## 实验简介：

实验所属系列： 数据安全

实验对象： 本科/专科信息安全专业

相关课程及专业： 计算机网络

实验时数（学分）：2学时

实验类别： 实践实验类

## **预备知识：**

关于wireshark的一些基础知识

      首先，wireshark不会像burp suite那样可以对数据包进行修改，它能做的只是监听网络流量信息并完整的记录下来。可以说，wireshark起到的是一个还原现场的作用。请记住，wireshark只是一个帮助你审计的工具，至于怎么去审计，只能靠自己去分析。

      其次，说说wireshark在安全方面的作用。Wiki上是这样描述的：对于安全人员而言，网络安全工程师可以使用wireshark来检查讯息安全相关的问题。对于网络安全而言，现场很重要，黑客攻击的过程和服务器被攻击的过程都必须使用网络，wireshark完全可以记录下来，这也正是wireshark强大的地方。

## **实验目的：**

通过该实验使用wireshark进行恶意流量分析，主要涉及知识点包括IOC，键盘记录器木马，ftp协议等。

## **实验环境：**

windows， wireshark

## **实验步骤一：**

场景

局域网段范围：10.0.0.0/24(10.0.0.0 到 10.0.0.255)

域： beguilesoft.com

域控：10.0.0.10 - BeguileSoft-DC

局域网网关：10.0.0.1

局域网广播地址：10.0.0.255

任务

分析现有的材料，针对受害的windows主机写一份应急报告。建议的模板如下：

总结:

        在xx时间, 一台window主机被xx感染

细节:

        IP address:

        MAC address:

        Host name:

        Windows user account name:

入侵指标IOC(Indicatorsof Compromised):

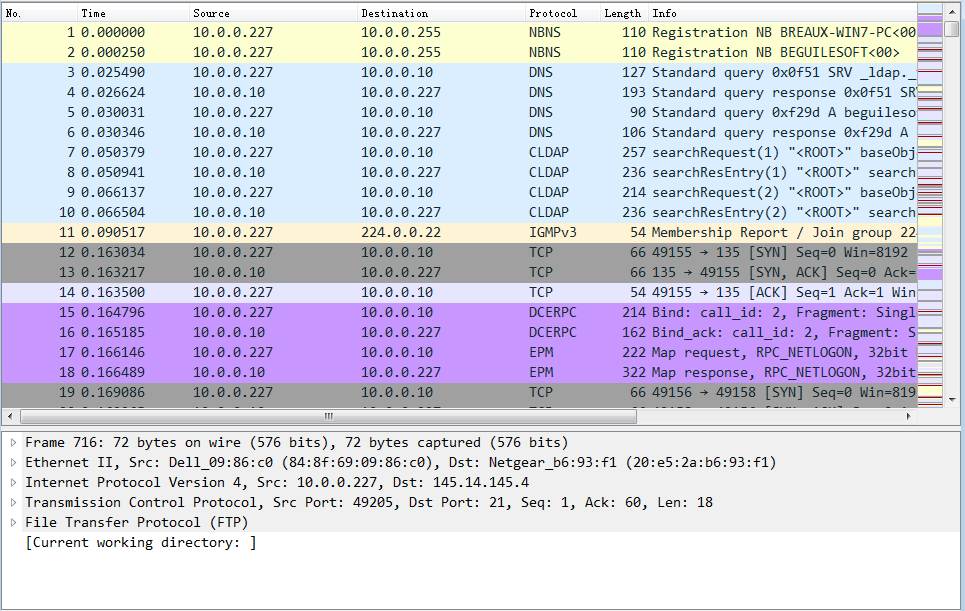
       [URLs, domains, IP addresses, andSHA256 hashes related to the infection should appear in this section]

