Amadey C2 Hunt

08 May 2023 18:42

Nice report from @McAfee_Labs on recent #Amadey intrusion and related #malware distribution.

I fancied a stab at some analysis of any #c2 IoCs available in the report to see what else we can find.

Let take a look at:

Lebro.exe

Lebro.exe, a component of Amadey, is a 235 KB file, compiled in C/C++. Lebro.exe is responsible for executing nbveek.exe, which is a next stage of the malware. The file is again dropped in TEMP folder.

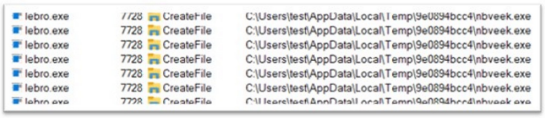
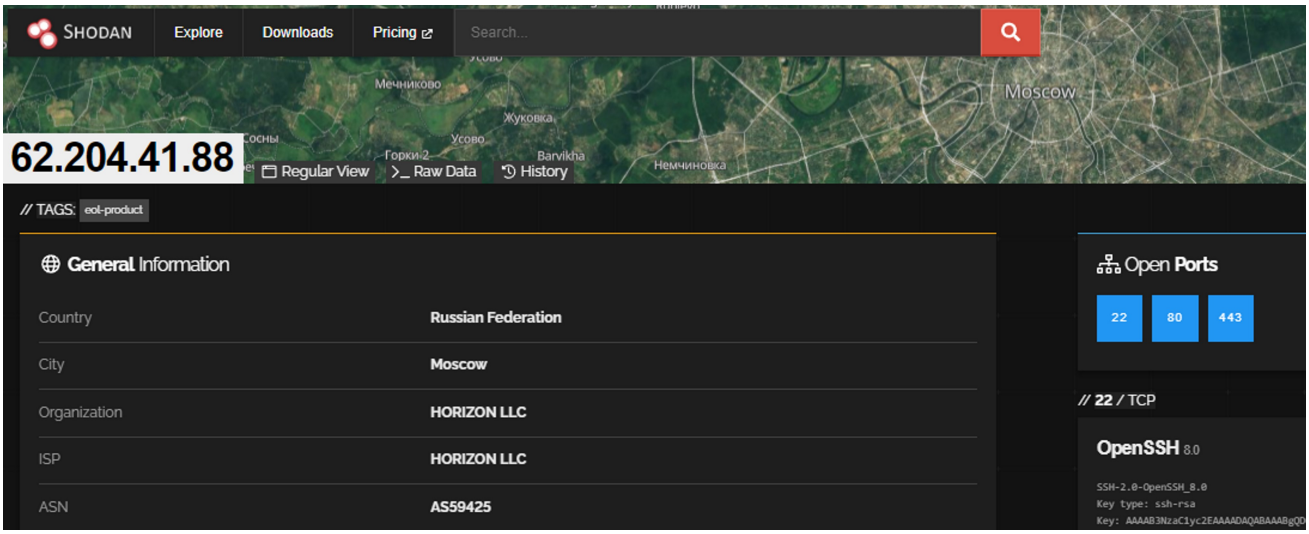


