Early Warning Intrusion Detection System

Panos Chatziadam, Ioannis G. Askoxylakis, Nikolaos E. Petroulakis,
and Alexandros G. Fragkiadakis

FORTHcert, Institute of Computer Science
Foundation for Research & Technology – Hellas (FORTH)
{panosc,asko,npetro,alfrag}@ics.forth.gr

1 Introduction

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

The system's architecture includes a network of distributed low-interaction sensors and a central server [1]. The sensors are small computing platforms [2] 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 for logging and further analysis.

The system follows the design of a Network Telescope [3] 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 is further enhanced by deploying sensors to willing partner organizations.

2 Motivation

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.

While traditional Honeypots can provide extensive information regarding an attack, they lack the ability of observing large scale events. 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 [4] on a global scale.

Furthermore, a globally scoped Network Telescope augmented by partner organization hosted sensors will expand EWIS's resolution beyond our national borders, providing an aggregate view of Internet traffic across operational boundaries.

T. Holz and S. Ioannidis (Eds.): TRUST 2014, LNCS 8564, pp. 222–223, 2014.

3 Approach

The deployed sensors continuously capture data from dark space Internet addresses spaces. 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. A visualization interface provides several views of the collected data such as Historical packet traffic trends, Top 10 style statistics [Fig. 1], Protocol breakdown statistics and Backscatter traffic trends. Subsequent phases of the project will encompass a more advanced visualization framework, automated detection procedures, as well as the possible integration of wireless intrusion detection sensors [5] [6].

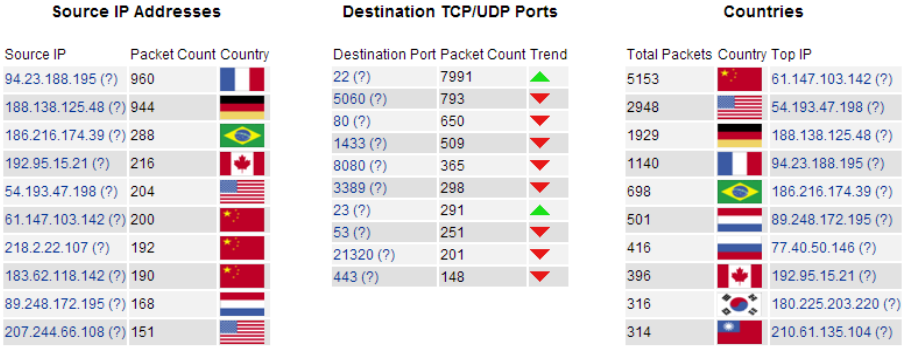

Fig. 1. Top 10 style statistics captured by an EWIS sensor

Acknowledgement. EWIS has been largely influenced by project NOAH.

References

1. Chatziadam, P., Askoxylakis, I., Fragkiadakis, A.: A Network Telescope for Early Warning Intrusion Detection. In: Proc. of the 2nd International Conference on Human Aspects of Information Security, Privacy and Trust, Heraklion, Greece, June 22-27 (2014)
2. Akram, R.N., Markantonakis, K., Mayes, K.: User centric security model for tamper-resistant devices. In: Proceedings - 2011 8th IEEE International Conference on e-Business Engineering, ICEBE 2011, pp. 168–177 (2011)
3. Irwin, B.: A framework for the application of network telescope sensors in a global IP network (January 2011), `http://eprints.ru.ac.za/2557/` (retrieved)
4. Spyridopoulos, T., Karanikas, G., Tryfonas, T., Oikonomou, G.: A game theoretic defence framework against DoS/DDoS cyber attacks. Computers & Security 38, 39–50 (2013)
5. Fragkiadakis, A.G., Tragos, E.Z., Tryfonas, T., Askoxylakis, I.G.: Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype. EURASIP Journal on Wireless Communications and Networking 2012(1), 73 (2012)
6. Fragkiadakis, A.G., Siris, V.A., Petroulakis, N.E., Traganitis, A.: Anomaly-based Intrusion Detection of Jamming Attacks, Local versus Collaborative Detection. In: Wiley Wireless Communications and Mobile Computing, pp. 1–19 (January 2013)