 提供了两个压缩文件，分别是告警日志和数据包。解压后分别如下所示

IMG_256



      数据包打开如下所示



涉及到很多协议，现在还没有头绪，我们先来看看告警日志



      第一条是接收到whatismyaddress.com的请求，这不一定是恶意软件产生的流量

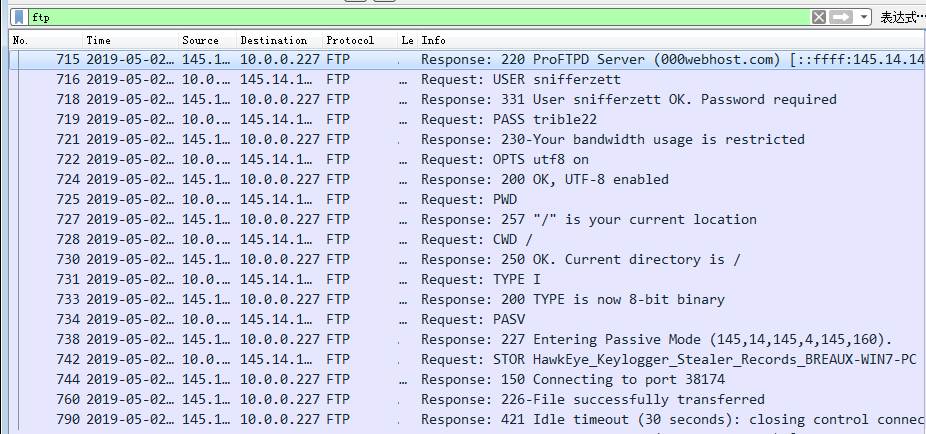
      第三条是使用到了ftp STOR,该命令用于存储文件到服务器上，这里提示是连接到外部网络，所以我们推测可能是恶意软件通过ftp协议将数据传输到其外网服务器上

      第四条可以看到日志提示我们这是一个名为Hawkeye Keylogger的木马

      通过搜索引擎在freebuf上有相关的分析文章：[https://www.freebuf.com/column/157857.html](https://www.freebuf.com/column/157857.html" \t "http://www.hetianlab.com/pages/teacher/_blank)

从文章中可以知道会涉及ftp协议，在告警日志中的第五条也可以看到ftp

      所以使用ftp过滤看看，如图所示

****

      可以看到ftp的第一条

**IMG_256**

      显示的是proftpd，这我们都知道是一款很常用的ftp服务端软件，可后面的000webhost.com是什么？

      进入其官网看看

<https://www.000webhost.com>

其实就是一家免费的虚拟主机商

      这样子的过滤其实还是有很多噪音，我们使用ftp常用的关键字来过滤吧，比如USER,PASS,STOR

      过滤命令如下

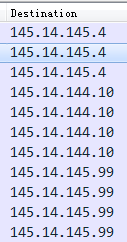
      ftp.request.command eq USER or ftp.request.command eq PASS or ftp.request.command eq STOR

