EDR Arch 101: API Hooking

[AFK.conf]

PS > ls env:

- Offensive Security Redwolves
- Twitter / GitHub @g0ttfrid
- Linkedin in/yurimaia

PS > Agenda

- EDR Architecture
- API Hooking

PS > Components

- The agent
  - Sensors
  - Telemetry
  - Detections
- Server (EDR dashboard || SIEM)

PS > Agent Design - Basic

- Static scanner
- Hooking DLL
- Kernel drive
- Agent service

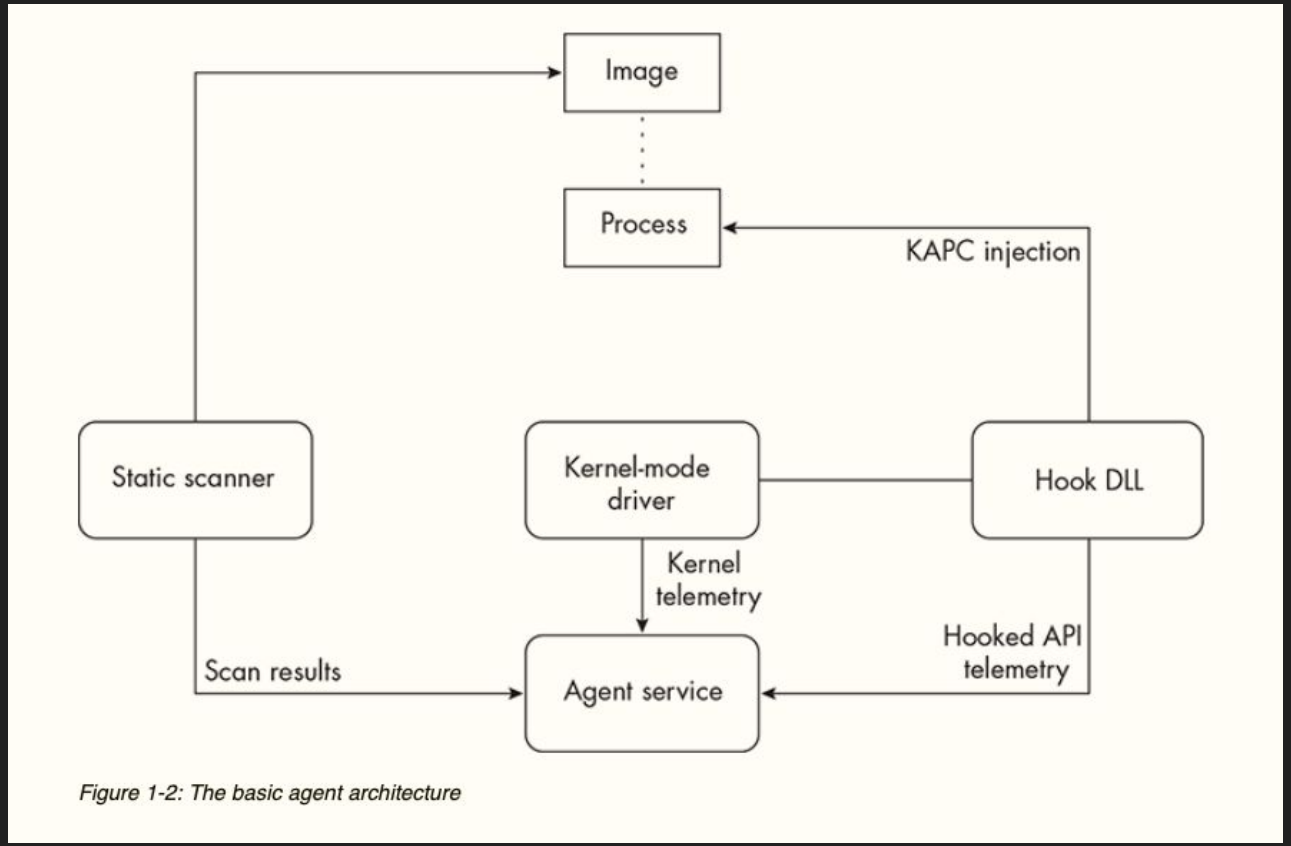


Figure 1-2: The basic agent architecture

PS > Agent Design - Intermediate

- Network filter drivers
- File system filter drivers
- ETW consumers
- ELAM components

