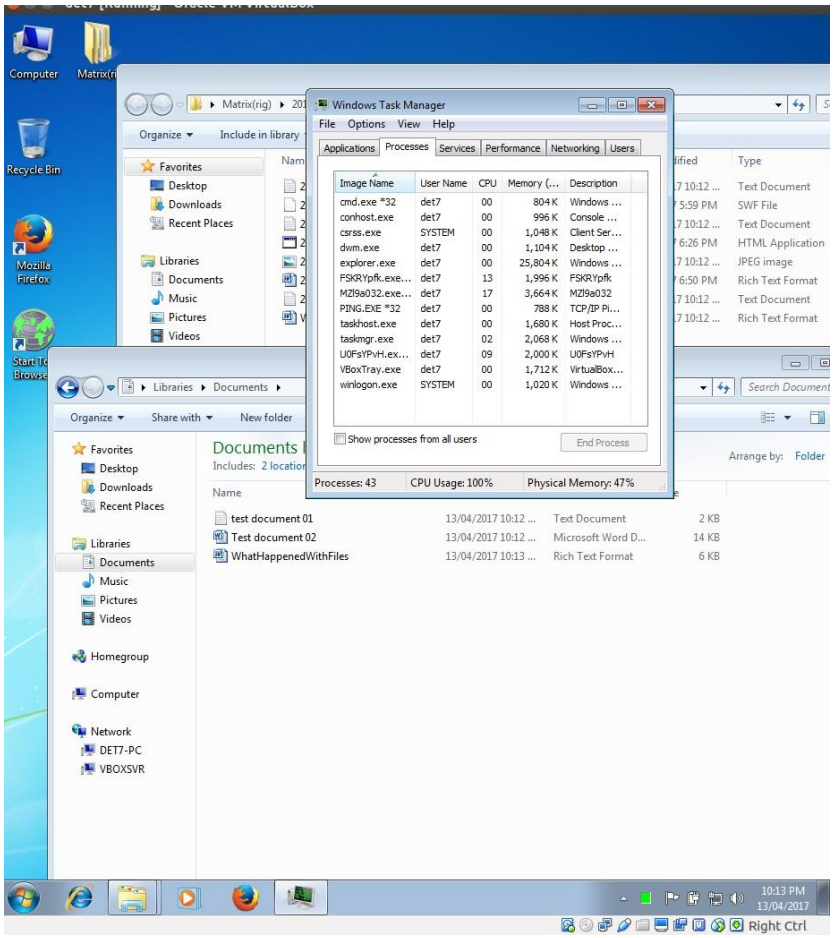
A look at Matrix(RIG)

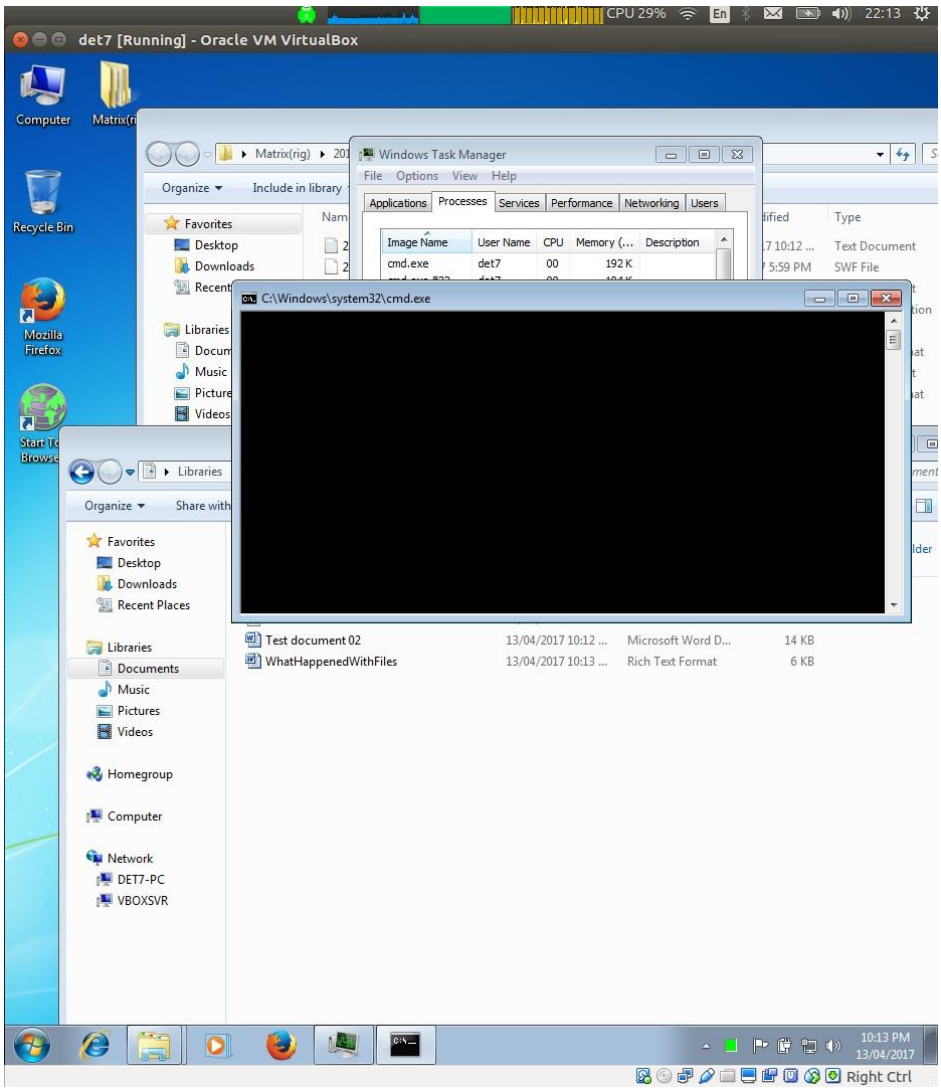
Matrix ransomware was using a waterhole attack from a compromised website.