      命令中or表示任一条件满足即可，eq是等于的意思，用于限定命令

      过滤后的结果如下所示



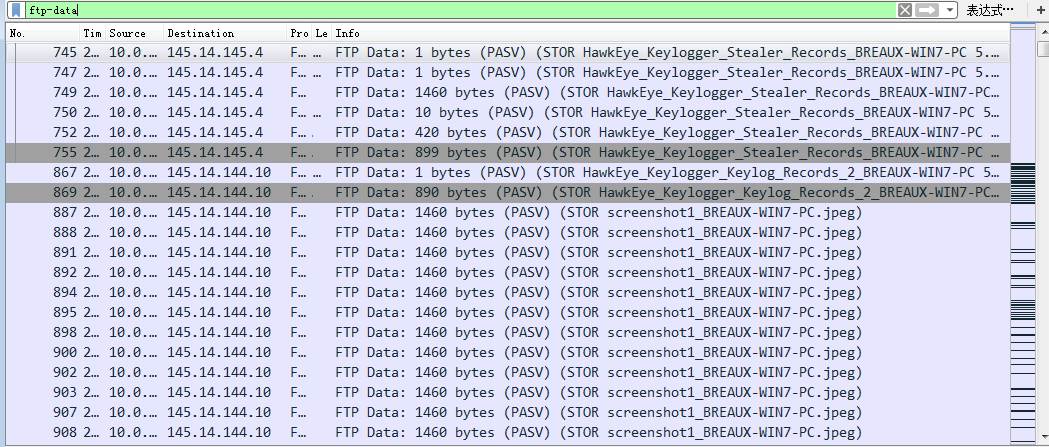
这里有一个比较奇怪的地方，就是外网的地址在变动

****

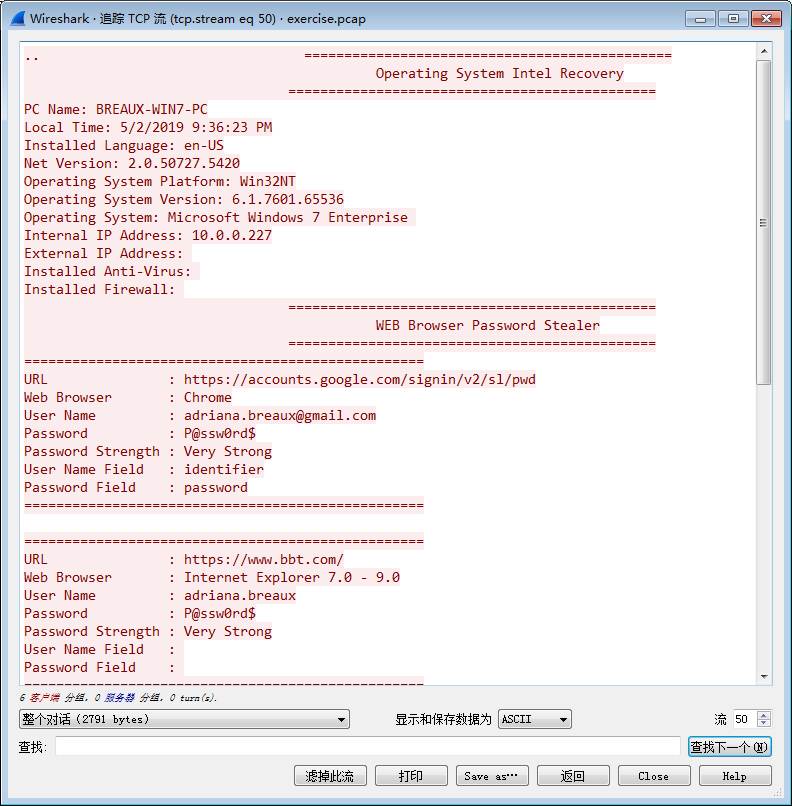
      这其实是因为攻击者用的是免费的虚拟主机，比如000webhost。如果更新页面或者传送数据则有可能会导致自动更换ip。

