Challenge Questions:

*Analyse the network components of the Dridex Malware*

*Important Note:*

*The data in this document is Copyright 2016 of Lloyds Banking Group. Please do not share this document or the data linked on this page with others. Some of the indicators of compromise such as IP addresses in this challenge could still be linked to active malware campaigns, and, in order to complete this challenge you are not required to connect to the IP addresses. Some of the information has been anonymised and associated traffic is fictional.*

Contents

[Overview 3](#_Toc468716681)

[Question 1 3](#_Toc468716682)

[Question 2 3](#_Toc468716683)

[Question 3 3](#_Toc468716684)

[Question 4 3](#_Toc468716685)

[Question 5 4](#_Toc468716686)

[Question 6 4](#_Toc468716687)

[Question 7 4](#_Toc468716688)

# Overview

Lloyds Banking Group has received intelligence from a reliable source that one of our external IP addresses are communicating to a Command & Control server associated with the Dridex malware. Your team has been tasked to analyse the Dridex malware and write an analysis report that answers all the questions below with as much detail as possible. You have also been provided information that the malware usually communicates via HTTP GET and HTTP POST requests on port 8080.

# Question 1

One of your malware analysts in the team has indicated that the payload of the malware uses a URL pattern which can be easily identified.

**Which regular expression (regex) you could use to detect the Dridex URL requests?**

*http://IPADDRESS/NlYVW39lKAO6seE/6u7zh96QXizKqBibVlh/63075FSeb0aZCN6/B*

*http://IPADDRESS/gU4obiJ4cGtA11SqZsK/1tqnbAK3D/0H1vHcsJ1tYavtLjAM/tonGSBLOSyncvR0K24zWWmL6z5Ow6S6I*

*http://IPADDRESS/g3qhq4wdykAOCDsxYAmg6vqFt0SrMKe/FcFR1Pv7GRcOfYNQ7fvaND9mG/5PXS8*

# Question 2

You are provided a packet capture (pcap file) with sample network traffic of the Dridex malware. The malware analysts have told you that the first POST request from the host to the Command and Control (C&C) server is encoded using XOR with the HEX key 7D. (**Note**: the XOR encoded data includes partially encoded BASE64 contents, please **do not** attempt to decode the contents as it contains malware. The focus is on readable text after decoding with the XOR key).

**What text is send by the infected host to the C&C server when it communicates with the C&C server during the first HTTP POST request?**



# Question 3

The payload of the malware instructs the infected host to download a configuration file that contains information on which sites to 'target'. The malware analysts have told you that the configuration file is obscured by the C&C server by using a distorted gzip header. The malware analysts share that by replacing the first 4 bytes of the distorted data with the hex values "1f 8b 08 00", the gzip file can be restored. The configuration is send by the server during the last HTTP POST request visible in the pcap file.

**Which IP addresses are listed as 'bconnect' and 'vncconnect' values in the Dridex configuration file downloaded by the infected host?**

# Question 4

**What further indicators of compromise can you identify after reviewing the pcap file?**

# Question 5

**The Dridex configuration file contains an injectgate and tokengate URI. Explain how do you think these are used by the creators of malware?**

# Question 6

The following IP addresses illustrate fictional Dridex C&C IP addresses collected during malware analysis.

16.182.220.165

91.22.7.180

33.19.235.22

173.192.90.86

122.154.17.5

69.82.179.36

11.128.64.15

31.199.87.145

43.62.159.75

**Which IP addresses in the network traffic below could potentially identify the high level infrastructure of the botnet and the individuals controlling the C&C servers?**



# Question 7

**What are the top 10 infected hosts that transferred the most data with the C&C servers?**