Persistent Cyberthreats

How Cybercriminals Use Stealth to Hide in Your Network

THE ATTACKS YOU CAN'T SEE COMING

Cybercriminals are constantly evolving their tradecraft and finding new ways to infiltrate IT environments. Today's attackers are financially motivated, and they're increasingly targeting small and mid-sized businesses (SMBs)—because they know these companies don't have the security posture or expertise found in larger enterprises.

And once a bad actor has slipped past an SMB's perimeter defenses, their next goal is to establish persistence on the device they've broken into.

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.

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.

THE LIMITATIONS OF PREVENTIVE SECURITY

There's no denying the importance of antivirus solutions, firewalls and other prevention-focused security tools. But despite playing a critical role in protecting devices, these systems alone aren't enough to defend against today's hackers.

"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."

HUNTRESS

In fact, cybercriminals have become quite capable of abusing and bypassing legitimate processes and applications—rendering many front-end security tools incapable of detecting them. Once they've crept past these outer defenses, attackers shift their attention toward establishing persistence.

This is why the importance of a layered approach to cybersecurity can't be understated. Businesses need to have systems, processes and people in place to not only identify when someone is actively trying to "break in"—they need to be equally equipped to find someone that's successfully snuck past those initial defensive layers.

HOW TO FIND—AND ELIMINATE—PERSISTENT THREATS

If you identify and remove a piece of malware, there's a good chance it'll find its way right back in. That's because you're only addressing a symptom rather than the root cause; in this case, the persistence.

Persistent threats are purpose-built to avoid detection; it's dangerous to rely on automated security tools or software-only offerings to try and stop them. After all, humans are smarter than machines—how can you expect an algorithm to outmatch an intelligent and highly determined hacker?

To fight fire with fire, defenders need to adopt a human-driven approach to the problem of persistence—one that balances technology with trained experts who understand attacker tradecraft well enough to see through the techniques bad actors use to deceive automated systems.

WANT TO TAKE YOUR PERSISTENCE KNOWLEDGE TO THE NEXT LEVEL?

Download our Persistence Knowledge Kit. It has everything you need to outsmart hackers who try to hide in plain sight.