## 实验步骤二

      那么攻击者究竟拿到了什么数据呢？我们使用ftp-data看看他通过ftp传送了什么



以第一条为例跟踪tcp流

****

      可以看到系统信息被获取到了，包括：

      主机名：BREAUX-WIN7-PC

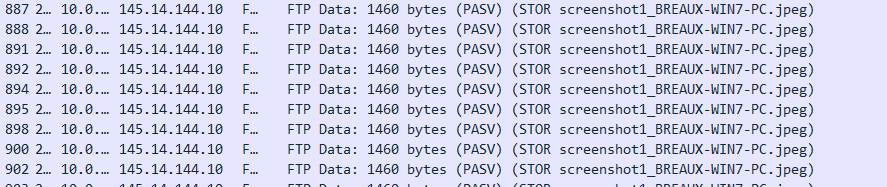
      用户名：Adriana.breaux

      MAC地址：84:8f:69:09:86:c0

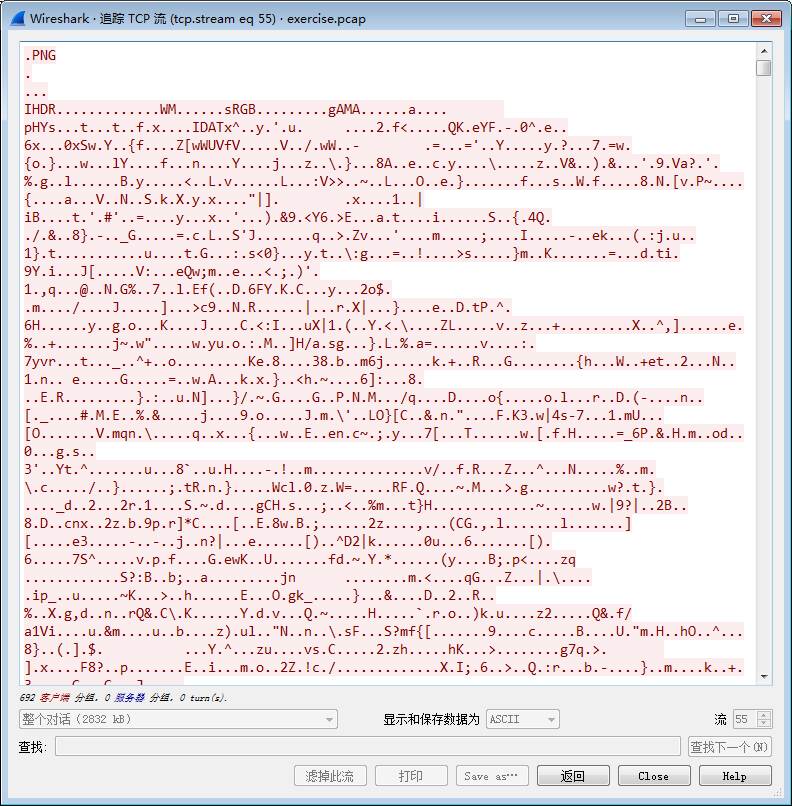
      Ip地址：10.0.0.227

      还有谷歌等网站的账号、密码都被攻击者获取到了

      我们注意到还有一部分的流量显示的是jpeg，推测可能是主机截屏的图片

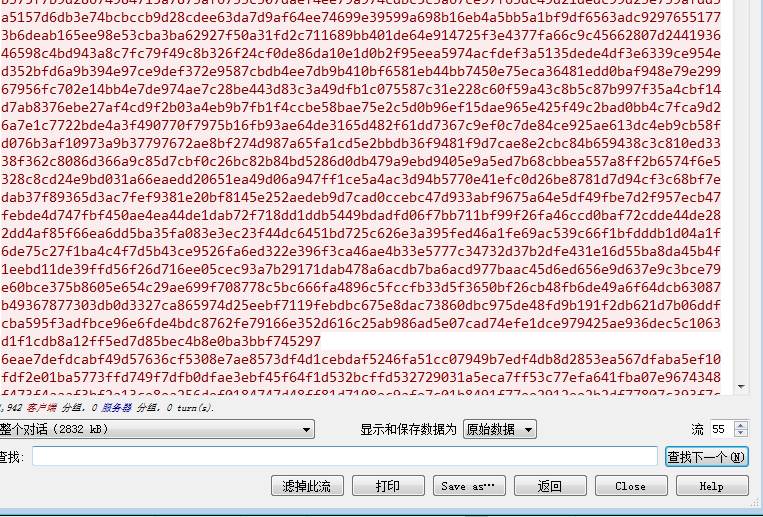
****

      选中一条，同样跟踪tcp流

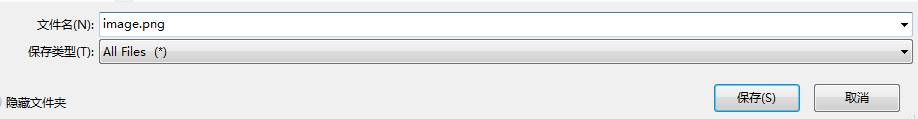
****

      从头部可以看到这其实是一个png的图片格式文件

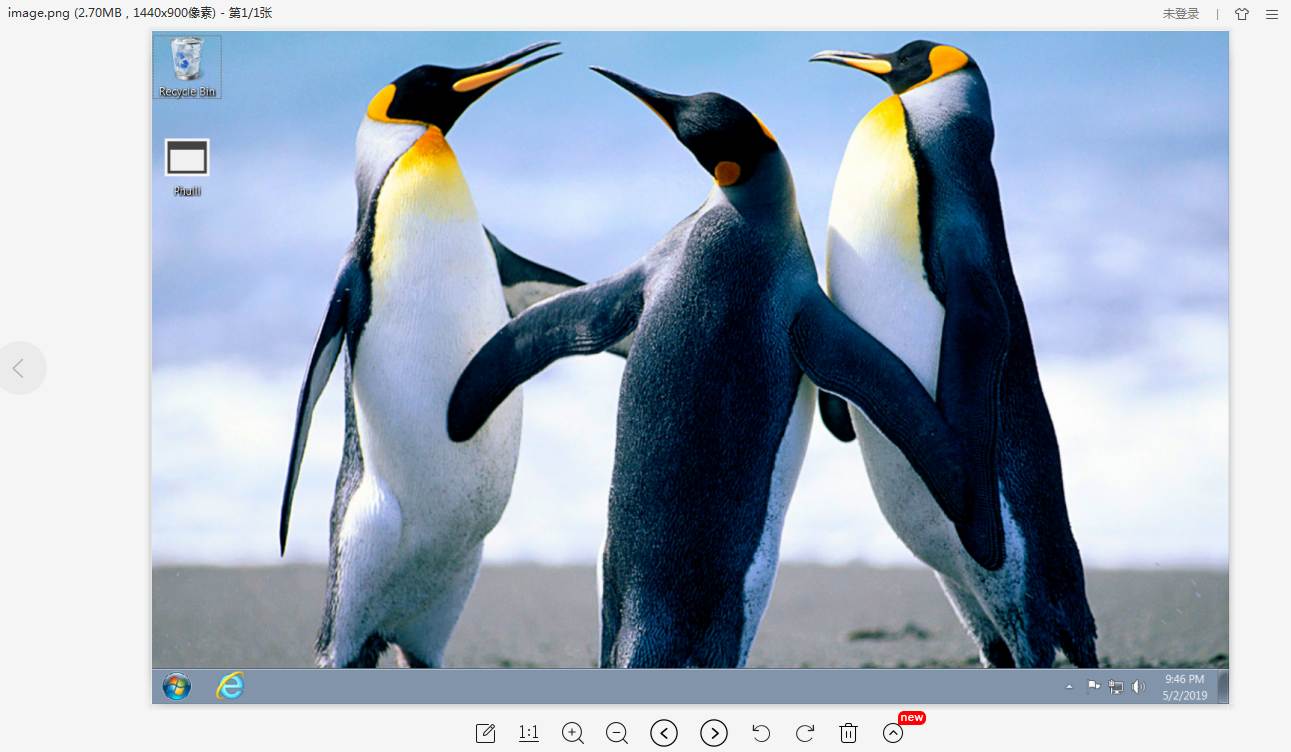
      选择：显示和保存为原始数据

****

      Save as...

****

      保存后打开如下所示

****

      可以看到确实是桌面截屏

## 实验步骤三

别忘了，我们还要写应急报告呢！

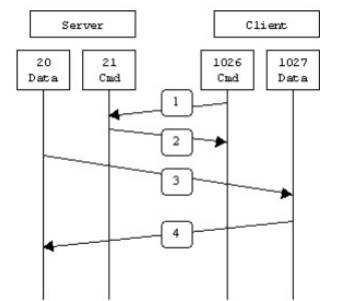
