Hunting for Persistence:
Finding Attackers Who Are Hiding in Plain Sight

In the cybersecurity arms race, attackers have a distinct advantage. While defenders are expected to get it right every time, an attacker only needs to find one weak point to get around an organization's defenses. Once inside, they establish persistence to dwell in an environment and remain undetected for weeks or sometimes months.

WHAT IS PERSISTENCE?

Persistence is a tactic that allows attackers to quietly maintain access to a system over time. This "dwell time" is often used to conduct additional research, explore the victim's environment and determine what the best (i.e. the most profitable) next step should be.

The longer an attacker persists on a device, the more intel they're able to gather—and the more damage they can ultimately do when deploying ransomware, stealing passwords or executing other malicious activity.

WHY HACKERS RELY ON PERSISTENCE

Hackers spend a lot of time and effort carefully crafting their attacks, gaining initial access and sneaking into their target's system. Now imagine losing all of that to a simple reboot of the machine. To solve for this, attackers establish persistence to maintain long-term access to the compromised system without having to re-infect it.

Persistence provides hackers with a longer shelf life and easy re-entry should they need it. Essentially, it's an attacker's safety net.

In addition to being quiet and stealthy, persistence-enabled attacks are specifically designed to survive many of the tricks and techniques that stop traditional malware in its tracks: system reboots, changed credentials and even restoring from backups.

> **"Persistence enables hackers who gain access into your environments to keep it—oftentimes without you knowing they have access in the first place."**

HUNTRESS

PERSISTENCE TECHNIQUES AND EXAMPLES

By design, persistence is hard to detect and typically uses forms of obfuscation or evasion techniques that automated tools can't pick up on. Let's dive into a few examples of what persistence looks like and how hackers use it to fly under the radar.

FILELESS MALWARE / LIVING OFF THE LAND	
KEY	`HKU\S-1-12-1-3199256917-1110659224-2114472586-2021617454\ SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
VALUE	`BCDPREPL`
DATA	`HC:\WINDOWS\SYSTEM32\WBEM\WMIC.EXE /OUTPUT:CLIPBOARD PROCESS CALL CREATE "POWERSHELL -W HIDDEN IEX([SYSTEM.TEXT.ENCODING]::ASCII. GETSTRING((GET-ITEMPROPERTY 'HKCU:\SOFTWARE\APPDATALOW\SOFTWARE\ MICROSOFT\6E687916-F514-D0A1-EF82-F90493D63D78').CIWMORUI))"`

In this example, attackers use legitimate programs to hide their persistence mechanisms. First, the 'bcdprepl' registry value is created within the user's run key; these values are always immediately started when the user logs in. The command that is then executed uses the legitimate wmic.exe application, which in turn starts a PowerShell command to extract and run a malicious payload stored in the registry. This is known as a "fileless" malware attack because there is no malicious file on the machine—the persistence is hidden within the startup code.

BACKDOORS	
KEY	`HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\ IMAGE FILE EXECUTION OPTIONS\SETHC.EXE`
VALUE	`DEBUGGER`
DATA	`C:\WINDOWS\SYSTEM32\CMD.EXE`

What we're looking at here are attackers who have created a backdoor using a debugging feature of Windows called Image File Execution Options. When one of these options is invoked—in this case, Sticky Keys (sethc.exe)—Windows will launch a command prompt (cmd.exe). Anyone can launch Sticky Keys from a login prompt by simply pressing the "Shift" key five times, which gives attackers access to a command prompt without logging in. To make matters worse, Image File Execution Options are generally used for developers as a debugging tool, which means using this key often provides elevated access to the machine.

HUNTING FOR PERSISTENCE

Persistence has quickly become a staple in the modern attacker's playbook, yet it is often overlooked by defenders. What's more, many tools fail to pick up on the persistence mechanisms that attackers use to hide from preventive tools and lurk in an environment.

Huntress was purpose-built to detect persistence mechanisms to identify—and eliminate—persistent actors who are dwelling in IT environments through unauthorized access. Our team understands how attackers operate—and we use that knowledge to monitor for persistence, and when found, deliver actionable recommendations and instructions for removal.

HOW HUNTRESS WORKS

1. **Detect**
   Huntress finds attackers who abuse legitimate Windows applications and processes to bypass other security systems and establish persistence.
2. **Analyze**
   Our threat hunters review suspicious activity and send you easy-to-understand incident reports that explain the scope and severity of a threat.
3. **Respond**
   Isolate endpoints, remediate threats and kick attackers to the curb—with one-click approval for automated actions, and clear instructions for manual tasks.
4. **Report**
   With detailed summaries and brandable reports, you can accurately measure (and articulate) the value you're getting from Huntress.

CURIOUS WHAT'S LURKING IN YOUR ENVIRONMENT?

Learn how **Huntress' Persistent Footholds** service can help you track down and eliminate hackers who are hiding in plain sight.

HUNTRESS

huntress.com @HuntressLabs Huntress Huntress