Good Evening, and welcome to my presentation. Today I will be talking about how a simple Keylogger can be enhanced with AI. So, *what is a keylogger?*. A keylogger is a type of malware that is designed to record the keystrokes of the computer it is planted upon. The time interval for every keystroke recorded can be altered to the threat actor's benefit, but everything recorded is usually saved on a file for the attacker to access. The Threat Actor would use such a tool to steal private information such as usernames, passwords, financial information, addresses, and other sensitive data. Now, for those of you who do not know about AI, it comes in many shapes and sizes. However, today we will be looking at Generative AI. *Generative AI* is a type of artificial intelligence that can replicate the speech of a human in both audio and text form depending on the type of platform you are using. LLMs (Large Language Models), are a form of Generative AI that can have trillions of parameters. Some examples of LLMs include Dall-E, ChatGPT, and Bard. The most popular out of the three would arguably be ChatGPT, as it has gained traction in the popular media and is commonly used by the average person. So the question we must ask ourselves is…*How can AI Enhance a Keylogger?* Well for starters, an LLM can easily construct code for a functional keylogger. This means that anybody with the access to an LLM such as ChatGpt would be able to create a keylogger with zero computer programming experience. Furthermore, it can make keyloggers with polymorphic behavior that is abnormal for any normal threat actor using a keylogger. This would help the threat actor avoid detection. AI Can also execute attacks using a keylogger at remarkable speeds. A good example of this is *WormChatGPT and BlackMamba*. WormGPT is basically a modified version of ChatGPT. They took this LLM and created their own version of it. They stripped it of all of the ethnic controls that the original ChatGPT had in place, which means it can be used for nefarious purposes. WormGPT is mainly used for phishing attacks, where the AI can construct a convincing email for the attacker to use. The platform has a 109 dollar subscription, which means anyone with the financial means can use it and conduct various cyber attacks with no prior experience. Another example is BlackMamba. BlackMamba is a Poc (Proof of Concept) Malware that was developed to use AI to construct a keylogger with polymorphic behavior and the ability to resynthesis the code for various capabilities. BlackMamba can implement AI into the attack code at remarkable speeds. It uses AI-driven methods as well, such as being able to avoid detection, and identify what keystrokes are important and which are not.So, with these threats, what are the…*Future Implications*? AI is only going to continue advancing at an exponential rate akin to the natural growth of new technology. This brings about multiple dangers, such as the ability for AI to mimic real individuals, hindering our perception of what is reality or AI-rendered. These new tactics give AI more attack techniques, and give better tools to those who are inexperienced threat actors. These new abilities only spell disaster for the future impact of AI malware. This only proves that there is a great urgency to remain at the forefront of these new discoveries. Staying ahead of the curve will ensure that security remains intact for the digital landscape. Thank you.