      现在还缺少IOC，所以我们需要整理下，需要整理出目标端口，ip等

      在这之前，我们需要先回顾下ftp协议，ftp协议用两个端口实现，分别是数据端口和命令端口。命令端口用于连接，数据端口用于传输数据。

      命令端口一般都是21。那么数据端口呢？

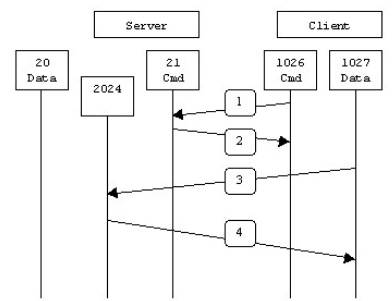
      这里又引入了主动模式（PORT）和被动模式（PASV）的概念。当客户端通知服务器它处于被动模式时才会启用，其标志就是客户端给服务端发送了一个PASV.

      主动模式：

****

      在第1步中，客户端的命令端口与FTP服务器的命令端口建立连接，并发送命令“PORT 1027”。然后在第2步中，FTP服务器给客户端的命令端口返回一个"ACK"。在第3步中，FTP服务器发起一个从它自己的数据端口（20）到客户端先前指定的数据端口（1027）的连接，最后客户端在第4步中给服务器端返回一个"ACK"。

      被动模式：

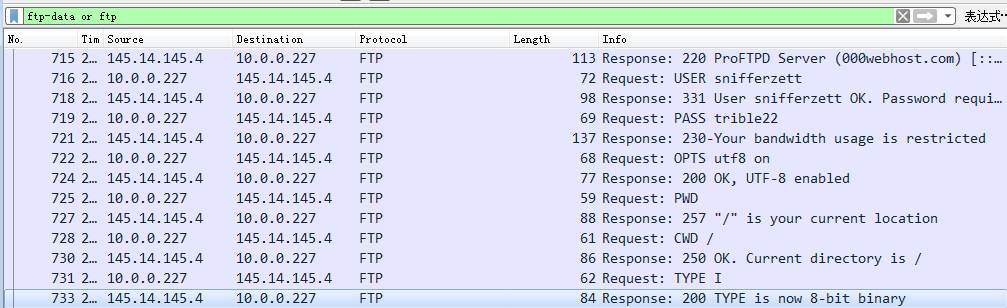
****

      在第1步中，客户端的命令端口与服务器的命令端口建立连接，并发送命令“PASV”。然后在第2步中，服务器返回命令"PORT 2024"，告诉客户端（服务器）用哪个端口侦听数据连接。在第3步中，客户端初始化一个从自己的数据端口到服务器端指定的数据端口的数据连接。最后服务器在第4 步中给客户端的数据端口返回一个"ACK"响应。