Figure 27: Dropping another executable in TEMP folder

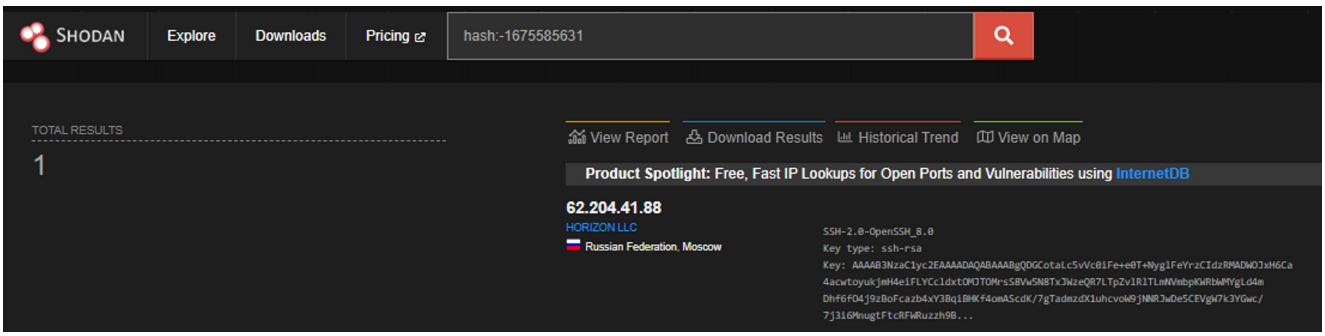
Stage 7: Analyzing nbveek.exe

The hashes of lebro.exe and nbveek.exe are same, they are the same binaries, hence it is **Amadey**. It is connecting to I[redacted] ***62.204.41.88.***

Lets take a look in Shodan:



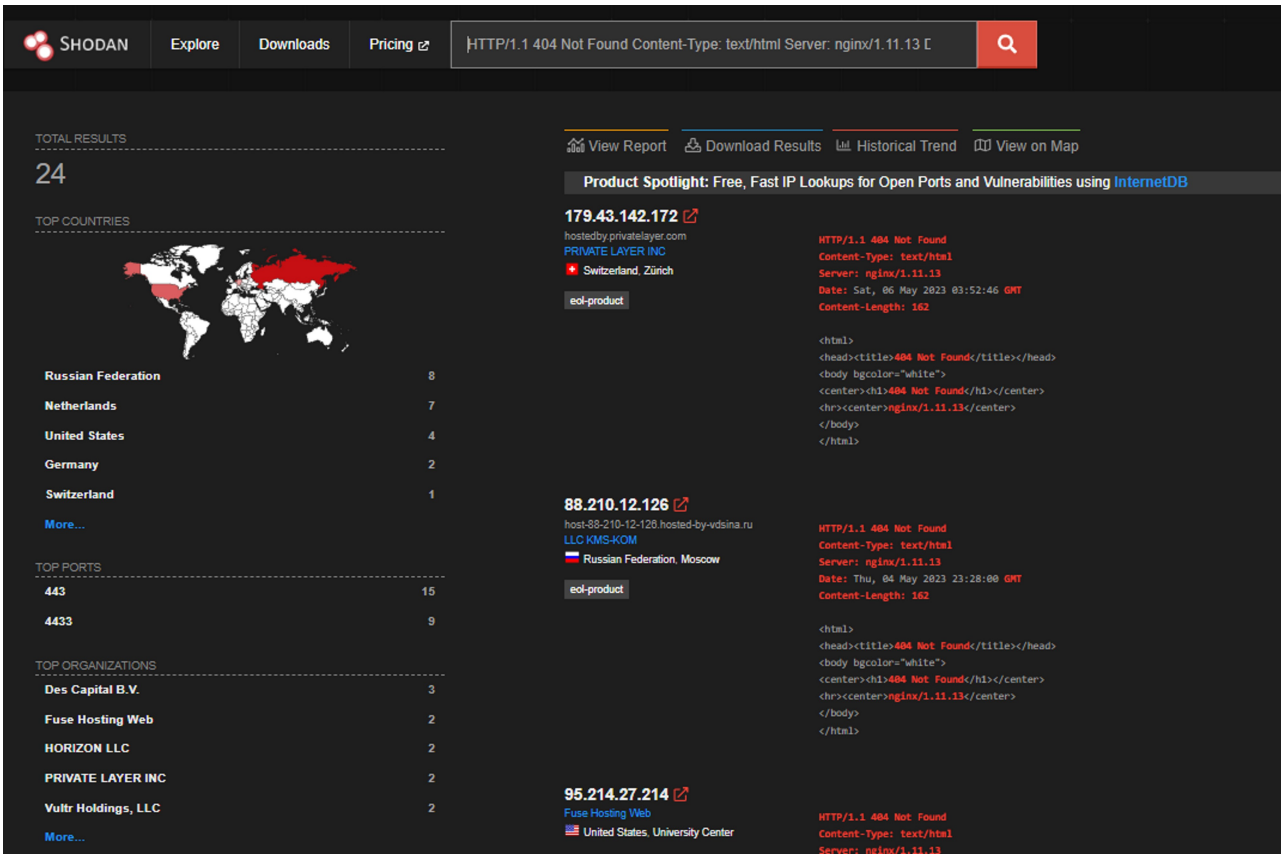
A nice friendly geolocation :D hosted at HORIZON LLC. First pivot off the SSH key, unfortunately it yields no results.