PS > Agent Design - Intermediate

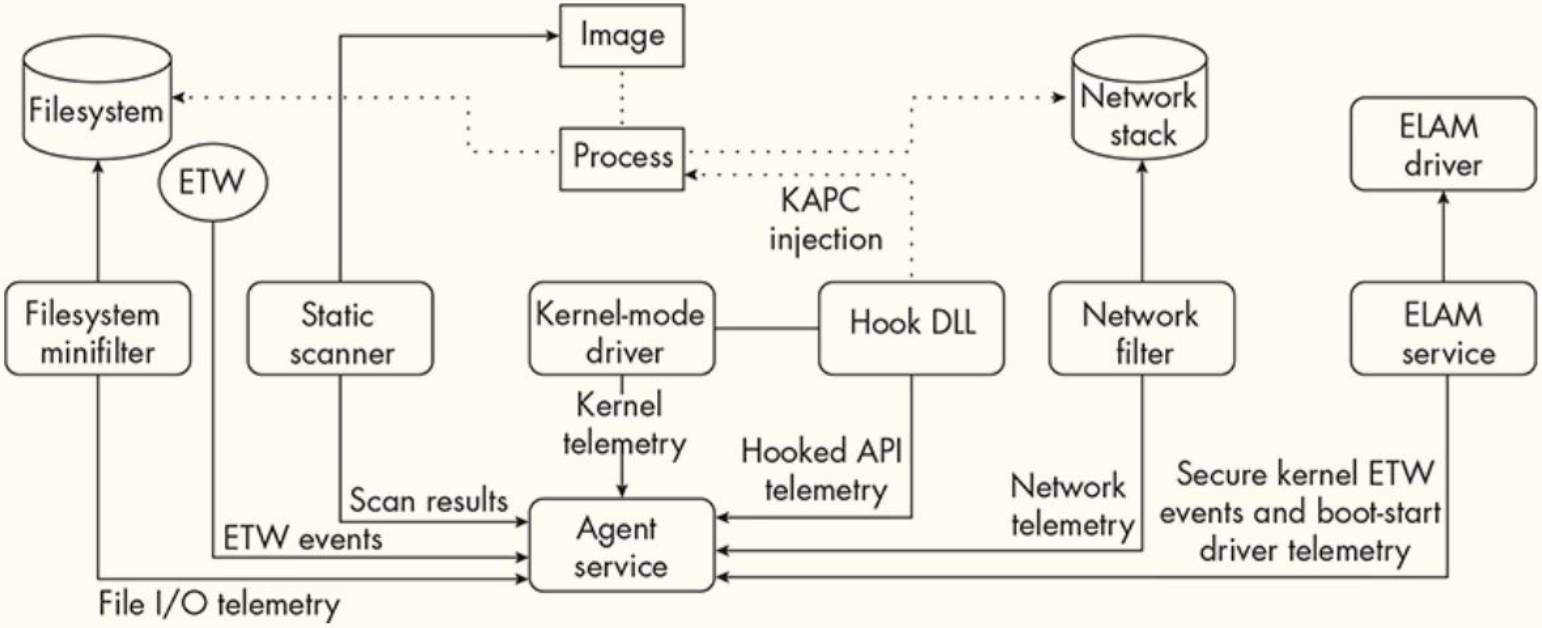


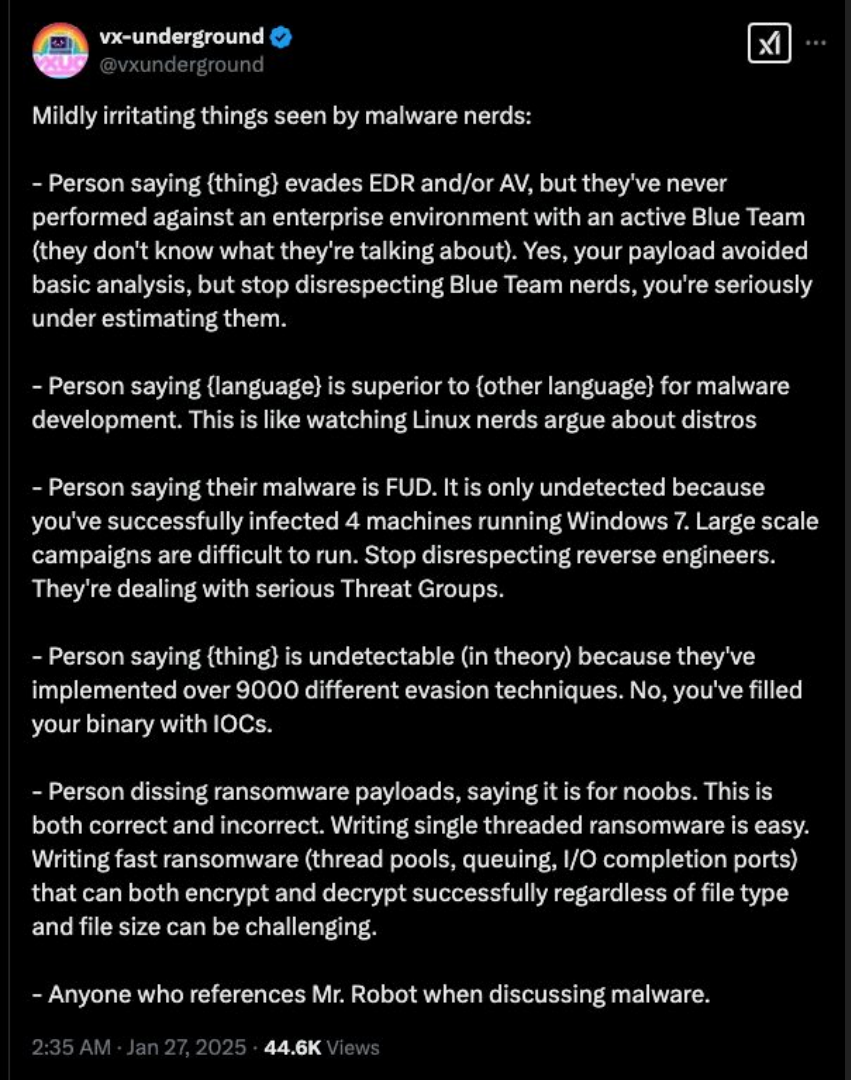
Figure 1-3: The intermediate agent architecture

PS > Agent Design - Advanced

- Hipervisors
- Adversary deception

PS > The challenges of EDR evasion

Execution != (Bypass||Evasion)



vx-underground
@vxunderground

Mildly irritating things seen by malware nerds:

- Person saying {thing} evades EDR and/or AV, but they've never performed against an enterprise environment with an active Blue Team (they don't know what they're talking about). Yes, your payload avoided basic analysis, but stop disrespecting Blue Team nerds, you're seriously under estimating them.

- Person saying {language} is superior to {other language} for malware development. This is like watching Linux nerds argue about distros

- Person saying their malware is FUD. It is only undetected because you've successfully infected 4 machines running Windows 7. Large scale campaigns are difficult to run. Stop disrespecting reverse engineers. They're dealing with serious Threat Groups.

- Person saying {thing} is undetectable (in theory) because they've implemented over 9000 different evasion techniques. No, you've filled your binary with IOCs.

- Person dissing ransomware payloads, saying it is for noobs. This is both correct and incorrect. Writing single threaded ransomware is easy. Writing fast ransomware (thread pools, queuing, I/O completion ports) that can both encrypt and decrypt successfully regardless of file type and file size can be challenging.

- Anyone who references Mr. Robot when discussing malware.

