Early Warning Intrusion Detection System (EWIS)

Overview

EWIS is a distributed global scoped Internet threat monitoring system with the potential of detecting large scale malicious events as early as possible; hence the name Early Warning Intrusion detection System (EWIS).

The system’s architecture includes a network of distributed low-interaction honeypots (sensors) and a central server.

The sensors are small computing units that, by design, are easy to deploy in a distributed fashion to a large number of partner organizations. They are preconfigured to be robust and secure and thus integrate non-intrusively to a network infrastructure. Each sensor collects network activity flows of potentially malicious intent from dark Internet address spaces and then relays this information to the central server.

The central server is hosted on high availability hardware for non-stop operation. It is a secured system with an efficient and scalable database, capable of storing hundreds of millions of records. In addition to the back-processing, the server hosts a user friendly visualization interface that provides several views of the collected data. Furthermore, a monitoring system monitors the health and availability of the sensors.

The system follows the design of a Network Telescope which similarly to a visual telescope, its resolution is relative to its size. As the number of deployed sensors grows, so does its resolution. EWIS’s resolution has been enhanced by deploying sensors to willing partner organizations.

Target Applications

Proactive cyber-security tools provide basic protection as today’s cyber-criminals utilize legitimate traffic to perform attacks and remain concealed quite often until it is too late. As critical resources, hidden behind layers of cyber-defenses, can still become compromised with potentially catastrophic consequences, it is of paramount significance to be able to identify cyber-attacks and prepare a proper defense as early as possible. Our vision was to establish a system that would be cost effective to implement, easy to deploy and provide us with sufficient data to create an Early Warning System that could potentially detect large scale events such as Worm(s) and Distributed Denial of Service (DDoS) attacks on a global scale.
Description

The deployed sensors continuously capture data from the dark space Internet addresses they have been assigned. As these addresses are not in use, any traffic reaching them is considered to be of exploiting and therefore malicious intent. The data flows captured are relayed to the central server on a timely basis via encrypted network tunnels. The server stores the sensors’ data to a local database in a way that it can be easily retrievable for analysis. The server provides several views of the collected data through a visualization interface accessible via http.

The visualization views provide quick access to:

- Historical packet traffic trends
- Top 10 style statistics that include source and destination IPs, source and destination ports, packet counts, packet historical trend, country of attack origin and time of attack
- Protocol breakdown statistics
- Backscatter traffic trends

The next phase of the project will include a more advanced visualization framework as well as automated procedures that will be able to correlate past and present data providing faster results with less human interaction.

Additional Information

The current deployment of EWIS consists of seven sensors that have been installed to an assortment of organizations ranging from small to large and from government operated to public sector. This implementation has helped create a functional framework for a globally scoped Network Telescope that could scale beyond our national borders. Organizations willing to host a sensor will help expand EWIS’s resolution and at the same time gain an aggregate view of Internet traffic across their operational boundaries.

Contact details: Ioannis Askoxylakis
cert@forthcert.gr
www.forthcert.gr