Chapter 2
Raptor:
Early Recognition and Elimination of Network Attacks

Slawomir Grzonkowski
Symantec, Ireland

Laurentiu Vasiliu
Peracton Ltd., Ireland

Adamantios Koumpis
National University of Ireland Galway, Ireland

ABSTRACT

The shift towards cyberspace created a very wide range of opportunities for various criminal activities, in both the real and the virtual world, such as identity theft, fraud, organized crime, and seriously organized crime, on an unprecedented scale. In this chapter, the authors propose a combination of integration activities for the best tools that help identify threats and security gaps for business and industrial users, for new analytical tools proposed to check if existing security features of the used networked structures are adequate and up-to-date and up-to-speed to address potential threat scenarios.

INTRODUCTION

The shift towards cyberspace created a very wide range of opportunities for various criminal activities, in both real and virtual world, such as identity theft, fraud, organized crime or seriously organized crime on an unprecedented scale. These activities are now easier than ever before and are much more efficient with the possibility of accessing the global scale from locations that are often beyond victim's jurisdictions. This is in particular critical for private and public organisations, as well as government agencies that are being exposed to new and pervasive threats that are hard to identify and contain. In the same time at every second, massive volumes of real time new data are being created worldwide. In order to process such data efficiently in an attempt to identify vulnerabilities and threats, robust analytics platforms capable of handling such volumes and complexities are required.

In this respect, this chapter presents a combination of integration activities for:

DOI: 10.4018/978-1-4666-6324-4.ch002

- Best of breed tools that helps identify threats and subsequently the relevant security gaps for business and industrial users that connect to new networks and thus exposing their systems to potential new entry points for cyber-attacks.
- New and innovative analytical tools proposed to check if existing security features of the networked structures used are adequate, up-to-date and up-to-speed to address potential threat scenarios.

The chapter concludes by testing and validating the chosen approach, developing conclusions and recommendations for best practice guidelines and policy actions to better protect European critical information infrastructure in five pilot case studies for

1. E-Government,
2. SMEs,
3. Financial industry,
4. Telecommunications, and
5. Power utility and energy providers.

It also introduces a standardized five level warning system proposal for detecting, managing and eliminating threats. This five level warning system proposal could be suitable for commercial exploitation to both EU and USA customers and aims to comply with the EU initiative on Critical Information Infrastructures Protection.

The proposed RAPTOR system architecture targets as end users IT financial/business networks, private, hybrid, public and government clouds, national electricity grids, industrial power facilities, financial organisations, telecom providers and strategic defence networks objectives.

The analytic tools covered are aimed to execute security checks in any network environment and able to go beyond computers line, down to PLCs (Programmable Logic Controllers) that are used for automation of electro-mechanical processes as well as critical mission servers used in Finance and eGoverment.

This may constitute a clear differentiation from other existing approaches and products currently offered in the market, and will help determine a much wider range of vulnerabilities and not only infect and disable the first line of computers but infect and disable a second line of servers and computers for industrial control with the ultimate goal to hamper and defect core applications in eGovernment, Finance and Power Industry.

RAPTOR tools are designed to scan the targeted networks within eGov / Finance / PowerGrid / Telecom organisations, will extract required data, process it, rank threats/vulnerabilities and then produce warnings, alerts and recommendations. RAPTOR aims to integrate best of breed tools that will help industrial users identify the relevant security features in case of linking their activities to new networks and thus exposing their systems to potential new entry points for cyber-attacks while also checking if existing security features of the already deployed networked structures are adequate, up-to-date and up-to-speed to address potential threat scenarios. As such, we employ the MAARS platform of Peracton Ltd. Ireland (www.peracton.com), where various data management approaches, analytics tools and methods can address the requirements of various threats, crimes, cyber-crimes, serious organized crimes and terrorism.

More specifically, the MAARS (Multi Attribute Analysis Ranking System) platform is a smart analytics recommendation and back-testing platform that allows ranking any entity that can be described by any number of attributes. This is done in a stable and consistent manner, based on any individual search criteria. The power of MAARS allows complex, high volume calculations to determine which results best suit a particular search profile with a simple click of a button and convenience of repeating this evaluation as often as they want. Further, results can be back-tested inside MAARS using historic data. MAARS has been matured and validated within Finance Industry, where it ranks any type of equities for any type of investment profile. However,