SECURITY RESEARCH

Detecting process injection with ETW

OFFENSIVE RESEARCH

Bypassing EDR real-time injection detection logic

OTHER

Malware Analysis ›

Powered By GitBook

Bypassing EDR real-time injection detection logic

⚠ This is not really about suppressing/bypassing event collection, and more on understanding EDR architecture design flaws, lazy detection logic, and correlation to minimize the chance of triggering alerts with events that are (at least partially) collected.

Some great posts on bypassing EDR agent collection:
Red Team Tactics: Combining Direct System Calls and sRDI to bypass AV/EDR (outflank)
A tale of EDR bypass methods (@s3cur3th1ssh1t)
FireWalker: A New Approach to Generically Bypass User-Space EDR Hooking (mdsec)
Hell's Gate (@smelly__vx, @am0nsec)
Halo's Gate - twin sister of Hell's Gate (sektor7)
Another method of bypassing ETW and