

Forum: [Hack Forums](#)

Thread: [How do Crypters work ? Seeking ressources to understand the fundamentals behind them](#)

KaotikYan - February 22, 2025, 2:57 pm

Hello everyone,

I'm trying to deepen my understanding of how crypters function, particularly the differences between techniques aimed at bypassing scantime detection versus runtime detection. Does anyone have recommendations for reliable resources that explain the core principles behind crypters and their evasion techniques ?

To give context: Earlier today, I messed around with a PowerShell reverse shell, testing various encryption methods I found online. I managed to temporarily evade Windows Defender (WD) detection (during runtime). However, the undetected status only lasted a few hours—even with auto file submission disabled in WD (i dont know if it changes anything). This makes me curious:

1. Scantime vs. Runtime: How do crypters adapt their methods for these two scenarios?
2. Detection Refresh: Why might WD still flag the file after a short period, despite disabling auto-submission?
3. Sustainable Evasion: Are there encryption/obfuscation strategies that maintain runtime undetection longer, or is constant iteration unavoidable?

Thx for taking the time to answer my curiosity!

KaotikYan - February 23, 2025, 2:05 am

really appreciate the lead, gonna dive into it and see where it takes me