THREAT USE CASE

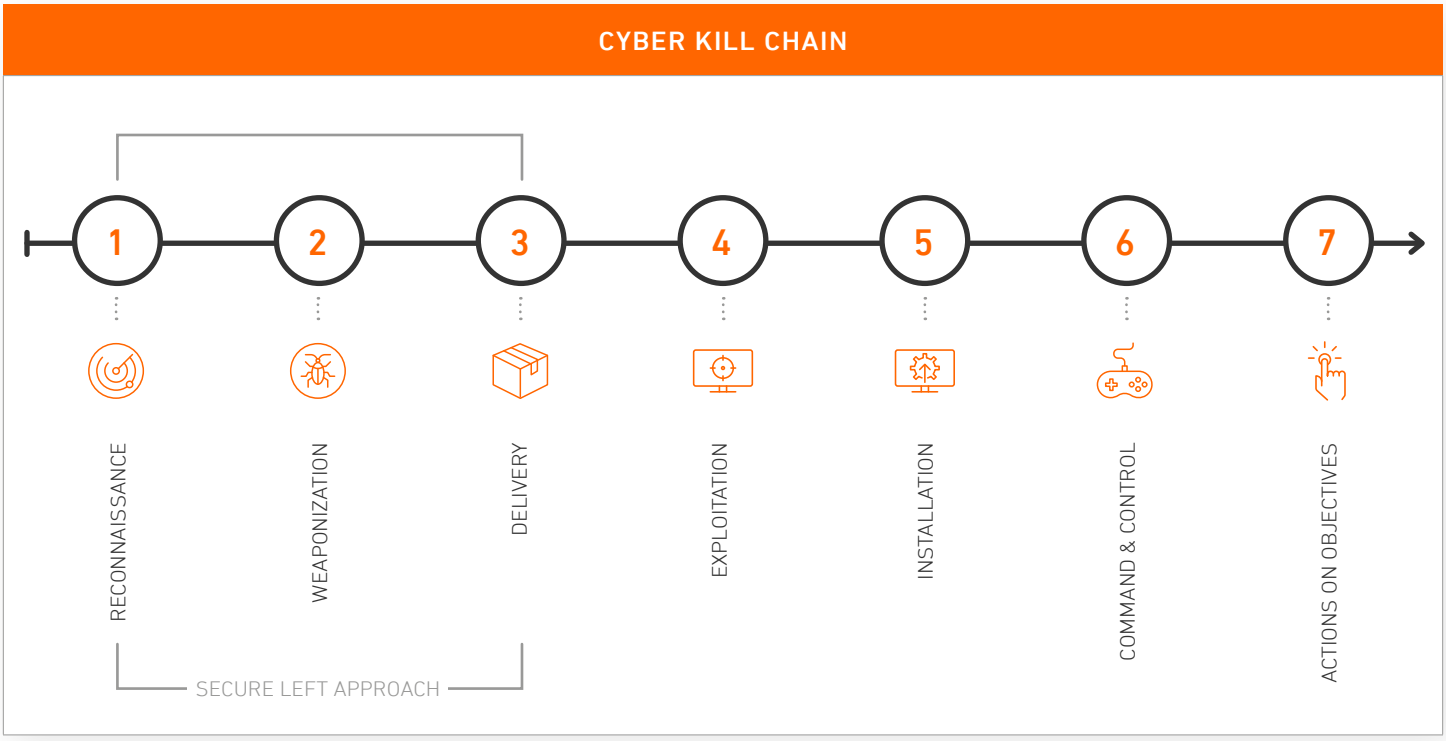
ARMOR'S DEFENSE AGAINST BOTNETS

INTRODUCTION

An internet bot, or "bot," is a computer that performs various tasks assigned to it by a command and control server. It executes simple, structurally repetitive tasks faster than humanly possible and is commonly used to automate administrative tasks or provide help and information to end users.

However, bots are also used by malicious threat actors to perform reconnaissance, discover weaknesses, infect computers with malware, or overwhelm servers with bandwidth utilization. Once a bot or group of botnets compromise machines or networks, they can then conduct reconnaissance, deliver payloads, move laterally through systems, install cyber weapons, and execute actions on target.

