RESEARCH NEWS

AI helps to detect cyberattacks on corporate networks

AMIDES Detects New Varieties of Cyberattacks

Cyberattacks have become a major risk for companies and other organizations. To prevent data theft, sabotage and extortion, many companies and government agencies are turning in response to Security Information and Event Management (SIEM) systems, which use detection rules, also known as signatures, to identify cyberattacks. However, researchers at the Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE have conducted extensive tests and concluded that it is easy for attackers to evade many signatures like these. AMIDES, a new open source system from Fraunhofer FKIE, is designed to help remedy the situation. It uses AI to identify attacks that traditional signatures miss.

The threat of cyberattacks and industrial espionage has risen further in 2024. According to a study by the Bitkom digital association, eight out of ten companies in Germany have fallen victim to data theft and similar attacks. The damage done by network intrusions runs into the billions of euros. But the issue is that the nature of the attacks and the methods used to carry them out are constantly in flux, with attackers often making only minor changes to evade detection. The end result is that theft and tampering often go unnoticed until it is too late.

Open source system detects signature evasion through adaptive misuse detection

So far, detection of cyberattacks at organizations has been based primarily on signatures, written by security experts on the basis of known attacks. These signatures are the centerpiece of a SIEM system. However, researchers at Fraunhofer FKIE in Bonn have discovered that it is easy for attackers to circumvent many signatures of this kind. Though methods from a related area called anomaly detection can be used as an alternative to identify attacks in spite of signature evasions, this approach frequently yields large numbers of false alarms — so many, in fact, that not all of them can even be investigated. To solve this problem, the researchers at Fraunhofer FKIE set out to strike a practical balance, developing a system that relies on machine learning to identify attacks that are similar to existing signatures, but do not exactly match them. Their solution, Adaptive Misuse Detection System (AMIDES), utilizes supervised machine learning to identify potential rule evasions while at the same time minimizing false alarms. The freely available open source software (see link below) is aimed primarily at larger organizations that already have central security monitoring systems and structures in place and are now looking to improve them.

"Signatures are the most important way to detect cyberattacks in enterprise networks, but they are not a magic bullet," says Rafael Uetz, a researcher at Fraunhofer FKIE and the head of the Intrusion Detection and Analysis research group. "Malicious activity can often be carried out undetected by slightly modifying the attack. Adversaries use various techniques to disguise what they are doing and evade detection, such as inserting dummy characters into command lines. The attacker writes their command specifically so the signature doesn't find it," he says, explaining the tactics employed by cybercriminals. This is where AMIDES comes in: The software extracts features from security-related events, such as the command line of newly launched programs. Machine learning is then used to identify command lines that are similar to those matching the detection rules but are not matching exactly. AMIDES would trigger an alarm in this case. The authors call this approach adaptive misuse detection because it adapts to the target environment by first being trained in how the environment normally behaves so it can correctly tell potential attacks apart from harmless events.

Adaptive misuse detection permits rule attribution

Along with the option to initiate warnings of potential evasion, the new approach also offers a function the researchers are calling rule attribution. When a conventional rule is triggered to detect misuse, an analyst can simply display the rule to find out what has happened, as rules normally contain a meaningful title and a description in addition to the signatures. But many systems based on machine learning lack this advantage, instead merely generating a warning without further context. Since adaptive misuse detection learns from SIEM detection rules, information on which features are contained in which rules is available during training, allowing AMIDES to gauge which rules are likely to have been evaded.

AMIDES has already been evaluated through extensive testing using real-world data from a German government agency. Uetz comments: "These tests showed that our solution has the potential to significantly improve detection of network intrusions." Set to its default level of sensitivity, AMIDES succeeded in identifying 70 percent of evasion attempts — without triggering false alarms. As far as speed is concerned, the measurements show that the system is fast enough for live operation, even in very large enterprise networks.

AMIDES download link:

GitHub — fkie-cad/amides: An Adaptive Misuse Detection System

Fig. 1 Researchers at Fraunhofer FKIE have developed AMIDES, a solution with the potential to significantly improve detection of network intrusions.

© 123RF Galina Peshkova / skorzewiak