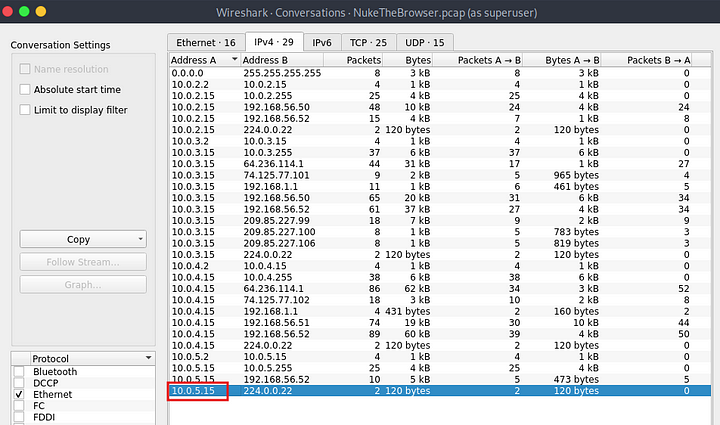
### **NukeTheBrowser — CyberDefenders**

**Scenario:** A network trace with attack data is provided. Please note that the IP address of the victim has been changed to hide the true location.

As a soc analyst, analyze the artifacts and answer the questions.

1. **Multiple systems were targeted. Provide the IP address of the highest one.**

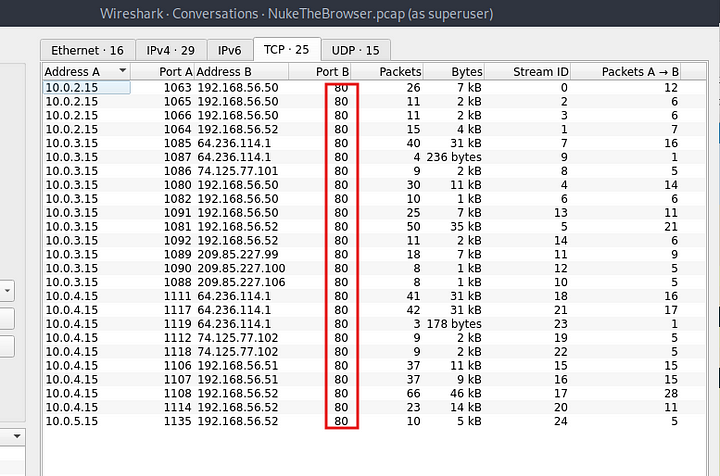
We can check the Statistics -> Conversations -> IPv4. Then sort by IP address.



**Answer:** 10.0.5.15

**2. What protocol do you think the attack was carried over?’**

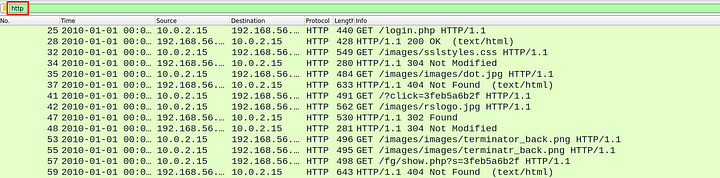
In the same conversations window, go to TCP, and check the ports being used. We can also check the protocol hierarchy.



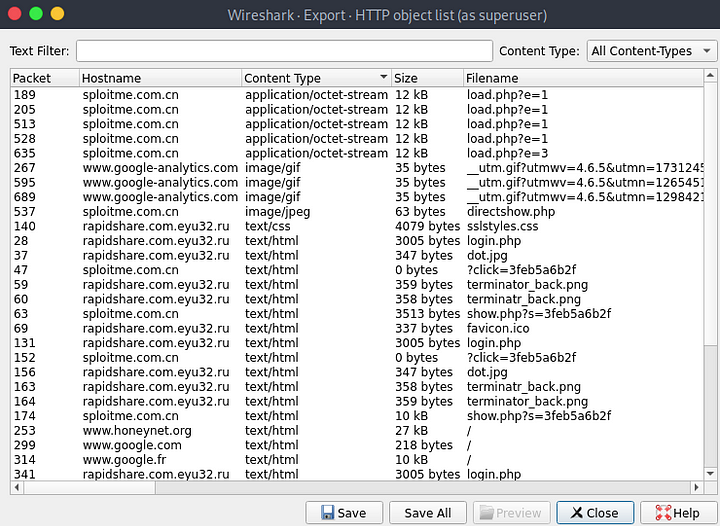
**Answer:** http

**3. What was the URL for the page used to serve malicious executables (don’t include URL parameters)?**

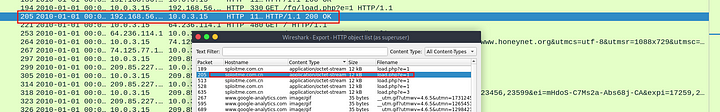
Let us check the http packets.