Mitigating the broad threat of bots requires a comprehensive security posture that involves identifying and blocking unwanted or malicious traffic before it hits your applications or network. Organizations should develop a layered security posture, one with a **"secure left"** approach that aims to thwart threat actors at every step of the Cyber Kill Chain.



In order to combat the threat of bot infections, organizations must "secure left" in their security posture, stopping threat actors before they compromise networks during the reconnaissance or delivery phases of the Cyber Kill Chain. Organizations also must ensure the latest software patches are installed or address vulnerabilities immediately when identified through various means such as vulnerability scanning. Finally, they should be vigilant to new malware or techniques identified by researchers.

HOW ARMOR DETECTS & RESPONDS TO BOTNETS

Armor's cloud security platform, the industry's leading threat detection and response platform, ingests logs from the Armor Anywhere agent and from cloud-native and third-party tools. It then correlates and analyzes those log events against threat intelligence from Armor and other third parties. The output is used to protect against discovered threats, bolster an organization's detection capabilities, and provide response in the event of an incident.

One key to combating the infection of bots and botnets is threat intelligence. Our **Threat Resistance Unit (TRU)** actively analyzes critical threats to our customers' environments and responds to the most challenging issues. They monitor new threats as they surface, which are collected from experiences with customers and a variety of the cybersecurity industry's most trusted threat intelligence sources.

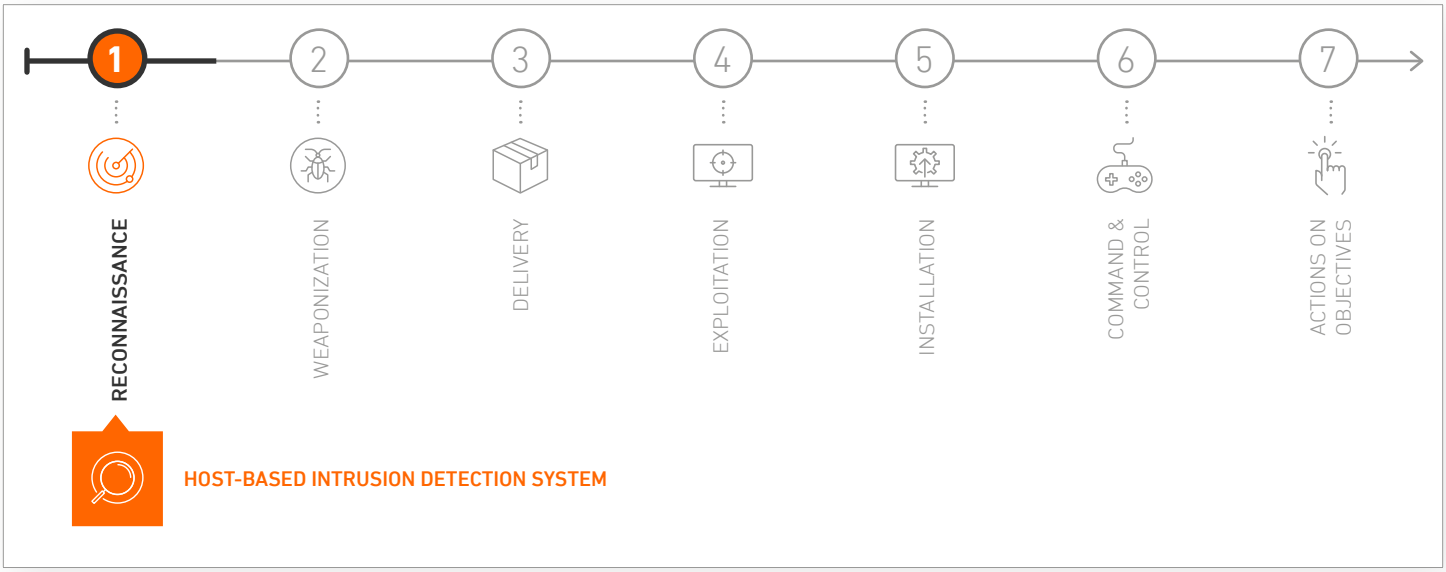
Threat Intelligence is critical to identifying automated malware attacks such as bots. Once malicious bots are identified inside your network, it is often too late—the threat actors have already gained access. One area of threat intelligence includes **IP Reputation Management (IPRM)**. Known IP addresses used by bad actors, such as commonly used command and control servers, are constantly discovered, updated, and blacklisted. Through our TRU, Armor can sometimes identify the latest threats before they are widely known and patched by software vendors.