On detonation it appeared quiet slow and clunky to me when executed, It took time to execute which I could only figure was the level on encryption been used.

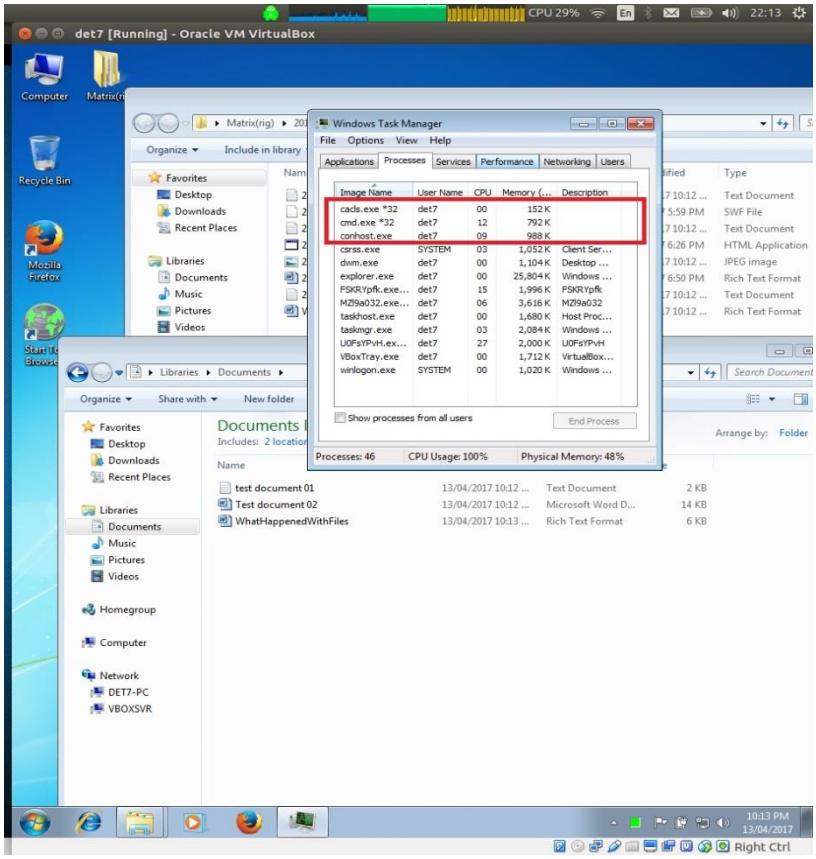


During execution note the FSKRYpfk.exe and MZl9a032.exe along with hidden CMD.exe window