Now let us check the http objects. Go to File -> Export Objects -> Http Objects.



We see above the objects from load.php are of type application/octet-stream. Let us examine the packets related to these. We can select any object from this and Wireshark will highlight the related packet.



Let us examine this packet by following the http stream.



As we can see above the magic bytes that represent an executable file.

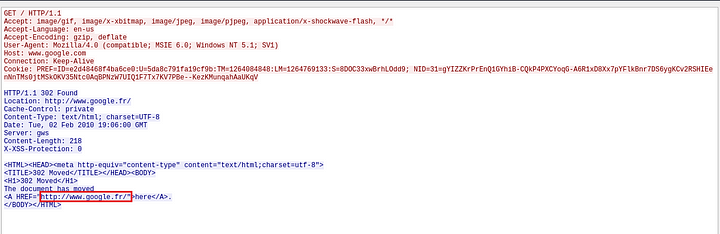
Answer: http://sploitme.com.cn/fg/load.php

**4. What is the number of the packet that includes a redirect to the french version of Google and probably is an indicator for Geo-based targeting?**

We can look at the http full request URL and the referer data to find out which packet redirected to the above mentioned site.



As we can see above, the google french site was requested after the packet number 299. Let us look at this packet.

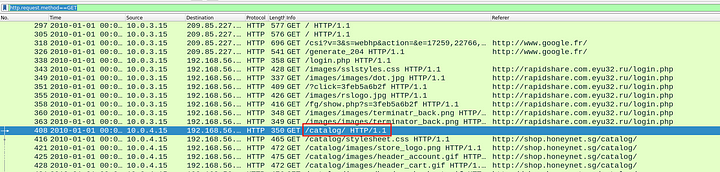


**Answer:** 299

**5. What was the CMS used to generate the page ‘shop.honeynet.sg/catalog/’? (Three words, space in between)**

Let us look at the http get requests.

http.request.method==GET



Let us examine the packet with the GET request to /catalog.

In the HTTP data, we can see the Content Management Service(CMS) used.

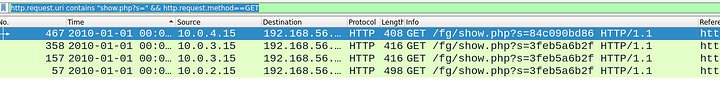


**Answer:** osCommerce Online Merchant

**6. What is the number of the packet that indicates that ‘show.php’ will not try to infect the same host twice?**

Filter the http traffic to show packets containing show.php.

http.request.uri contains "show.php?s=" && http.request.method==GET



We got 4 packets. Let us examine the difference between these.

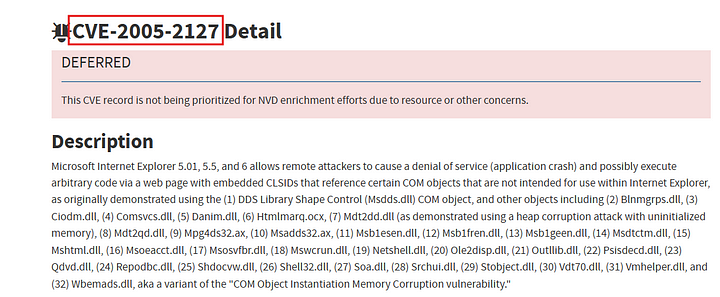
Three of he packets led to the execution of an obfuscated java script. But one of these packets did not execute any code.



**Answer:** 366

**7. One of the exploits being served targets a vulnerability in “msdds.dll”. Provide the corresponding CVE number.**

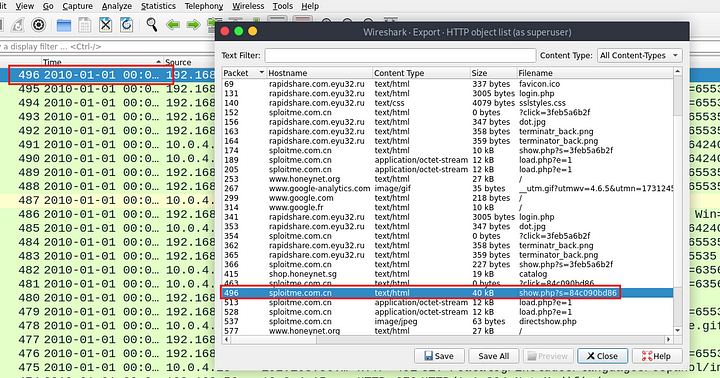
We can search on google to check for this vulnerability.



