Automated Moving Target Defense

Automated Moving Target Defense (AMTD) is an emerging approach to cybersecurity that seeks to disrupt the traditional security model by constantly changing the target that attackers are attempting to breach. Rather than relying on static security measures that can be studied and bypassed by attackers, MTD seeks to create a dynamic and unpredictable security environment that makes it difficult for attackers to succeed.

In the context of cybersecurity, Moving Traget Defense involves implementing a variety of measures that make it difficult for attackers to locate and exploit vulnerabilities. These measures might include randomizing network configurations, frequently changing access credentials, and dynamically adjusting network routing paths.

According to Gartner analyst Lawrence Pingree for a successful attack:

- Attackers must discover service ports, protocols, version information, and application or application infrastructure to execute their attacks properly.
- Attack tools (largely scripts) rely on a defined and static attack surface area (also called a vulnerability) – which acts as their key.
- Attackers must maintain a presence on exploited systems (persistence), to execute later stages such as lateral movement, or data theft.

However, if the attacker is standing in an ever-changing quicksand (attack surface), their “key” (exploit) can’t open the door (target).

Automated Moving Target Defense in Action

One example of a technology that employs automated MTD principles is Cloudbrink’s high-performance Zero Trust Network Access (ZTNA) solution (the highest-performing VPN replacement). Cloudbrink’s ZTNA employs a number of automated MTD techniques to keep attackers on their toes and minimize the risk of successful breaches.

Rotating certificates

One of the key ways that Cloudbrink’s ZTNA delivers automated MTD is by rotating security certificates every 8 hours or less. By constantly changing the certificates used to authenticate user connections, Cloudbrink’s ZTNA makes it difficult for attackers to intercept and decrypt traffic. Another great advantage is that you never need to worry if you remembered to revoke a certificate; the system does it in hours or minutes if requested.

Temporal PoPs

In addition, Cloudbrink’s ZTNA employs a dynamic network architecture that can use thousands of elastic Points of Presence (POPs) called FAST Edges (Flexible, Autonomous, Smart & Temporal). These FAST Edges are temporal in nature, meaning that they only exist for as long as a user is connected to the network. This means there is no fixed place for attackers to target, making it difficult for them to gain a foothold in the network. Plus, if they were to gain a presence, the FAST edge would not last long enough for them to execute later stages of attack such as lateral movement.

Cloudbrink’s ZTNA is an excellent example of how AMTD can be implemented in practice to deliver a high-performance and secure network access solution. By rotating security certificates every 8 hours and using elastic Points of Presence that are temporal, Cloudbrink’s high-performance ZTNA provides an excellent choice for the hybrid workforce.

Request a demonstration here
See the ESG group’s technical validation

Hybrid-Access-As-A-Service