      简单地说，就是，在主动模式下一般默认的数据端口为20，在被动模式下数据端口就不一定了。

      接下来我们回到数据包中看看ftp过程中用到了哪些端口。

      这里要注意，在wireshark中要想把完整的ftp协议过滤出来需要使用 ftp-data or ftp,只用单个的话只能过滤出ftp命令端口的流量或数据端口的流量，是不完整的

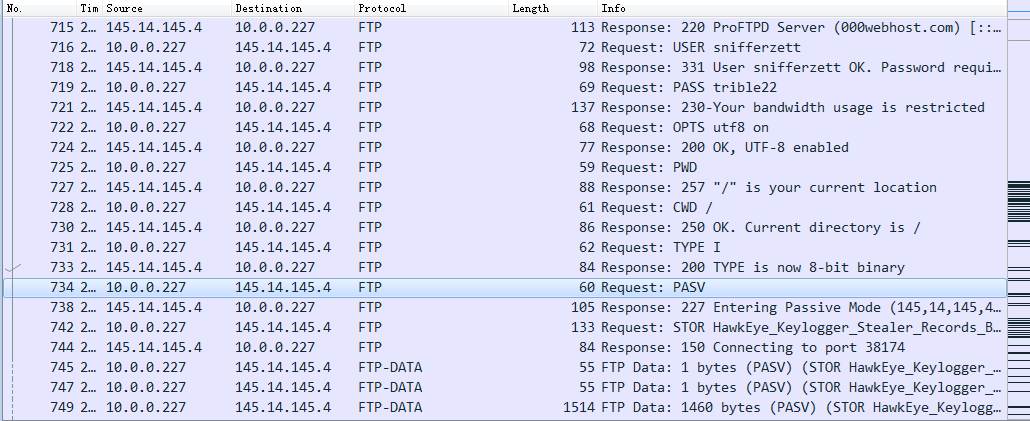
****

      先来看第一个外网ip：145.14.145.4

      715条的状态码220表示对新用户的服务已经准备好

      716,719可以看到受害者机器通过用户名密码连入ftp服务端

      一直到734条可以看到受害者机器向145.14.145.4发出PASV,前面提到，发出PASV,就说明后面的数据传输过程中服务端使用的端口就不是20了。

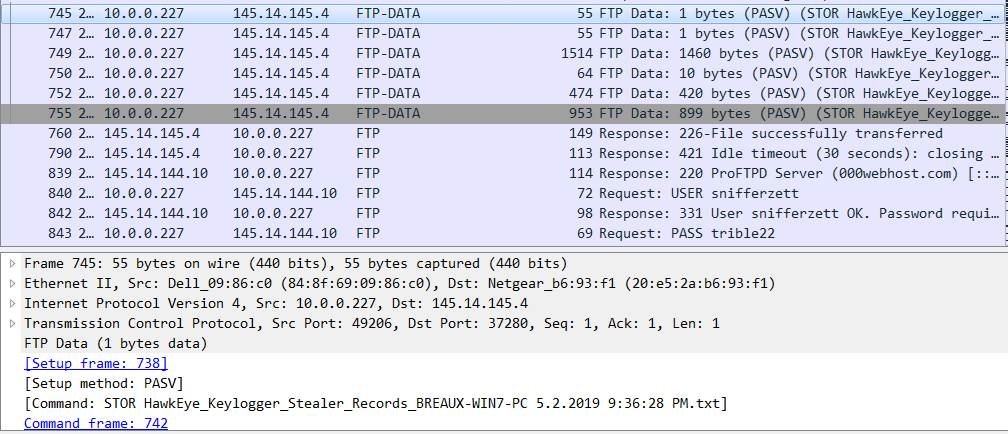
****

      在715到744之间都是命令端口通信的流量。

      所以此时的IOC是

      Ip:145.14.145.4  port:21  url:000.webhost.com

