Researchers create malware based on artificial intelligence

DeepLocker is unrecognized and 'performs malicious behavior as soon as this AI code detects the target via face detection, location or voice'.

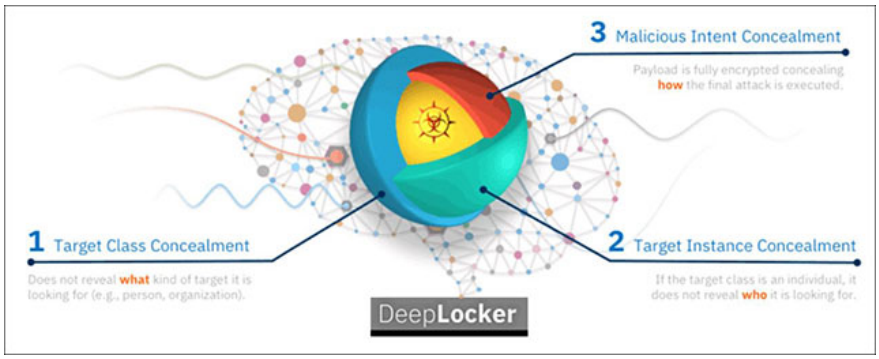
Artificial intelligence (AI) is still thought to be the potential solution for detecting malicious code, preventing attacks on the network before they seriously affect.

But it can also be used to support a new generation of malicious code to infiltrate the best security defense systems, poisoning even a computer system or attack only when the victim's face is camera identification.

To describe this scenario, researchers at IBM Research created DeepLocker - a new attack tool supported by AI, only revealing its purpose when it entered the victim device.According to the researchers, DeepLocker is not identified and 'performs malicious behavior as soon as this AI code detects the target via face detection, location or voice'.

Describing that this malicious code uses a spray and pray approach (targeting the whole group and attacking continuously instead of being carefully chosen) like traditional malware, researchers think it is very dangerous. Because it can affect millions of devices without being detected.

Malware can hide under many transmission applications (such as video calling) to avoid being detected by virus software until reaching the victim, through indicators such as voice recognition, face, location and other features at the device level.



DeepLocker does not perform behavior until he reaches the victim

'What's special about DeepLocker is that the use of AI creates' triggering conditions 'to perform attacks that are almost impossible to reverse engineer,' the researchers explained.'Malware will only unlock when approaching

the victim'.

To describe DeepLocker's ability, the researchers created cloaked simulations for the famous extortion code WannaCry in a video calling application without being detected by security tools.

When conditions are triggered, DeepLocker does not execute malicious code until it recognizes the victim's face, and can use the image.'When the victim sits on the computer and uses the application, the camera recognizes the face and the malicious code is executed by the victim's face, which is already programmed to open the attack'.

All that DeepLocker needs is just your photos, can be found in any of your social networking sites like Facebook, Instagram . Trustware has recently launched as an open source face recognition tool called Social Mapper, can be used to find victims on many social networks.

The IBM Research team will publish more details about DeepLocker at the upcoming Back Hat USA event.

See more:

1. Google's DeepMind can diagnose eye diseases exactly like doctors
2. Train AI with Ninja game do you want to try?
3. How can the AI ??see us behind the walls?