Emotet, for example, is a malware trojan that originally aimed to steal financial data and credentials from host computers. It has been updated and reconfigured to work primarily as a loader, depositing malicious payloads including ransomware into infected systems. Once executed, the malware will execute PowerShell commands that enable it to begin retrieving malicious payloads. The loader can then deliver different forms of trojans or malware, many of which are available for sale on underground forums. In order to protect networks from Emotet, organizations must strive to detect it before it can enter the network.

Armor provides cloud security controls that aim to detect and respond to cyberattacks at various stages of the Cyber Kill Chain. As part of a layered approach to cybersecurity, Armor provides:

- Host-based Intrusion Detection System (HIDS)
- File Integrity Monitoring (FIM)
- Vulnerability Scanning
- Automated Security and Compliance (CSPM)
- Antivirus/Antimalware (AV/AM)
- IP Reputation Management
- Threat Intelligence

Armor continuously monitors customer environments for known malicious indicators and observables that can signal an intrusion at the earliest stage of the Cyber Kill Chain. Our **host-based intrusion detection system (HIDS)** monitors cloud network traffic during the reconnaissance stage, blocking known bad indicators immediately when they are detected.



If an undetected threat actor is able to progress to the **exploitation phase** of the kill chain, changes to the integrity of operating system and application software files can be detected by our **file integrity monitoring (FIM)**, as they are checked against a known good state. FIM looks for changes to critical OS, directories/files, registry keys, and their associated values. It also watches for changes to application files, rogue applications running on the host, and unusual process and port activity, as well as system incompatibilities.

Vulnerability scanning can further identify potential security concerns in services and associated network ports, anomalies in packet construction, and potential paths to exploitable programs or scripts.

Antivirus/antimalware controls detect, quarantine, and block malicious software from executing on servers and workstations.

ADDITIONAL TIPS FOR PROTECTING YOUR ORGANIZATION FROM BOTS AND BOTNETS

PATCHING

Organizations must continuously patch against vulnerabilities, both known and unknown. Minimizing the potential attack surface is critical.

DATA SEGMENTATION

Not all data is critical for business continuity, nor should all data be accessible to everyone. Least privilege access is key to securing critical data.

OFFLINE DATA BACKUPS

Users must have multiple backups of their critical data, applications, and application platforms. These backups must be air-gapped from the internet, password-protected, and tested. Best practices include the rule of 3/2/1 (3 copies, 2 storage media, 1 offsite).

WHITE LISTING SOLUTION

Limit the use of applications and processes that are allowed to run in your environment by providing a short list of approved applications and processes. Similar to a VIP list for your PC, if it's not on the list, it's not allowed.

PRACTICE LEAST PRIVILEGE ACCESS CONTROL

Ensure the user has the least privilege for their job. This also applies to services.

ENDPOINT PROTECTION SOLUTION

This solution should include endpoint detection and response capabilities for laptops, workstations, and mobile devices. It utilizes antivirus (AV) and antimalware (AM) to block cyberattacks. It is also used to quickly detect and remediate any malicious activity or infection that has made its way onto the endpoint.

ARMOR ANYWHERE

Armor Anywhere is Armor's flagship technology that provides threat detection and response as well as helps organizations meet compliance. Armor Anywhere combines workload protection, analytics from cloud-native sources, and other security data to provide unparalleled insight into threats facing organizations in any environment.

Organizations with mission-critical applications can choose Armor's high-performance hosting infrastructure and still enjoy the security benefits of Armor Anywhere.

ABOUT ARMOR

Armor is a global cybersecurity software company that simplifies protecting your data and applications in private, public, or hybrid clouds—or in an on-premise IT environment. Armor Anywhere provides technology to detect and respond to threats and can be activated in minutes. Armor also helps organizations comply with major regulatory frameworks and controls. Armor's cybersecurity experts monitor customer environments 24/7/365 and, if an attack takes place, helps customers respond quickly and effectively. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167