

Forum:[Hack Forums](#)

Thread: [\[GUIDE\] Simple Windows Hardening Steps to Block Basic Infostealers](#)

psycheuser - August 22, 2026, 9:23 pm

With the massive rise in infostealers lately, relying on default Windows Defender settings isn't always enough, especially since raw malware execution can exfiltrate browser credentials and session tokens in seconds.

Here are a few quick, low-resource tweaks you can implement to harden your daily driver machine:

1. Enable Defender ASR (Attack Surface Reduction) Rules

You can use PowerShell (as Admin) to block common malware vectors like executable content from email clients or blocking office applications from creating child processes:

```
Add-MpPreference -AttackSurfaceReductionRules_Ids 561df5c4-6e61-4113-af34-95a26e6ae7f6  
-AttackSurfaceReductionRules_Actions Enabled
```

2. Configure AppLocker or WDAC

Block untrusted executables from running out of user-writable directories like AppData\Local\Temp or Downloads. Setting up simple path rules prevents accidental clicks from executing payloads immediately.

3. Protect Your Browser Data

Infostealers target browser SQLite databases to rip stored credentials. Consider moving sensitive logins to a dedicated, encrypted password manager with master password authentication enabled, rather than saving them directly in Chrome or Edge.

4. Turn on Tamper Protection

Ensure Tamper Protection is enabled in Windows Security settings so malicious scripts cannot programmatically disable your real-time scanning or exclude directories without authorization.

Just some basic OpSec steps to add a few layers of defense. Stay safe out there!

DramaKing - August 23, 2026, 11:54 am

These are good steps, but I had one conversation where it was shown that Tamper Protection does allow exclusions.

psycheuser - August 24, 2026, 11:30 am

(Aug 23, 2026 11:54 AM)DramaKing Wrote: [\[CITE\]](#) These are good steps, but I had one conversation where it was shown that Tamper Protection does allow exclusions.

Appreciate the input, man. You're spot on—Tamper Protection definitely isn't a silver bullet, especially if an attacker gets high-privilege execution or uses a BYOVD trick to fiddle with registry keys. Are you using strict WDAC policies to handle that, or do you have a different workaround you like for locking down those exclusions?