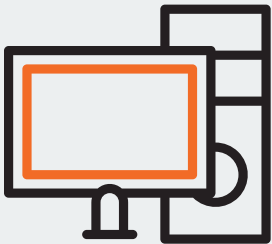


The Missing Piece in Your Security Stack

In the cybersecurity arms race, the attackers have a distinct advantage. While defenders are expected to get it right every time, an attacker only needs to be one step ahead to get around an organization's defenses. Once inside, they can remain undetected for weeks or sometimes months.

How It Works



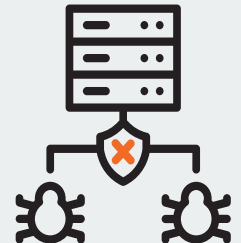
Installation: agent installed on workstations and servers to collect and send information about malware persistence mechanisms.



Examination: data is examined by automated engines to highlight new or unknown persistence mechanisms.



Hunt: Team hunts through new and unseen persistence mechanisms to investigate and confirm the presence of malicious footholds.



Mitigation: Upon discovery of a threat, actions are performed to mitigate the threat including removing the foothold and related artifacts.

Attacker Evasion Techniques

Trusted Application Abuse

Rather than write new malware to disk, malware authors may try to exploit readily available trusted applications to launch their malicious activities. Because these applications are used for normal system operation, traditional security tools may be configured to allow these operations to run in order to avoid potential service disruption.

Obfuscation

In cybersecurity, finding ways to conceal malicious behavior often uses common off-the-shelf methods. For example, encoding converts the malware file into a different format to evade standard signature-based detection. Packing is a method that compresses the file and bundles it with extraction code, making it both smaller and harder to analyze by traditional file scanners.

Trusted Infrastructure Abuse

With the rise of cloud applications, attackers use legitimate, publicly hosted services and toolsets as part of their attack infrastructure. These services are typically not blocked at an enterprise's gateway and enable outbound communications to hide in plain site. Most overlooked threats not only adapt to hide themselves from preventative measures, they establish persistence on the machine

Why persistent footholds? If we think about an attacker, they spend time and effort carefully crafting their attacks, discovering ways to trick victims into opening their attachments, and slipping past endpoint detection mechanisms. Now imagine losing all that effort to a simple reboot of the machine. To solve for this, attackers have figured out ways to establish a foothold, or persistence, to remain on the system long-term.