1400 - Weaponizing Machine Learning: Humanity Was Overrated Anyway

Sunday at 14:00 in Track 2
45 minutes | Demo, Tool
Dan "AltF4" Petro*Senior Security Associate, Bishop Fox*

Ben Morris*Security Analyst, Bishop Fox*

At risk of appearing like mad scientists, reveling in our latest unholy creation, we proudly introduce you to DeepHack: the open-source hacking AI. This bot learns how to break into web applications using a neural network, trial-and-error, and a frightening disregard for humankind.

DeepHack can ruin your day without any prior knowledge of apps, databases - or really anything else. Using just one algorithm, it learns how to exploit multiple kinds of vulnerabilities, opening the door for a host of hacking artificial intelligence systems in the future.

This is only the beginning of the end, though. AI-based hacking tools are emerging as a class of technology that pentesters have yet to fully explore. We guarantee that you'll be either writing machine learning hacking tools next year, or desperately attempting to defend against them.

No longer relegated just to the domain of evil geniuses, the inevitable AI dystopia is accessible to you today! So join us and we'll demonstrate how you too can help usher in the destruction of humanity by building weaponized machine learning systems of your own - unless time travelers from the future don't stop us first.
Dan "AltF4" Petro
Dan Petro is a Senior Security Associate at Bishop Fox, a consulting firm providing cybersecurity services to the Fortune 500, global financial institutions, and high-tech startups. In this role, he focuses on application penetration testing and network penetration testing.

Dan likes to hear himself talk, often resulting in conference presentations including several consecutive talks at Black Hat USA and DEF CON in addition to appearances at HOPE, BSides, and ToorCon. He is widely known for the tools he creates: the Rickmote Controller (a Chromecast-hacking device), Untwister (a tool used for breaking pseudorandom number generators) and SmashBot (a merciless Smash Bros noob-pwning machine). He also

organizes Root the Box, a capture the flag security competition.

Dan holds has a Master of Science in Computer Science from Arizona State University and still doesn't regret it.

@BishopFox
@2600altf4
Ben Morris
Ben Morris is a Security Analyst at Bishop Fox, a consulting firm providing cybersecurity services to the Fortune 500, global financial institutions, and high-tech startups. In this role, he focuses on application penetration testing, network penetration testing, and red-teaming.

Ben also enjoys performing drive-by pull requests on security tools and bumbling his way into vulnerabilities in widely used PHP and .NET frameworks and plugins. Ben has also contributed to Root the Box, a capture the flag security competition.

#defcon25/by_track/track2/Sunday #defcon25/By_Day/_Sunday