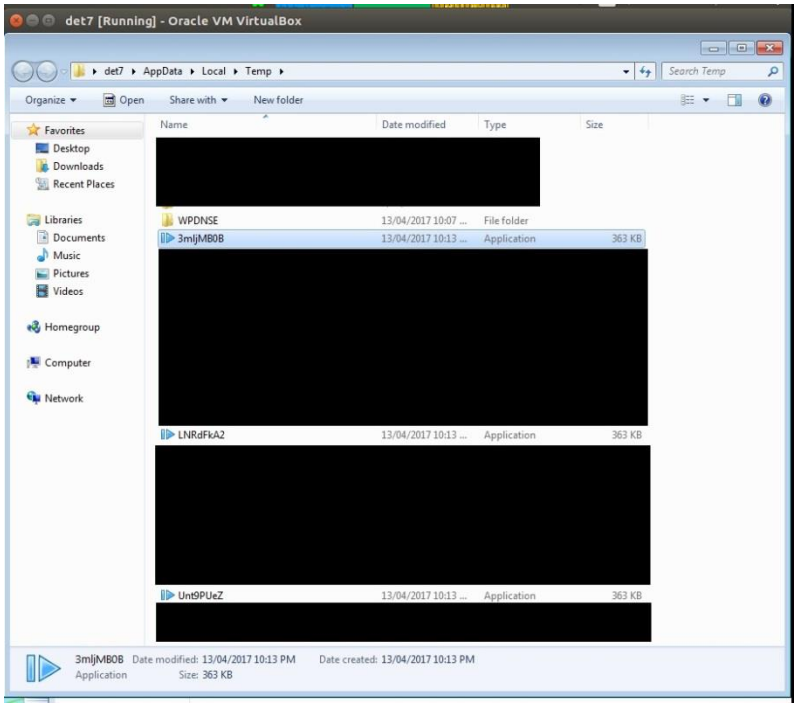
There was also times where it made no attempt to hide its execution (popup command prompt windows) and could be seen working in task manager. I am guessing by that point they consider they have you owned, so no need to hide.



Later in the execution I noted additional executables launching highlighted.

