Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales
Departamento de Computación

Analyzing Windows Telemetry component

Tesis de Licenciatura en Ciencias de la Computación

Pablo Agustín Artuso
LU: 282/11
artusopablo@gmail.com

Director: Rodolfo Baader <rbaader@dc.uba.ar>
Codirector: Aleksandar Milenkoski <amilenkoski@ernw.de>

Buenos Aires, 2018

Abstract (english version)

Abstract (spanish version)

Greetings

Motivation

Table of content

Introduction

Explain that this study was carried out in a particular version of windows (1607) 64 bits Enterprise, which lacked of different things (for instance: documentation for different events)

Basic concepts

Reverse Engineering

Key concepts about what RE means, from a general perspective, how it should tackled which tools are usually there. 64 bits, calling convention ..

Debugging

Explaniation of the concept of debugging, what is the different with doing static RE. Some words specifically for KERNEL debugging.

Tools

IDA pro

Introduction to IDA pro. Explaniation of what it is and how it works.

WinDBG

Introduction to WINDBG pro. Explaniation of what it is and how it works.

YARA ?

XPERF?

Windows components

Event Tracing for Windows

Complete explainiation of how it works due to its importance for the rest of the analysis. Different components: session, providers, consumers ,etc .

Telemetry

Full description of the different features / characteristic which are involved in this analysis. Explaniation of how the worflow of the data is followed.

Previous Work

Some lines about previous works in this topic. Most of them focused on just analysis from traffic / documentation.

Analysis

Specifying the goals we want to achieve and how to get them.

Understanding how Telemtry makes use of ETW

How ETW works internally: Functions that are being called,

When and how providers are registered

How writes are carried out

Relation between ETW session and ETW providers

Identifying the buffers

Provider GUID vs Group Provider GUID

Checking correctness of logged events

Automatization of event logging

Service isolation

Triggers

searching for new triggers

YARA

Difference among configuration levels of telemtry

Analysis of sent data over the channel to Microsfot backend services

Results

Conclusions