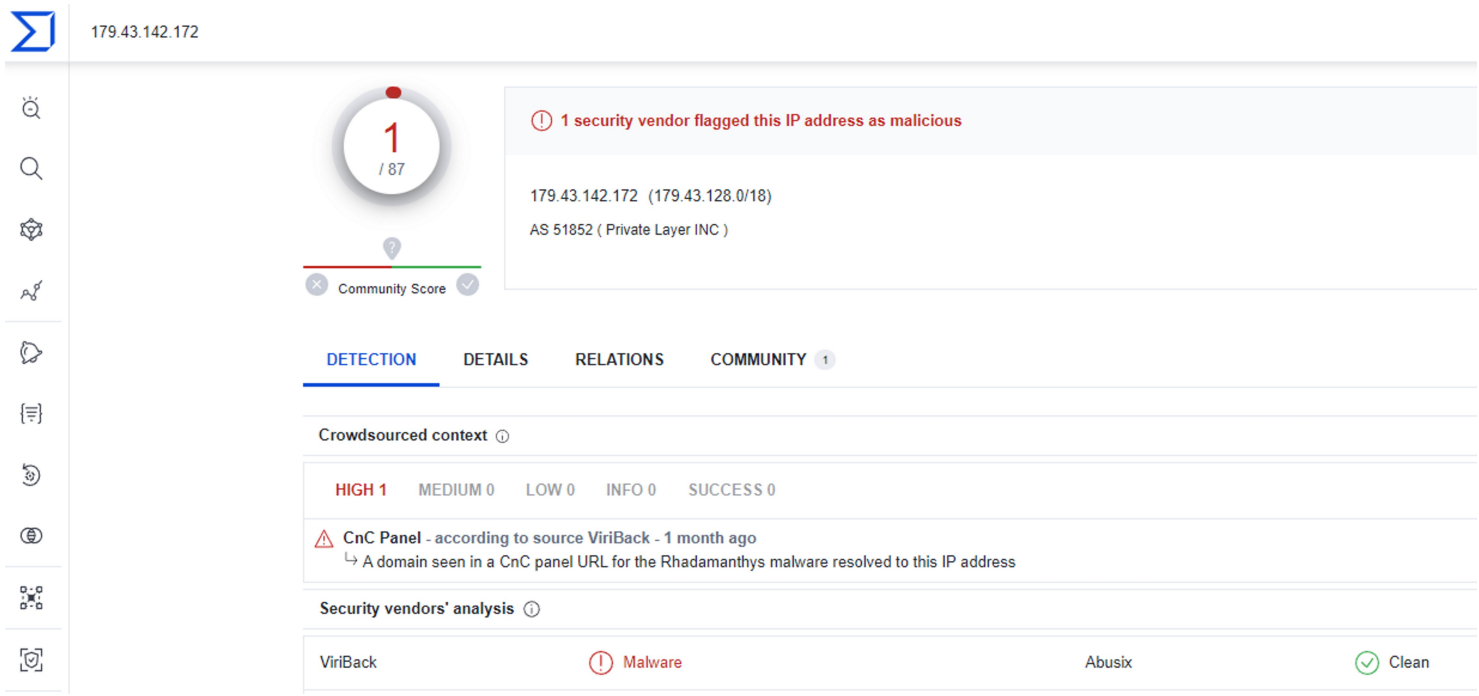
Next lets take a look at the service running on port 443:

