature tools may have unintended adverse impacts on an organization’s mission/operations. It is also extremely important to secure these tools and resources as they present a significant danger in being commandeered and used against the defender. The same can be said for offloading resources. As the number of services providers increases and becomes more competitive and secure, this option becomes more viable. At the same time, it is important to examine these service providers and their requirements to ensure compatibility and compliance with the mission’s goals and purpose.