2:35 AM · Jan 27, 2025 · **44.6K** Views

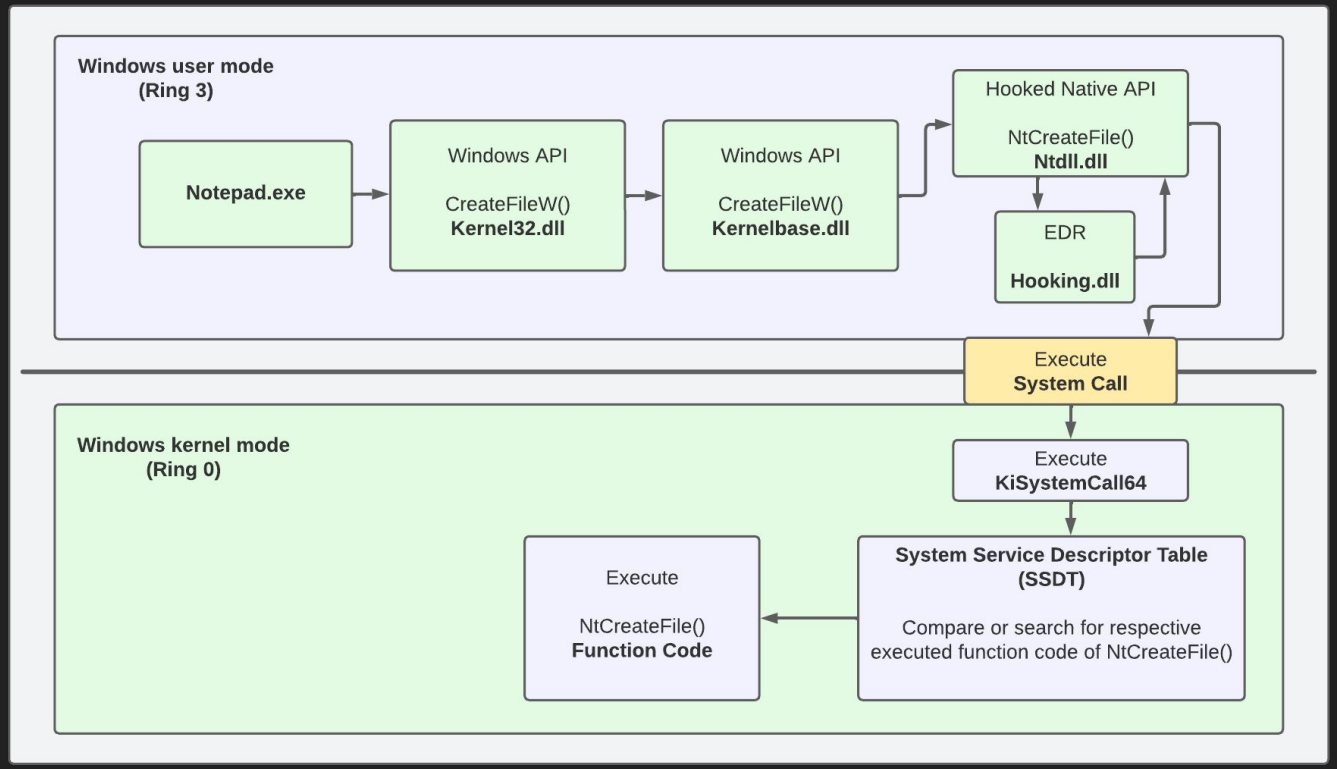
vx-underground
@vxunderground

People need to seriously stop dissing Blue Team nerds. If you've ever tried to deploy malware against an enterprise network with an active Blue Team with software restriction policies, path-based execution restriction, a team that has an effective and up-to-date EDR (custom detection rules) coupled with an AV, and an active SOC..... it can be extremely challenging.

These Blue Team nerds are not dummies and they take their job extremely seriously

2:40 AM · Jan 27, 2025 · **25.8K** Views

PS > API Hooking



The figure shows the principle of EDR user mode API-Hooking on a high level

PS > API Hooking

- PoC

PS > refs

Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems.: Hand, Matt: 9781718503342: Amazon.com: Books
Endpoint Detection and Response: How Hackers Have Evolved | Optiv
Blinding EDR On Windows - Red Team Blog
A blueprint for evading industry leading endpoint protection in 2022 | Vincent Van Mieghem
A story about tampering EDRs - RedOps
A tale of EDR bypass methods | S3cur3Th1sSh1t
Direct Syscalls vs Indirect Syscalls - RedOps - English
Bypassing User-Mode Hooks and Direct Invocation of System Calls for Red Teams - MDSec
https://github.com/microsoft/Detours/wiki/
0x09AL/RdpThief: Extracting Clear Text Passwords from mstsc.exe using API Hooking.