      745开始是通过被动模式连接后进行数据传输了

****

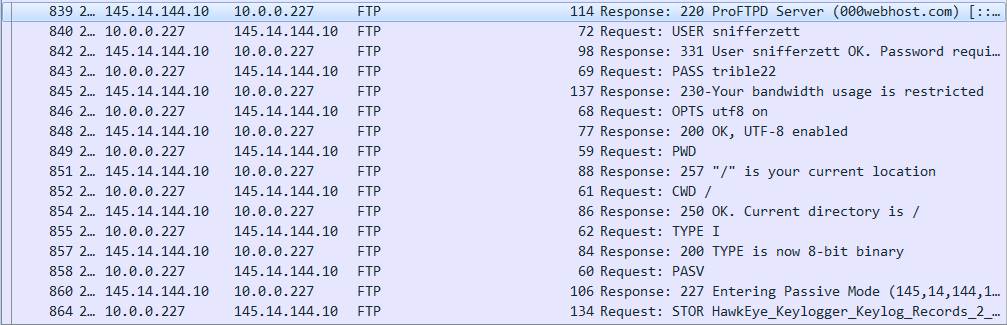
      以755为例，查看dst port为37280，即此时145.14.145.4使用的数据端口是37280

      所以第二条IOC为

      Ip:145.14.145.4  port:37280  url:000webhost.com

      第一个外网地址分析完了，接下来看第二个，145.14.144.10

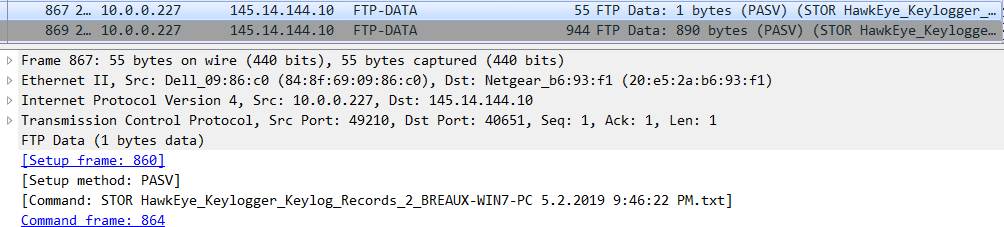
      从839开始

****

      看到858又是PASV，有了上次的基础，这次两条IOC就很简单地得出了：

      命令端口的通信流量Ip:145.14.144.10  port:21  000webhost.com

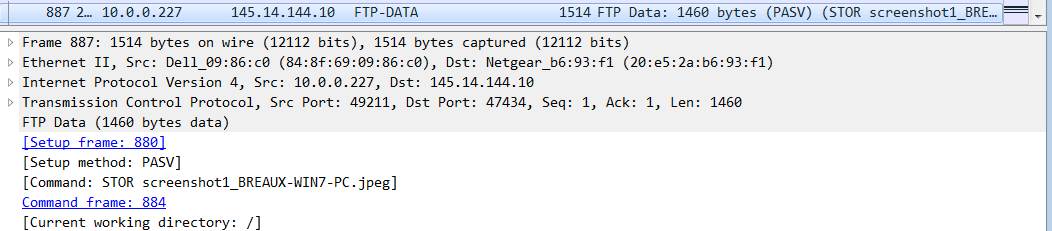
      数据端口的通信流量以867为例



      得到IOC:

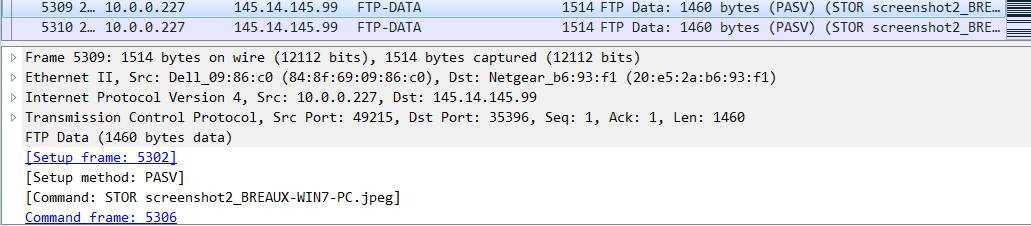
      Ip:145.14.144.10  port:40651  url:000webhost.com

