Why do automated attacks target the same locations on every computer?

Short answer: Attackers don't know anything about your specific environment, so their automation is written against locations that exist on virtually every machine — user profile folders, drive letters, and application data directories. That predictability is a weakness defenders can exploit.

The predictable targets

- **User profiles and desktops:** on Windows, `C:\Users\[Username]` reliably holds valuable data. A script walks every user directory without needing to understand the system.
- **Drive letters:** automated tools enumerate `C:\`, `D:\`, and beyond to find network shares, external drives, and mounted partitions to encrypt.
- **Application data folders:** every OS keeps credentials, cookies, and configuration in known paths — prime targets for credential theft.

Turning predictability against the attacker

The attack pattern isn't thoughtful; it's a blunt sweep of well-known locations. Cyber Crucible monitors exactly those known identity-theft and data-theft entry points. Any program reaching for data at those locations — along with its parent and child processes and associated libraries — has its intent assessed in a fraction of a second, and is intercepted if that intent is malicious.

Revision #3
Created 2026-07-20 19:23:37 UTC by Dennis Underwood
Updated 2026-07-21 19:31:51 UTC by Dennis Underwood