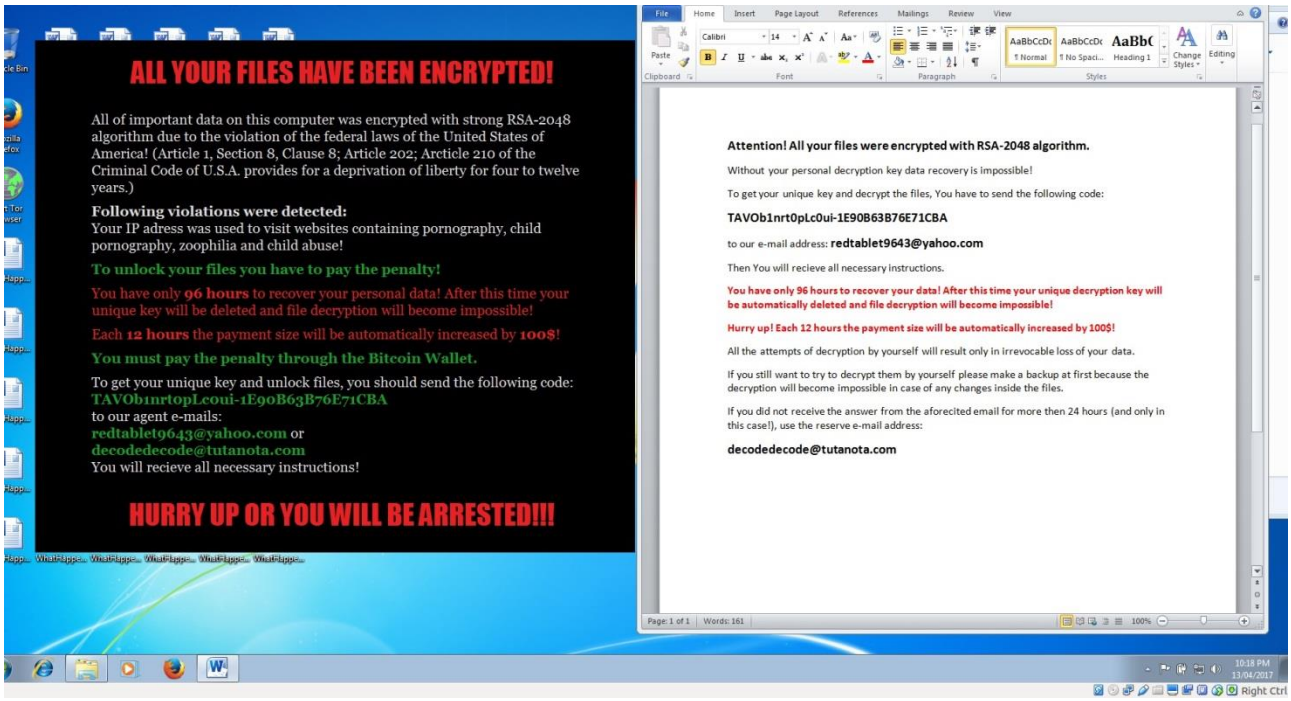


Following a lot of these files lead me to the appdata temp folder

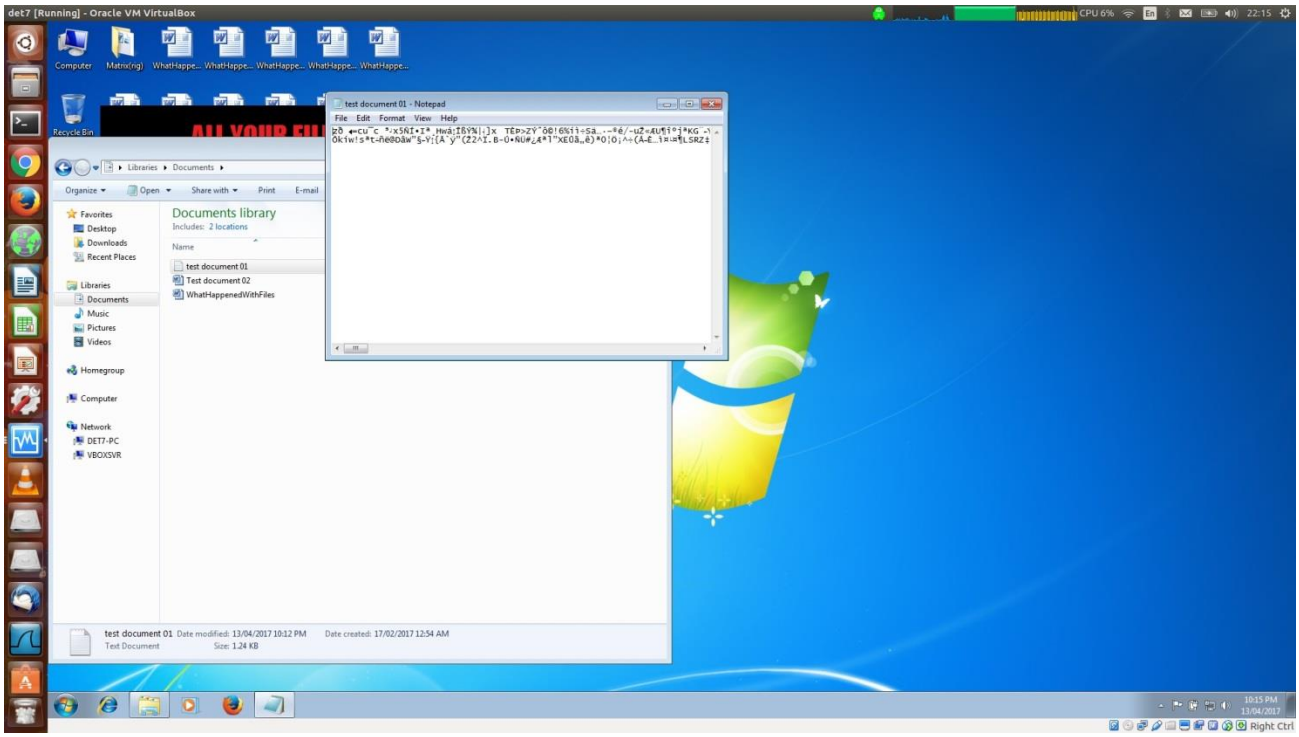


Finally after what seemed like a VERY long time in comparison to a lot of other ransomware I have executed it reached a ransom demand state. What I found unusual about this is that it was run by an executable where most ransom demands are usually dropped on the desktop or the desktop background is changed to the demand note. To a normal user this would make it harder to navigate around as the window had no way to close or minimise it.