**Answer:** CVE-2005–2127

**8. What is the name of the executable being served via ‘http://sploitme.com.cn/fg/load.php?e=8' ?**

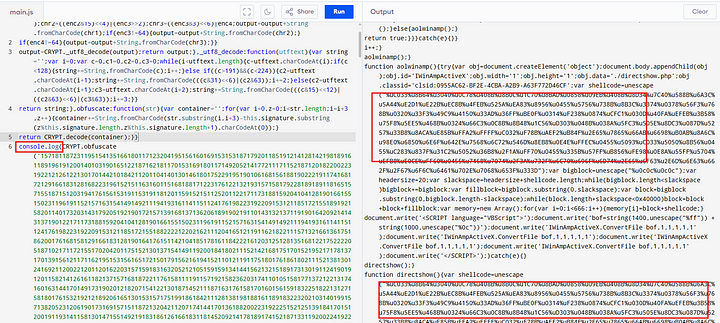
Let us check the http objects again to see if any of the objects were served with this URL.



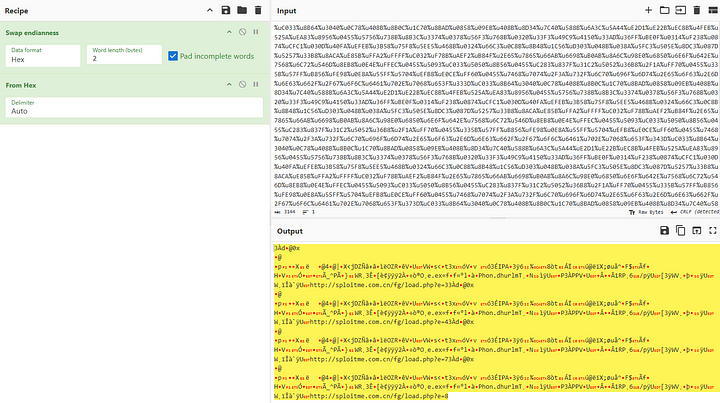
Let us examine the packet number 496.



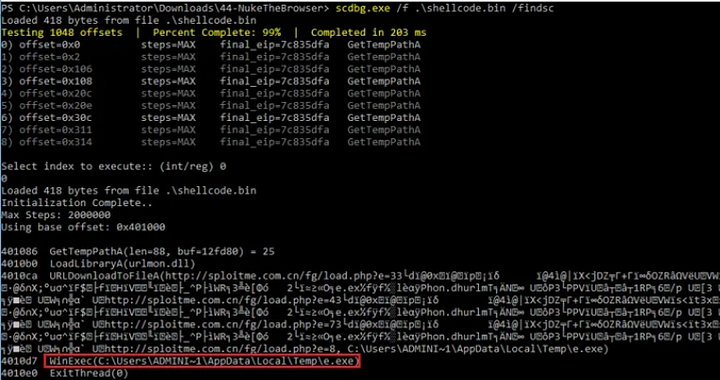
There is a java script code being delivered. Let us examine this code. We can replace the eval command with the console.log() function. Then run it to check the obfuscated code.



Now we can post this de obfuscated code to cyberchef to decode it.



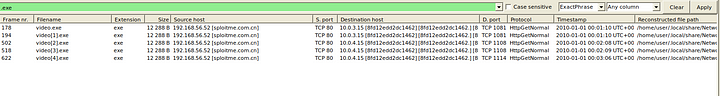
Now, we can take this code and analyse it with scdbg to see the executable that is downloaded.