Nothing on the hash, lets modify the query slightly to remove the date information: https://www.shodan.io/search?query=HTTP%2F1.1+404+Not+Found+Content-Type%3A+text%2Fhtml+Server%3A+nginx%2F1.11.13+Date%3A+GMT+Content-Length%3A+162++%3Chtml%3E+%3Chead%3E%3Ctitle%3E404+Not+Found%3C%2Ftitle%3E%3C%2Fhead%3E+%3Cbody+bgcolor%3D%22white%22%3E+%3Ccenter%3E%3Ch1%3E404+Not+Found%3C%2Fh1%3E%3C%2Fcenter%3E+%3Chr%3E%3Ccenter%3Enginx%2F1.11.13%3C%2Fcenter%3E+%3C%2Fbody%3E+%3C%2Fhtml%3E

Bingo we have some results:

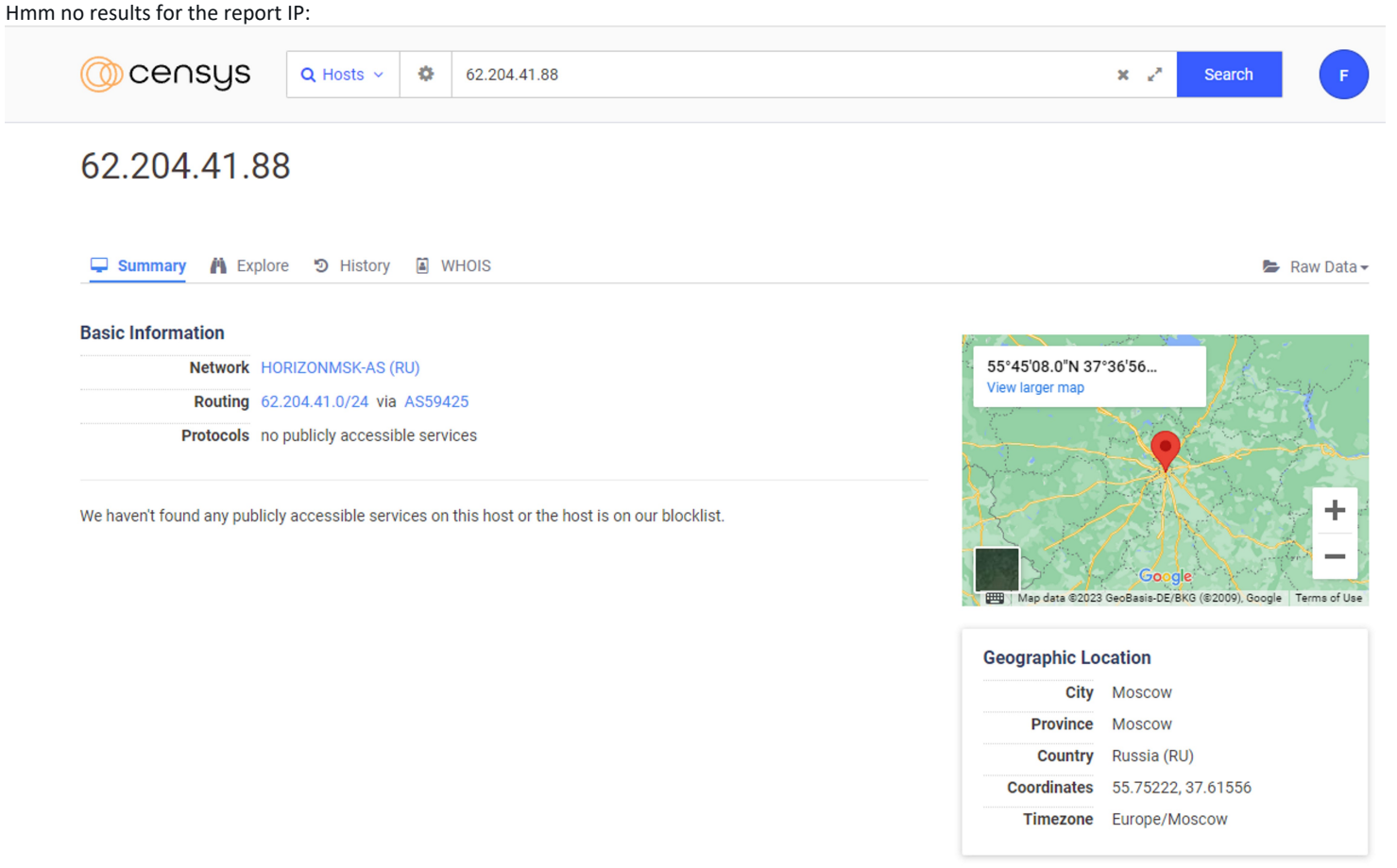


The results look interesting and all appear to be using ports 443/4433. Lets check the first result in VirusTotal, it has a very low detection rate (1 hit) and appears associated with #Rhadamanthys stealer C2. Lets check a few more to validate the results, yep they all appear to be infrastructure related to stealer malware.

