### **Network Analysis — Malware Compromise**

This is a walkthrough of the BTLO lab Network Analysis — Malware Compromise which is a medium level difficulty lab.

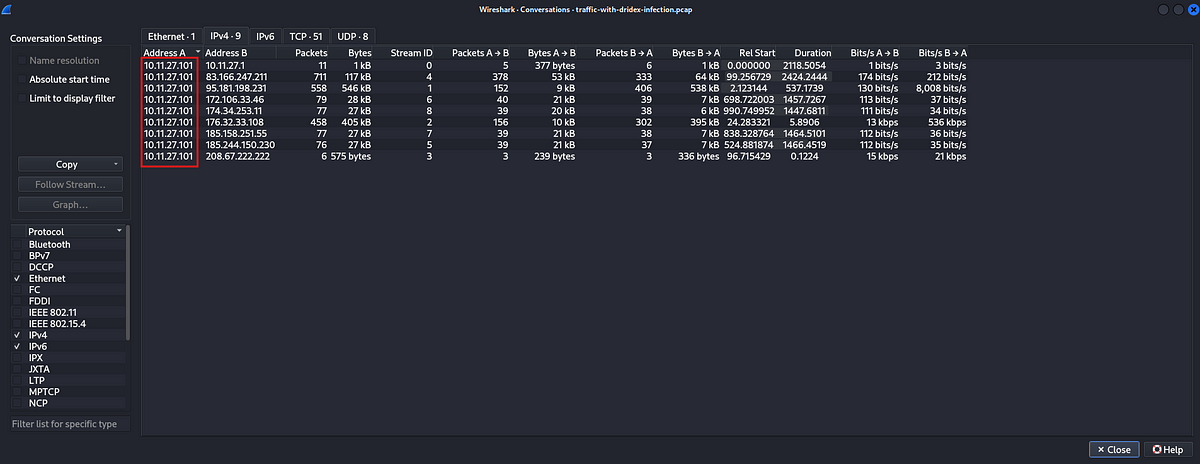
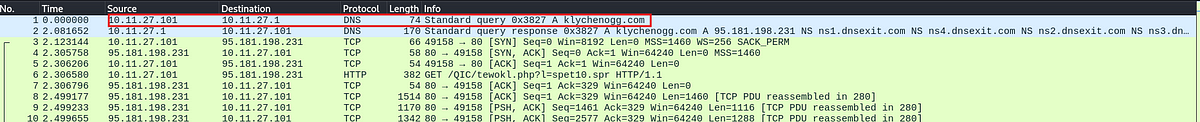
Scenario: A SOC Analyst at Umbrella Corporation is going through SIEM alerts and sees the alert for connections to a known malicious domain. The traffic is coming from Sara’s computer, an Accountant who receives a large volume of emails from customers daily. Looking at the email gateway logs for Sara’s mailbox there is nothing immediately suspicious, with emails coming from customers. Sara is contacted via her phone and she states a customer sent her an invoice that had a document with a macro, she opened the email and the program crashed. The SOC Team retrieved a PCAP for further analysis.

We are provided a pcap file to analyse.

Investigation:

1. What’s the private IP of the infected host?

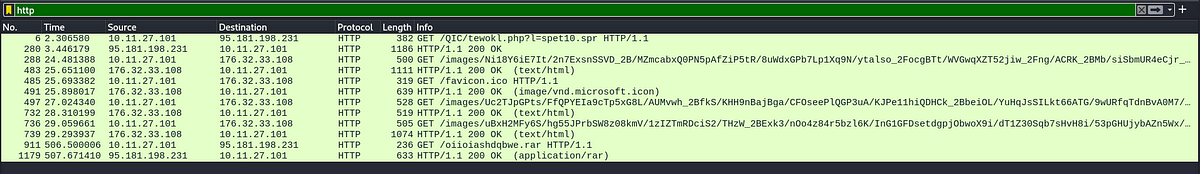
If we look at the first packet in the capture, the IP address 10.11.27.101 is making a DNS request to the IP address 10.11.27.1 for information about the klychenogg.com address. It is clear that the Ip address of the victim is 10.11.27.101. We can also confirm that by checking Statistics -> conversations section, here we can see that there are only two private IP addresses in the capture and one of them has the most traffic.