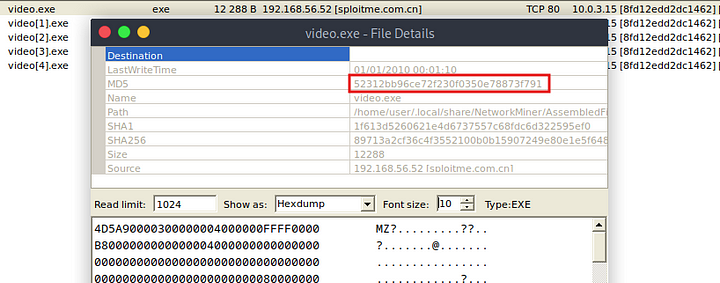
**Answer:** e.exe

**9. One of the malicious files was first submitted for analysis on VirusTotal at 2010–02–17 11:02:35 and has an MD5 hash ending with ‘78873f791’. Provide the full MD5 hash.**

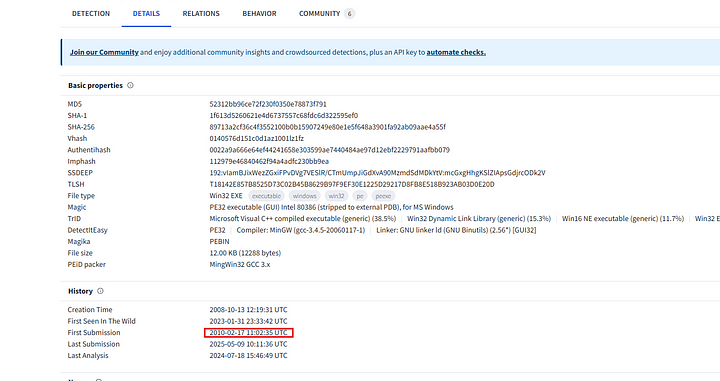
We can use NetwrokMiner to check for the executables downloaded.



Now we can double click these files to see the hash of these files.



Now we can submit this hash to VirusTotal to verify when this was first submitted.



**Answer:** 52312bb96ce72f230f0350e78873f791

**10. What is the name of the function that hosted the shellcode relevant to ‘http://sploitme.com.cn/fg/load.php?e=3'?**

From the obfuscated code we could figure out where the above mentioned URL was used.



Further analysis of the Javsscript gives us the answer.

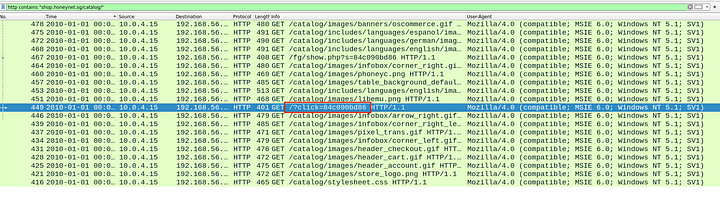


**Answer:** aolwinmap

**11. Deobfuscate the JS at ‘shop.honeynet.sg/catalog/’ and provide the value of the ‘click’ parameter in the resulted URL.**

Filter for http containing **shop.honeynet.sg/catalog/.**

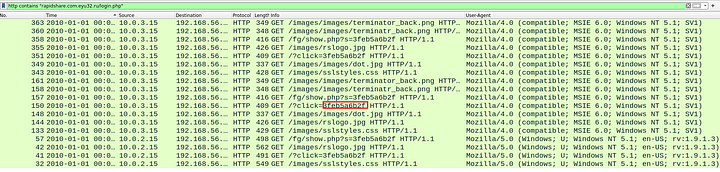
http contains "shop.honeynet.sg/catalog/"



We can see the value of the click parameter.

**Answer:** 84c090bd86

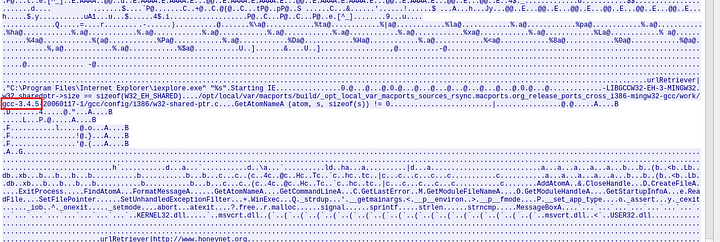
**12. Deobfuscate the JS at ‘rapidshare.com.eyu32.ru/login.php’ and provide the value of the ‘click’ parameter in the resulted URL.**

****

Answer: 3feb5a6b2f

**13. What was the version of ‘mingw-gcc’ that compiled the malware?**

Follow the packet from the last question.



**Answer:** 3.4.5

**14. The shellcode used a native function inside ‘urlmon.dll’ to download files from the internet to the compromised host. What is the name of the function?**

****

Answer: URLDownloadToFile

This is the end of this walkthrough.