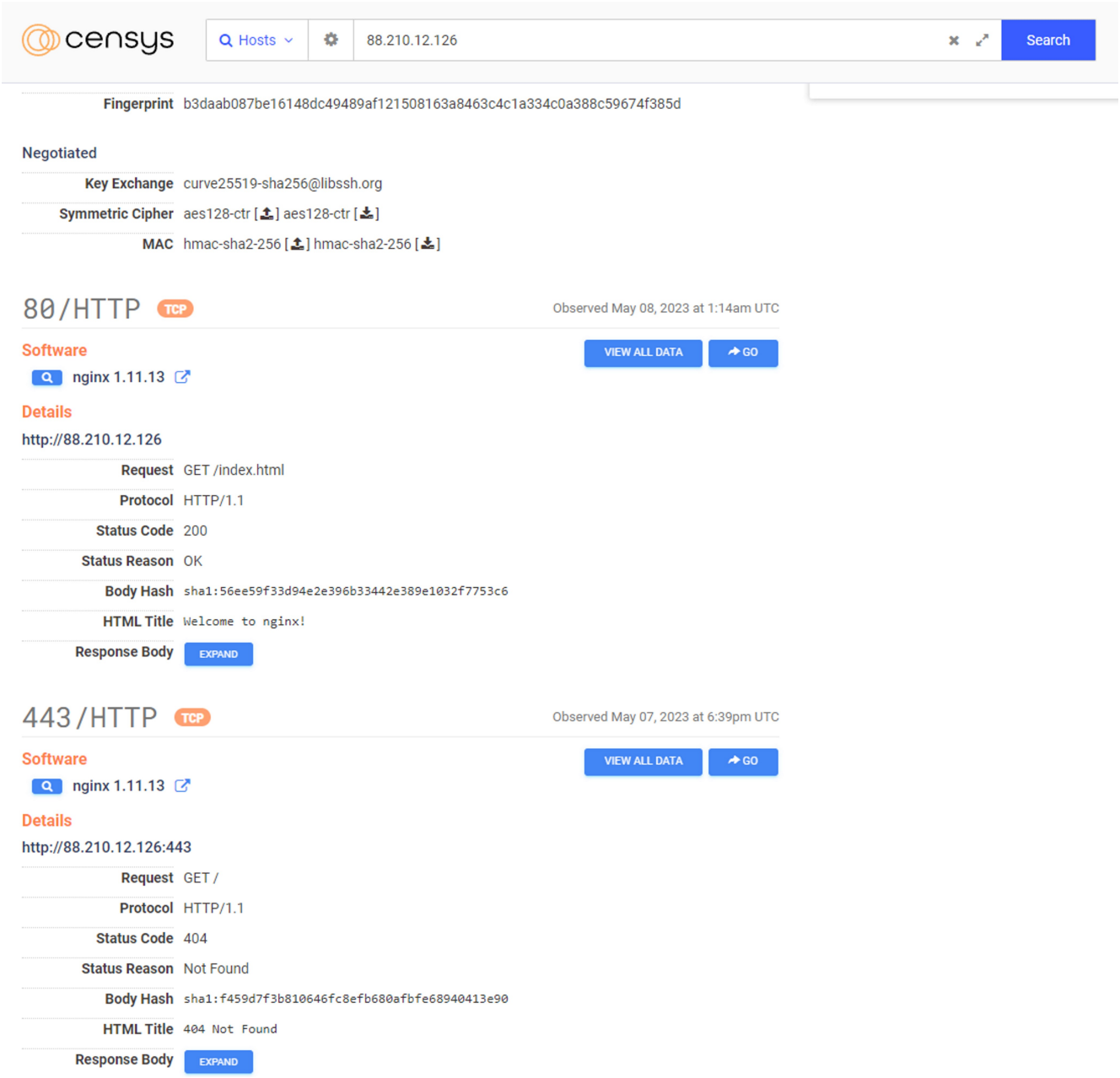


So lets take a look at Censys and see if we have any variation on the results:

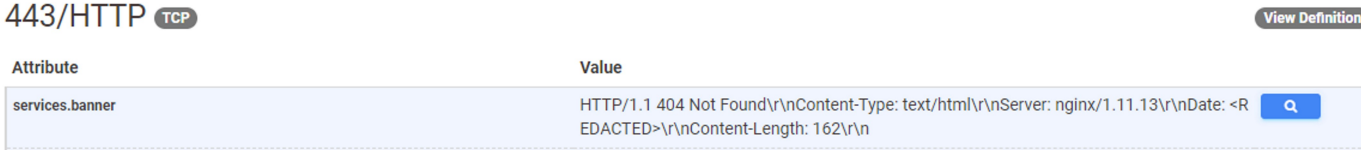
Hmm no results for the report IP:



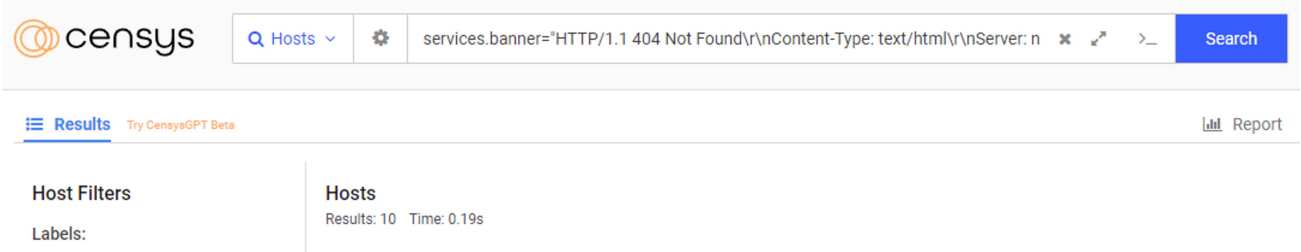
Lets try another:



Next lets search on the HTTP services.banner present on port 443:
https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=services.banner%3D%22HTTP%2F1.1+404+Not+Found%5Cr%5CnContent-Type%3A+text%2Fhtml%5Cr%5CnServer%3A+nginx%2F1.11.13%5Cr%5CnDate%3A++%3CREDACTED%3E%5Cr%5CnContent-Length%3A+162%5Cr%5Cn%22



10 results, at first glance we have some overlap with Shodan but there are some newly identified hosts.



Stealer C2s:

108[.]61[.]189[.]120142[.]11[.]215[.]202142[.]11[.]215[.]202144[.]76[.]33[.]241159[.]65[.]13[.]48176[.]11

3[.]115[.]86179[.]43[.]142[.]172179[.]43[.]154[.]245185[.]225[.]73[.]180185[.]246[.]220[.]162185[.]43[.]223[.]200192[.]30[.]243[.]151194[.]180[.]48[.]102216[.]250[.]255[.]120216[.]250[.]255[.]1552607:5500:3000:1954::231[.]41[.]244[.]8145[.]77[.]66[.]15146[.]151[.]25[.]14662[.]204[.]41[.]21062[.]204[.]41[.]8879[.]137[.]194[.]24080[.]66[.]88[.]7284[.]54[.]50[.]15884[.]54[.]50[.]15985[.]217[.]144[.]8288[.]210[.]12[.]12689[.]22[.]230[.]17591[.]215[.]85[.]15795[.]214[.]27[.]214