Answer: 10.11.27.101

2. What’s the malware binary that the macro document is trying to retrieve?

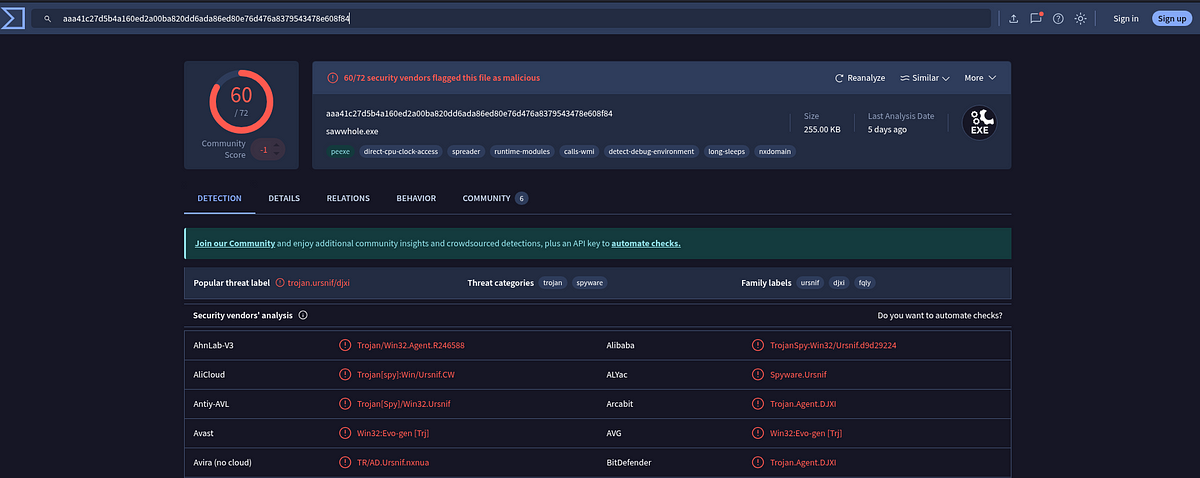
Let us check the http traffic using the wireshark filter http.



If we look at the packets closely, the first thing that sticks out immediately is the .spr extension. Let us inspect the packet by following the http stream.



In the HTTP response we can see that the data starts with MZ and followed by “This program cannot be run in DOS mode.”. This is the indication of a Windows executable file. But the file had an extension of .’spr’ which is not an extension for an executable file.

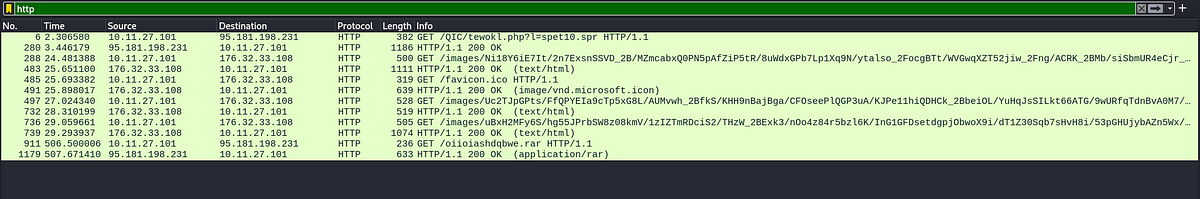


Further analysis on Virustotal, with the hash of the file confirms that this is a malicious file.

