1100 - If You Give a Mouse a Microchip... It will execute a payload and cheat at your high-stakes video game tournament

Saturday at 11:00 in Track 3
45 minutes | Demo

skud (Mark Williams)*Embedded Software Engineer*

Sky (Rob Stanley)*Security Software Engineer, Lead*

The International, a recent esports tournament, had a 20 million dollar prize pool with over five million people tuned in to the final match. The high stakes environment at tournaments creates an incentive for players to cheat for a competitive advantage. Cheaters are always finding new ways to modify software, from attempting to sneak executables in on flash drives, to using cheats stored in Steam's online workshop which bypasses IP restrictions.

This presentation describes how one can circumvent existing security controls to sneak a payload (game cheat) onto a target computer. Esports tournaments typically allow players to provide their own mouse and keyboard, as these players prefer to use specific devices or may be obligated to use a sponsor branded device. These "simple" USB input devices can still be used to execute complex commands on a computer via the USB Human Interface Device (HID) protocol.

Our attack vector is a mouse with an ARM Cortex M series processor. The microcontroller stores custom user profiles in flash memory, allowing the mouse to retain user settings between multiple computers. We modify the device's firmware to execute a payload delivery program, stored in free space in flash memory, before returning the mouse to its original functionality. Retaining original functionality allows the mouse to be used discreetly, as it is an "expected" device at these tournaments. This concept applies to any USB device that uses this processor, and does not require obvious physical modifications.

This delivery method has tradeoffs. Our exploit is observable, as windows are created and in focus during payload delivery. The advantage to this approach is that it bypasses other security measures that are commonly in place, such as filtered internet traffic and disabled USB mass storage.
skud (Mark Williams)
Mark Williams is an embedded software engineer with experience in robotics and computer vision. His interest in embedded systems security and research builds off of a love for DIY

projects, microcontrollers, and breaking things.

@skudmunky
Sky (Rob Stanley)
Rob Stanley is a lead security software engineer with a background in reverse engineering. He enjoys working with low-level software, taking things apart and putting them back together, and malware analysis. Lately, he has turned his passion towards sharing his knowledge by teaching, and authoring CTF challenge problems.

#defcon25/by_track/track3/saturday #defcon25/By_Day/_saturday