ESET Tech Center

Sandboxing technology in ESET LiveGuard Advanced

Mitch | ESET Nederland - 2022-11-29 - Comments (0) - Endpoint Solutions

Solution

Advanced persistent threats require a behavioral approach to detection – instead of trying to detect malware based on what it is (signature-based), behavioral malware detection relies on what the malware does. The deployment of a security sandbox in the organization’s network adds a layer of security to increase threat detection before executing in a live or production environment. The additional security layer is represented by ESET's Cloud-based Sandbox – ESET LiveGuard Advanced.

The network security sandbox is an isolated test environment. The system in this environment executes the suspicious program, observes its behavior, and then analyzes it in an automated manner. The network security sandbox blocks malicious samples based on their behavior before it runs on the endpoints.

The network security sandbox consists of multiple types of sensors that listen to network traffic containing active code. These sensors conduct static analysis of the code. The sandbox also includes a virtual execution environment for in-depth inspection of running samples that uses multiple detection methods including behavior-based detection, in-memory introspection, and extrapolation models powered by Machine learning. This approach is more efficient than just comparing the signatures of files. Sandboxing looks beyond the appearance of the binary. Because it observes what the file does, sandboxing is more conclusive in determining if the file is malicious than signature-based detection.

Analysis in the sandbox uses many of ESET’s internal tools for static and dynamic analysis, memory dumping, unpacking, and similarity matching. It evaluates the sample’s behavior and uses reputation data and threat intelligence feeds to increase detection accuracy.

Process of threat analysis

When a sample is sent to ESET LiveGuard Advanced, the process of threat analysis begins:

1. Three separate Machine learning models, including Deep Learning, compare the sample with millions of known malware samples for similarities.
2. The system executes the sample in a virtual environment or sandbox. It simulates user behavior to trick malware samples and uses Deep Learning neural network

models to compare sample behavior with the behavior of all known malware samples available.

3. The latest version of ESET's Award-winning scanning engine is used to take everything apart and analyze for anything unusual.
4. The final result is calculated based on all techniques available and provided to the customer.

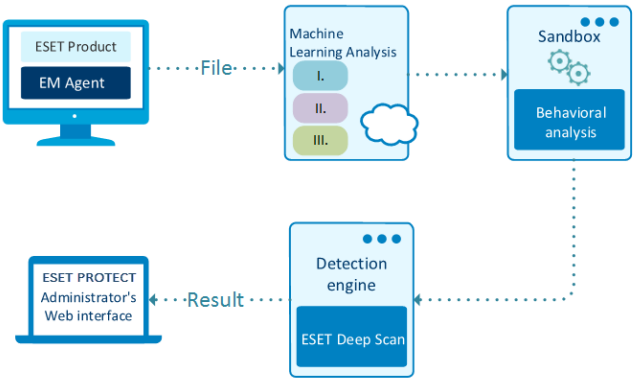

Figure 1-1
