1030 - (Un)Fucking Forensics: Active/Passive (i.e. Offensive/ Defensive) memory hacking/debugging.

Saturday at 10:20 in Track 4
20 minutes | Hacker History, Art of Defense, Demo, Tool
K2*Director, IOACTIVE*

How to forensic, how to fuck forensics and how to un-fuck cyber forensics.

Defense: WTF is a RoP, why I care and how to detect it statically from memory. Counteract "Gargoyle" attacks.

Defense: For one of DEF CON 24's more popular anti-forensics talks (see int0x80 - Anti Forensics). In memory (passive debugging) techniques that allows for covert debugging of attackers (active passive means that we will (try hard to) not use events or methods that facilities are detectable by attackers).

Offense: CloudLeech - a cloud twist to Ulf Frisk Direct Memory Attack
K2
K2 (w00w00, ADM, undernet, efnet, The Honeynet Project) is a devil in the details person who does not take themselves too serious and appreciates a good laugh. Earlier DEF CON presentations included polymorphic shellcode in the form of ADMMutate (see ADM Crew), low-level process detection, with page table analysis (Weird-Machine motivated shell code) and using the branch tracing store backdoor trick on Windows to counter Ransom ware, detect RoP (RunTime + HW Assisted) and draw cool graphs – "BlockFighting with a Hooker: BlockfFghter2!". All three of these are open source tools available github.com/K2 (EhTrace and inVtero.Net are under active development).

@ktwo_K2
GitHub: https://github.com/K2

#defcon25/by_track/track4/saturday #defcon25/By_Day/_saturday