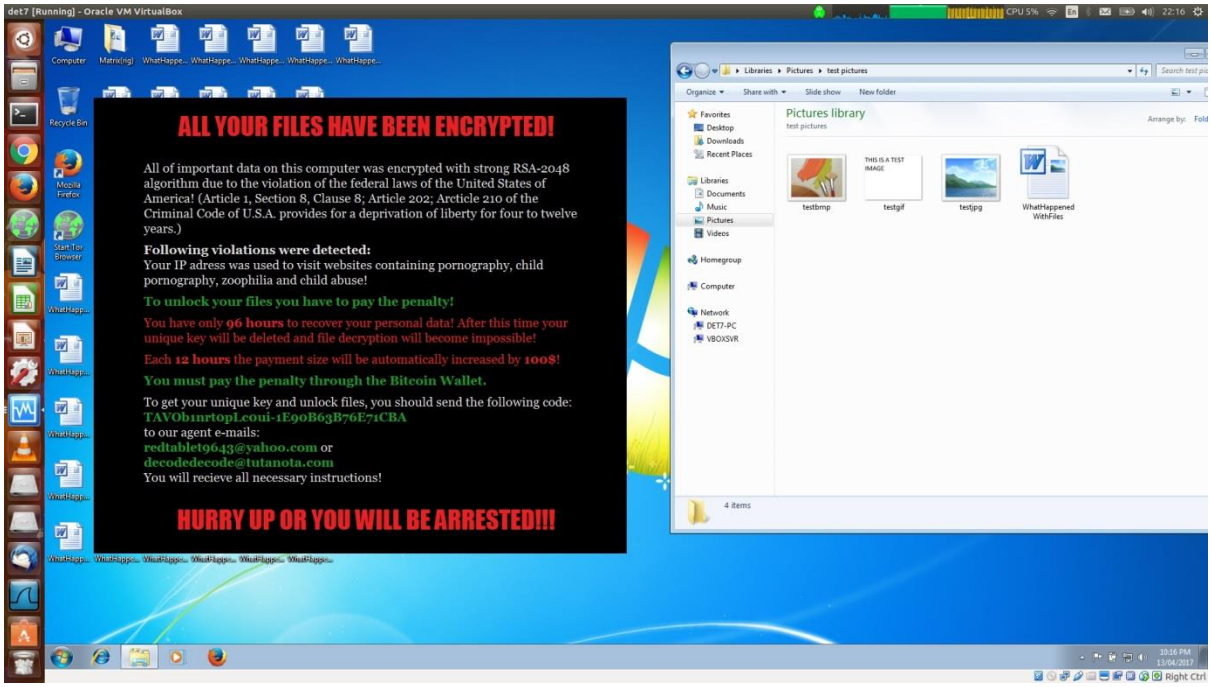
Word documents were generated and dropped just about everywhere, an example of one here which repeats parts of the ransom demand.



The encryption appeared effective against document types, scrambling my txt, word and PDF sample documents.



It was also reasonably effective against pictures with exception of .GIF file types.

