EMAS – a solution to analyse binaries

The Europol Malware Analysis Solution (EMAS) is a dynamic, automated malware analysis solution, which executes malware samples submitted by European Union (EU) Member States (MS) in a tightly controlled sandbox environment.

The sandbox is used to simulate a host computer (similar to the one any regular user can have), as well as an attached local area network and, to some extent, Internet connectivity.

The concept

The EMAS focuses on the detection of all malware activities, including the network traffic that the malware causes (email, Peer To Peer (P2P) networks, network connections to Command & Control (C&C) centres as well as replication through network and network shares).

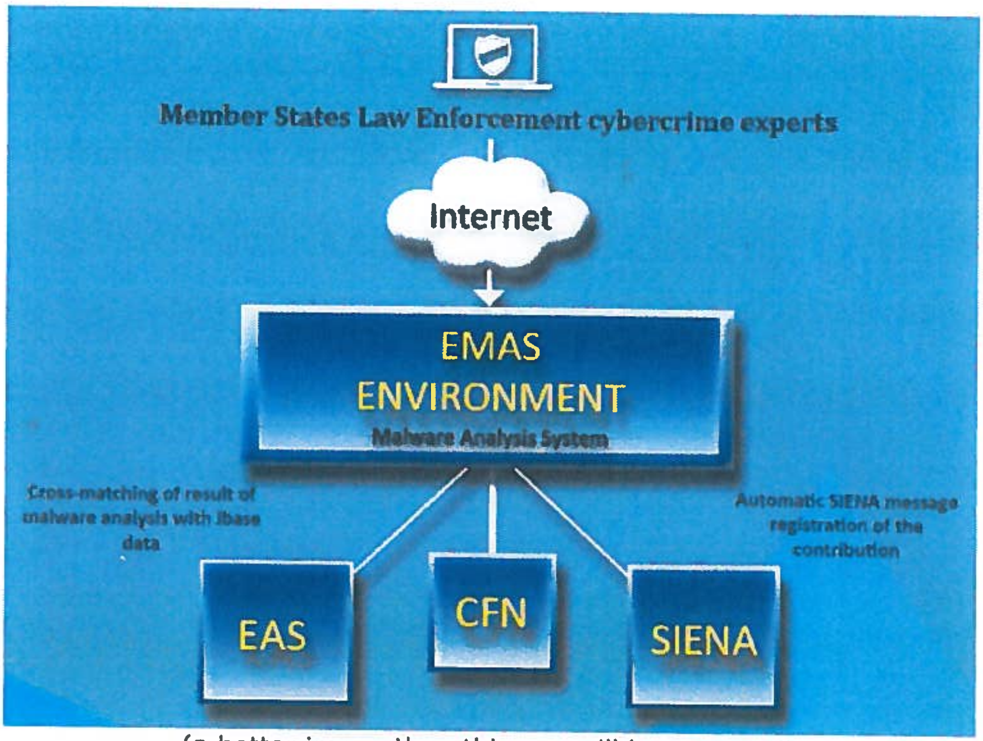
It provides a simulated environment to the sample under analysis that consists of custom-made versions of userland APIs (Application Programme Interface) necessary for the sample to execute. Various technologies are supported by the various solutions including the API hooking. It also implements measures to ensure its existence is not notified by the malware sample.

Special care is taken with respect to networking APIs. All networking requests issued by the sample under analysis are redirected to simulated components. If, for instance, a sample intends to spread itself via email, it has to contact an SMTP server to send that email. The connection attempt to TCP port 25 is detected, and instead of opening a connection to the real server, the connection is redirected to a simulated mail server.This is not noticeable for the sample under analysis, and it will start sending the mail commands including the malicious payload.

The information routing

The malicious files are submitted by the EU MS law enforcement agencies via the Europol's Large File Exchange solution (LFE). This malware contribution is then made official via SIENA message addressed to the Focal Point Cyborg, and therefore securely stored and dealt with according to the applicable handling codes.

Once the malware is received and analysed by the sandbox, reports containing the behaviour of the malware are created almost instantly and the results sent back to the countries who submitted the malware.


Member States Law Enforcement cybercrime experts
Internet
EMAS
ENVIRONMENT
Malware Analysis System
Cross-matching of result of malware analysis with Ibase data
Automatic SIENA message registration of the contribution
EAS
CFN
SIENA

(a better image than this one will be prepared)

The added value

The power of EMAS is not only the possibility of creating analysis reports. Its revolutionary feature resides in the production of intelligence for police investigators.

All the information received is stored in a central database. The automated cross-checks can unveil links between attacks performed in different countries with the same malware, or with the same criminal organisation behind the same malware family, connecting to the same domains and related to different investigations within the EU and beyond.

The future

The solution is dynamic and evolving so new functionalities can be constantly introduced. EMAS 2.0 will become available to the law enforcement cyber investigators by the end of the year. This will allow them to upload malware samples and receive the results directly via internet, with SIENA messages created in the backend.