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 Process Injection via ETW registration (@modexpblog)
> Data Only Attack: Neutralizing EtwTi Provider (@slaeryan, kernel mode)

Introduction

In the previous post we discussed how solutions that use reliable, kernel-based sources for remote memory allocation events can use these to identify many of the in-the-wild injections with relative ease, regardless of the specific technique used, and without worrying that the event source is trivial to bypass from the user-mode. Most notably Microsoft uses that ETW, though there are vendors who do it better.

Today I wanted to share how easy it is to bypass any memory allocation-based logic. We will also bypass thread initialization alerting, which combined give us a technique undetectable by MDATP and many other EDRs out there, as of today.

It is important to expose detection gaps like this, not only to force security vendors to improve defenses, but primarily to build awareness around inherent limitations of these solutions and the need for in-house security R&D programs, or at least use of well-engineered managed detection services for more complete coverage.

> ⓘ Check out my previous post on detecting process injection with kernel ETW.

T1055 vs EDR

Let's first take a look at what independent evaluations can tell us about process injections, and if there is even anything to bypass.