

Lab 10: Malware Command and Control - Part 2

ITSC 303: Malware Analysis

Table of Contents

[Lab Outcome 2](#_Toc492040039)

[Background Reading 2](#_Toc492040040)

[Introduction 2](#_Toc492040041)

[1.0 Dridex Loader: C2 Encryption Overview and Extraction 3](#_Toc492040042)

[2.0 Sign-Off: Lab 10 – Malware Command and Control Part 2 6](#_Toc492040043)

[References 7](#_Toc492040044)

Malware Analysis

Lab 10: Malware Command and Control - Part 2

Lab Outcome

This lab will focus on the following outcome:

* Analysis of command and control obfuscation mechanisms.

Background Reading

* [Threat Spotlight: Spam Served With a Side of Dridex](https://blogs.cisco.com/security/talos/spam-dridex) (https://blogs.cisco.com/security/talos/spam-dridex)

Introduction

In this part of the lab, you will delve deeper into the command and control obfuscation mechanisms that are used by malware authors to bypass security mechanisms and make analysis more difficult for reverse engineers. You will review an encryption mechanism used by a Dridex loader binary and you will be tasked with decrypting your own captured packet capture based on its implementation.

1. Dridex Loader: C2 Encryption Overview and Extraction

Dridex is a popular banking Trojan variant that has been distributed in a wide array of spam campaigns. A loader is typically delivered via malicious Word document macros, which makes a number of command and control connections containing system fingerprint data. This data is encrypted using a 4-byte XOR key (shown in the blue rectangle in Figure 1) that is generated randomly at run-time and which is then appended to the encrypted body of information (shown in the red rectangle in Figure 1).

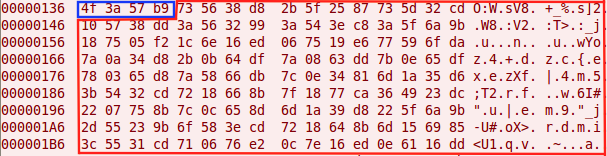


Figure 1: Packet Capture of Dridex Loader Communications

Source: Wireshark, 2016. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Using the analysis environment set up in the previous lab, start INetSim to receive HTTP requests.
2. Begin a packet capture using Wireshark.
3. Run the supplied Dridex loader sample.

You see a connection to 92.63.88.83.

1. Right-click the TCP connection and select **Follow TCP Stream**.

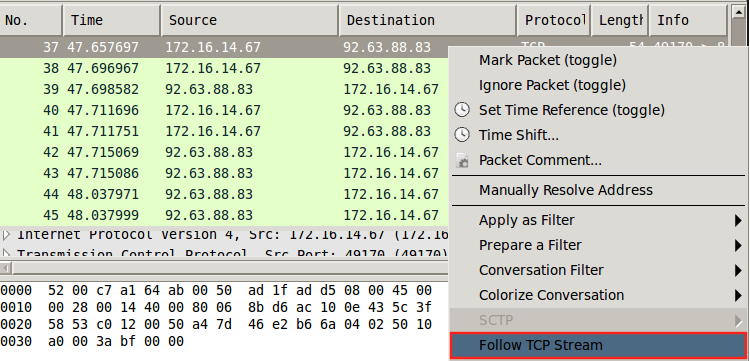


Figure 2: Follow TCP Stream

Source: Wireshark, 2016. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

The Wireshark recorded connection is isolated to only those related to this particular TCP stream. The stream content is displayed.

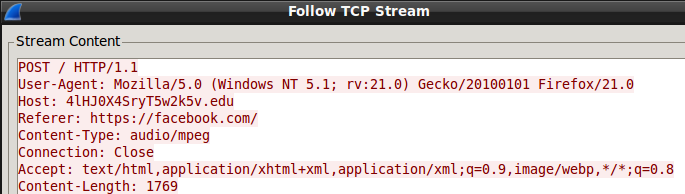


Figure 3: Follow TCP Stream Data

Source: Wireshark, 2016. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Go back to the previous Window and select the POST request from the isolated stream. .Assads ads sad awes cash ag egad
2. Right-click the **Media Type** section from the analyzed HTTP stream and select **Export Selected Packet Bytes** to save the bytes in a binary format.

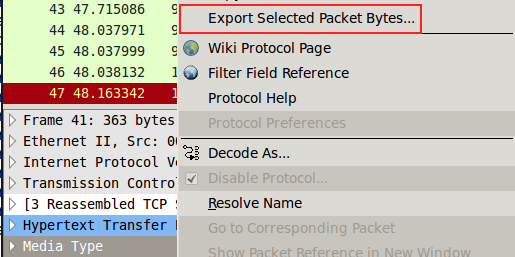


Figure 4: HTTP Media Type Export Selected Packet Bytes

Source: Wireshark, 2016. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Each byte of the XOR key is used to encrypt each respective byte. Key bytes are not repeatedly applied to the same byte, for example:

DE AD BE EF

⊕ ⊕ ⊕ ⊕

AA BB CC DD

---------------------

73 22 72 32

1. Using the data that you dumped to disk using Wireshark, write a program in the language of your choosing to decrypt the data sent in the body of the HTTP POST.

Ensure that your program has the ability to decrypt any stream produced by Dridex, and not just the one you dumped to disk.

KEY: A solution is provided with lab contents.

1. Sign-Off: Lab 10 – Malware Command and Control Part 2

Detach this page and submit it to your instructor.

Name:

Student ID:

|  |  |
| --- | --- |
| **Item** | **Initial** |
| Dridex Traffic Decrypter |  |

# References

Combs, G. (2016). Wireshark [Computer software]. Retrieved from https://www.wireshark.org/.