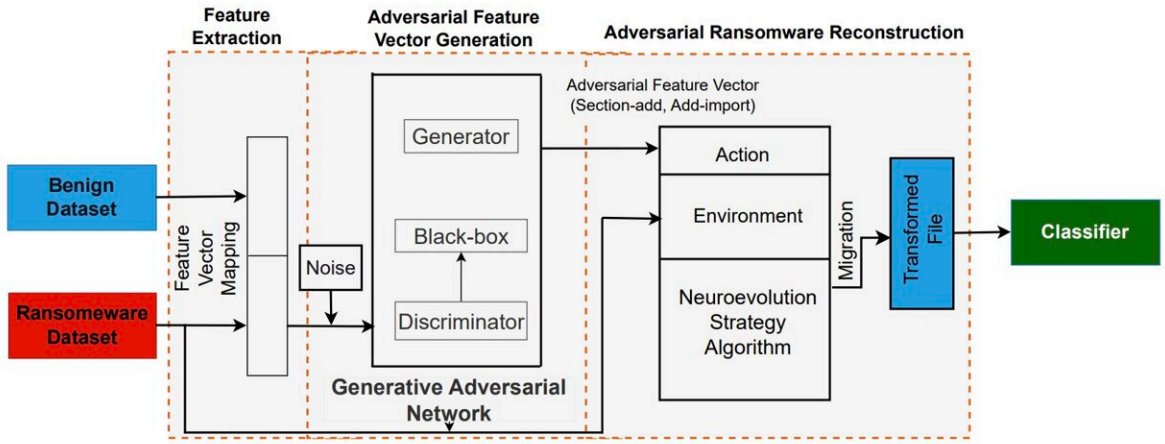
New ransomware attack based on an evolutional generative adversarial network can evade security measures

June 6 2024, by Ingrid Fadelli



Overview of EGAN, an Evolution GAN adversarial Ransomware Examples Generator. Credit: Commey et al.

In recent years, cyber attackers have become increasingly skilled at circumventing security measures and successfully targeting technology users. Developing effective methods to detect, neutralize or mitigate the impact of these attacks is of utmost importance.

Among the types of cyber-attacks that can cause significant damage to victims are those utilizing ransomware, malicious software that denies

users access to their accounts, websites or computer systems until they pay the attacker a specific sum of money. Some of these attacks can learn to evade security measures using generative adversarial networks (GANs), deep learning architectures that can improve their performance on a given task via trial and error.

GAN-based architectures consist of two artificial neural networks that compete against each other to generate increasingly "better" results on a specific task. In this instance, this could entail analyzing the features of malware that evaded security measures and becoming more skilled at designing this malware.

Researchers at Texas A&M University and Ho Technical University recently developed a new approach to produce adversarial ransomware samples, which they term evolution generative adversarial network (EGAN). This method was found to generate ransomware that could successfully evade numerous commercial AI-powered anti-virus solutions and malware detection methods.

The work is published in the *2023 IEEE 48th Conference on Local Computer Networks (LCN)*.

"Adversarial Training is a proven defense strategy against adversarial malware," Daniel Commey, Benjamin Appiah and their colleagues wrote in their paper. "However, generating adversarial malware samples for this type of training presents a challenge because the resulting adversarial malware needs to remain evasive and functional.

"This work proposes an attack framework, EGAN, to address this limitation. EGAN leverages an Evolution Strategy and Generative Adversarial Network to select a sequence of attack actions that can mutate a Ransomware file while preserving its original functionality."

EGAN, the framework developed by Commey, Appiah and their colleagues combines an evolution strategy (ES), an optimization method based on the concept of evolution, with a GAN. The ES agent in EGAN is placed in competition with an algorithm trained to classify ransomware, testing various functionality-preserving actions that can be applied to ransomware samples.

"The approach identifies the most optimal sequence of actions that leads to misclassification for each given ransomware sample," the researchers wrote in their paper. "If the ES agent's manipulations prove effective, a GAN is used to generate an adversarial feature vector that alters the ransomware file to appear benign."

Comey, Appiah and their colleagues evaluated their approach in a series of experiments and found that it enabled the generation of ransomware that successfully evaded many commercially available anti-virus and malware detection systems. These findings demonstrate the significant threat posed by adversarial ransomware, highlighting the need to develop stronger security measures that are better at preventing these attacks.

"We tested this framework on popular AI-powered commercial antivirus systems listed on VirusTotal and demonstrated that our framework is capable of bypassing the majority of these systems," Commey, Appiah and their colleagues wrote in their paper.

"Moreover, we evaluated whether the EGAN attack framework can evade other commercial non-AI antivirus solutions. Our results indicate that the adversarial ransomware generated can increase the probability of evading some of them."

In the future, this recent work could inspire the development of new cyber-security techniques to protect computer systems against adversarial ransomware. Meanwhile, the researchers plan to continue

investigating the risks of adversarial malware.

"In future research, we plan to investigate other actions and additional structures of PE (portable executable) file exploitation that can evade dynamic analysis," the researchers concluded in their paper. "Our experimentation shows that the actions currently employed lack the robustness needed to evade dynamic analysis from the Cuckoo sandbox."

More information: Daniel Commey et al, EGAN: Evolutional GAN for Ransomware Evasion, *2023 IEEE 48th Conference on Local Computer Networks (LCN)* (2023). DOI: 10.1109/LCN58197.2023.10223320