      从887开始又一次建立数据传输，端口47434

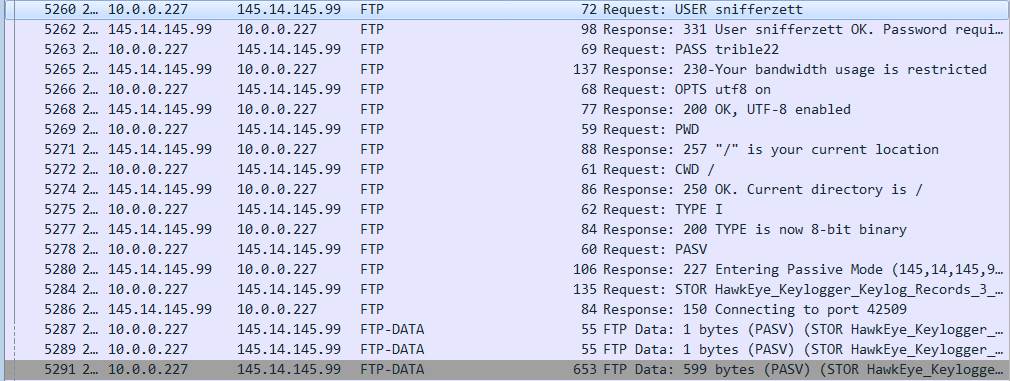
****

      所以IOC为：

      Ip:145.14.144.10  port:47434  url:000webhost.com

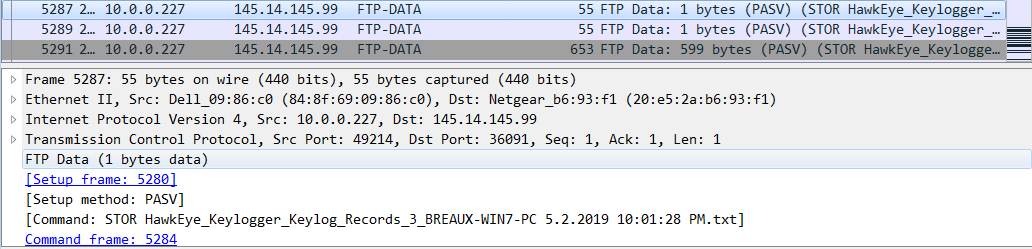
****

      然后看第三个外网ip145.14.145.99，从5260开始

****

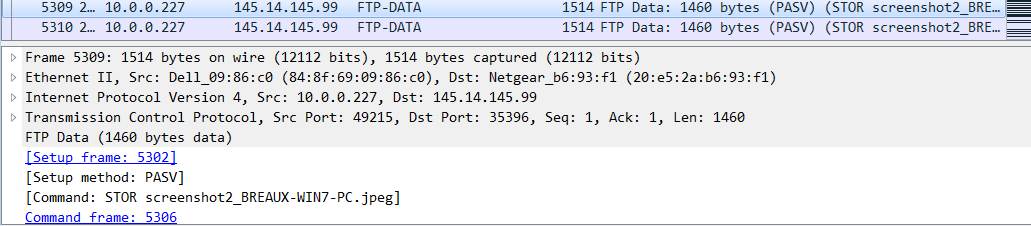
      同理可得两条IOC:

      Ip:145.14.145.99  port:21  url:000webhost.com

****

      Ip:145.14.145.99 port:36091 url:000webhost.com

      5309开始又建立了一次数据传输

****

      此时端口成了35396，所以IOC:

      Ip:145.14.145.99  port:35396  url:000webhost.com

      把红色字体的信息整理起来就得到应急报告了。

## IOC

综上所述，答案如下：

1）在2019年5月2日21点36分，Adriana.breaux的windows主机被Hawkeye Keylogger恶意软件感染。

2）细节：

      主机名：BREAUX-WIN7-PC

      用户名：Adriana.breaux

      MAC地址：84:8f:69:09:86:c0

      Ip地址：10.0.0.227

3）IOC:

      Ip:145.14.145.4   port:21         url:000.webhost.com

      Ip:145.14.145.4   port:37280   url:000webhost.com

      Ip:145.14.144.10 port:21         url:000webhost.com

      Ip:145.14.144.10 port:40651   url:000webhost.com

      Ip:145.14.144.10 port:47434    url:000webhost.com

      Ip:145.14.145.99 port:21         url:000webhost.com

      Ip:145.14.145.99 port:36091   url:000webhost.com

      Ip:145.14.145.99 port:35396   url:000webhost.com。