Report on Duqu: A collection of computer Malware

Aril Johannes Schultzen

September 8, 2015

Contents

Abstract

This report on Duqu (a collection of computer malware) was an assignment given in the course UNIK4740. It is mainly based on *Duqu: A Stuxnet-like malware found in the wild.* by Boldizsár Bencsáth et al (October 2011) and *W32.Duqu: The precursor to the next Stuxnet* by Symantec (November 2011).

1 Introduction

2 Prerequisite knowledge

Though not a technical marvel, Duqu exploits numerous mechanisms and features in the Winodws Operating system. Some of these mechanisms will be explained in this section and should be understood before venturing further into this report.

2.1 DLL

A DLL (Dynamic Link Libraries) is Microsoft's implementation of the *shared library* concept used in both Windows and the OS/2 operating system. It can contain both code and data and shares it's file format with the Windows Executable file (EXE). A DLL can be used by multiple programs at the same time. The idea is that it promotes reuse of code while achieving higher memory efficiency. WHY VULNERABLE?

2.2 Drivers

A Driver (also known as Device driver) an abstraction layer that provides a software interface to the hardware. A driver can either be written in kernel mode or user mode. When running in kernel mode, the driver has access to every resource and all hardware, this also means that every CPU instruction can be executed and every memory address can accessed. An application written in user-mode can not directly access hardware or memory but has to use APIs instead. This isolation makes a crash in user-mode recoverable instead of catastrophic as in a kernel-mode. WHY VULNERABLE?

2.3 The Windows registry

The registry is a database used in Microsoft Windows to store settings and options. It can be considered an alternative to the use of INI files. The use of the registry is not compulsory.

2.4 RPC

Remote Procedure Calls (RPC) is a system that allows programmers to write distributed software without worrying about the underlying network code. It is most often used to create a server/client model. [1]

2.5 Code-signing

3 Injection

Show list of trusted processes. Usually anti-virus.

Complete Bibliography

[1] Microsoft TechNet. *What Is RPC.* https://technet.microsoft.com/
en-us/library/cc787851.aspx. Accessed: 8-09-2015.