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.*[1] by Boldizsár Bencsáth et al (October 2011) and *W32.Duqu: The precursor to the next Stuxnet*[3] by Symantec (November 2011).

1 Introduction

Duqu is a collection of malware discovered by The Laboratory of Cryptography and System Security (CrySyS) of the Budapest University of Technology and Economics in Hungary. They analyzed it and named it Duqu from the prefix " DQ" that the key logger use to name its files. It is an interesting piece of code despite it being anything but technically astonishing. It is however interesting because of its similarities with *Stuxnet* and *Stuxnets* modular design and how these modules combined can be used to create a targeted thread to control systems in nuclear facilities. It is believed that the creator(s) of Duqu also created *Stuxnet* or at least had access to *Stuxnets* source code.

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. [4]

3 Installation

In one of the most discussed examples oh Duqu installation, Duqu was delivered to the target by using a malformed Microsoft Word document. The Word document contained an exploit in the Win32k TrueType font parsing engine which allowed arbitrary code to run in kernel mode. According to Microsoft the Duqu malware exploits a problem in T2EMBED.DLL which is called by the TrueType font parsing engine in some cases.[2] Once the Word document is opened and the exploit triggered, the code will do a check to determine whether or not the target has been infected. This is done by checking the registry for the following value:

```
HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows\
   CurrentVersion\Internet Settings\Zones\4\"CF1D"
```

Unless the value is found, indicating that the computer is compromised, the code decrypts two files from the Word document:

1. jminet7.sys or cmi4432.sys, both drivers.
2. netp191.pnf or cmi4432.pnf, both DLLs.

The code then executes the driver file which injects code into services.exe. This behavior is defined by the config file (either netp192.pnf or cmi4464.pnf respectively). Before it exits completely, the code wipes itself from memory by overwriting itself with zeroes.

Complete Bibliography

[1] Boldizsár Bencsáth et al. *Duqu: A Stuxnet-like malware found in the wild*. Report. Accessed: 7-9-2015. Budapest University of Technology and Economics: Department of Telecommunications.

[2] Ryan Naraine. *Microsoft issues temporary 'fix-it' for Duqu zero-day*. `http://www.zdnet.com/article/microsoft-issues-temporary-fix-it-for-duqu-zero-day/`. Accessed: 8-09-2015.

[3] Symantec. *W32.Duqu: The precursor to the next Stuxnet*. Report. Accessed: 8-9-2015. Symantec Security Response.

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