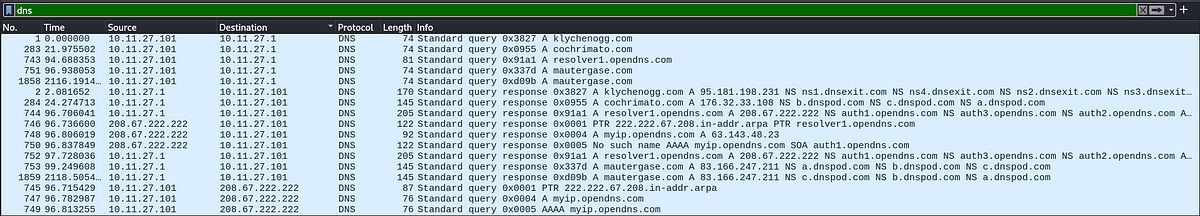
Answer: sept10.spr

3. From what domain HTTP requests with GET /images/ are coming from?

Let us look at http packets again.



We can see that the requests for /images/ are coming from a single IP address, which is 176.32.33.108. To find the domain associated with this IP address, we can look at the DNS packets.



More specifically, we can look at packets where dns.a == 176.32.33.108



Answer: cochrimato.com

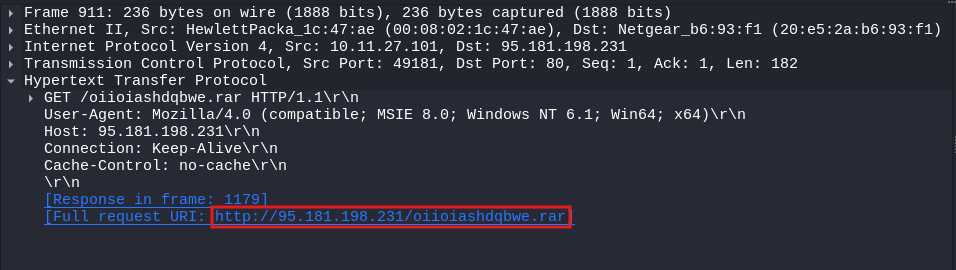
4. The SOC Team found Dridex, a follow-up malware from Ursnif infection, to be the culprit. The customer who sent her the macro file is compromised. What’s the full URL ending in .rar where Ursnif retrieves the follow-up malware from?

We can specifically search for http request which contain .rar extension in the URL’s

http.request.full\_uri contains “.rar”



To get the full URL, we can look at the packet details pane.

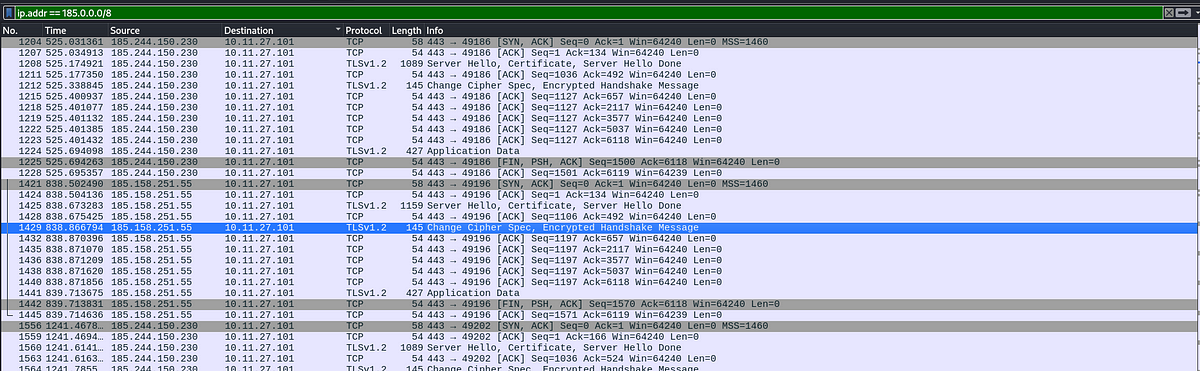


Answer:<http://95.181.198.231/oiioiashdqbwe.rar>

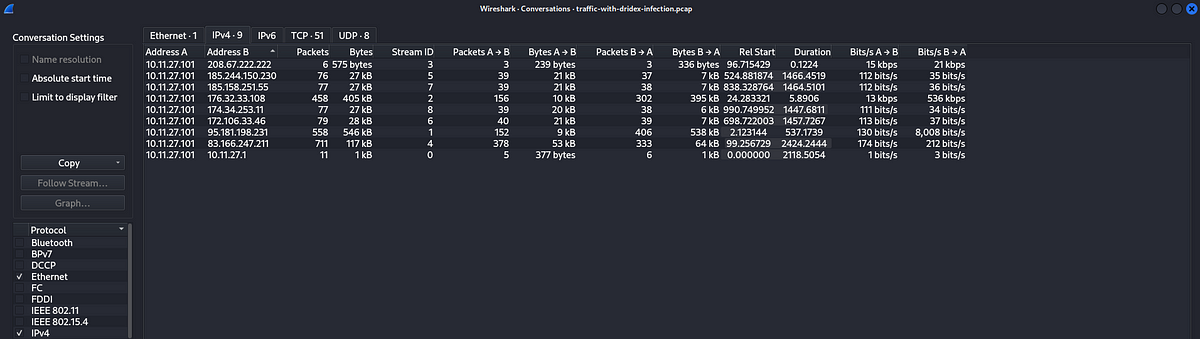
5. What is the Dridex post-infection traffic IP addresses beginning with 185.?

We can filter out the packets containing IP addresses which start with 185.

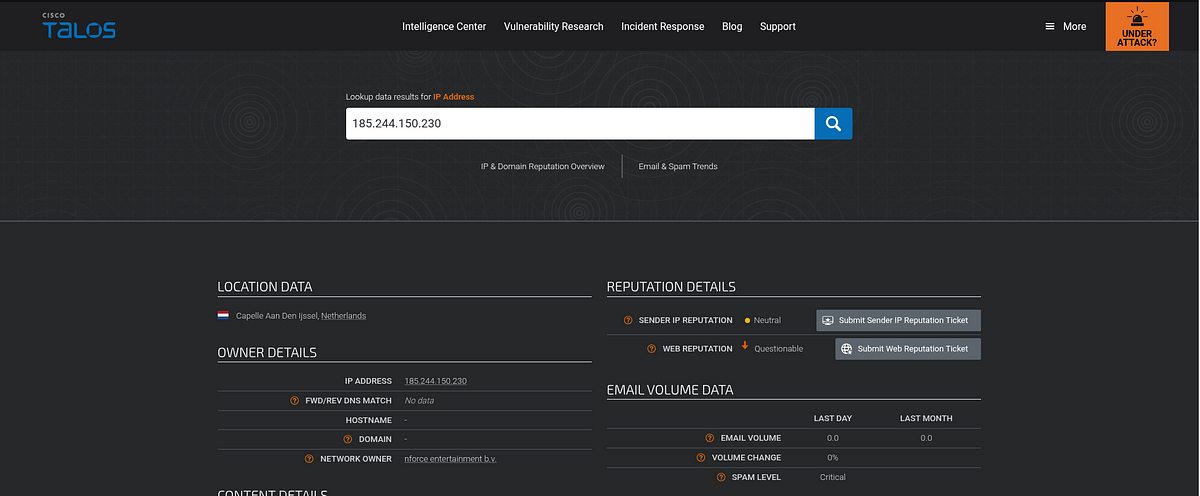
ip.addr == 185.0.0.0/18



There are two IP addresses starting with 185, let us check the conversations tab to check which of these IP addresses is communicating with our host the most.



Both of them have similar kind of conversation statistics. Now let us check for the reputation of these IP addresses.



Answer: 185.244.150.230

This is the end of the walkthrough.