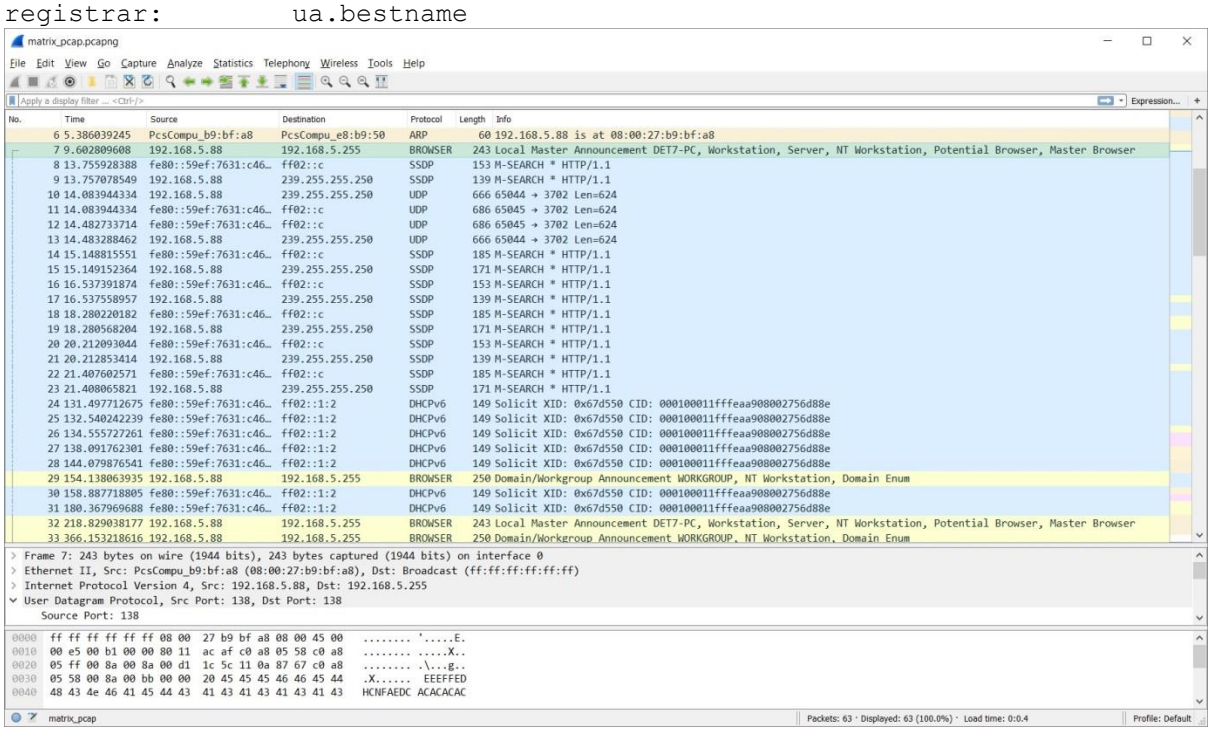


Packet capture

Starts buy quiring the gateway

Quirries a ukranian whois server - stat3.s76.r53.com.ua

```
r53.com.ua
registrar:          ua.bestname
```

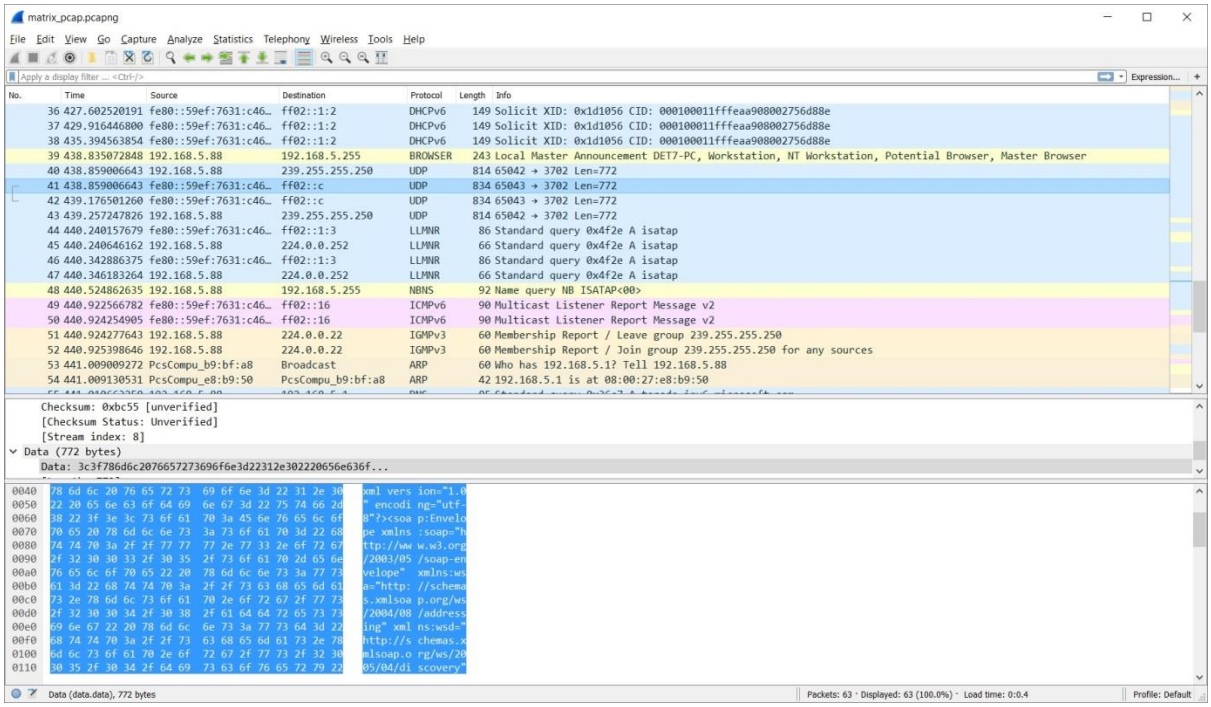


the victim machine then escalates to become the master browser.

SSDP (upnp) is then used to feel out the local network

Some ipv6 traffic which I currently have not worked out.

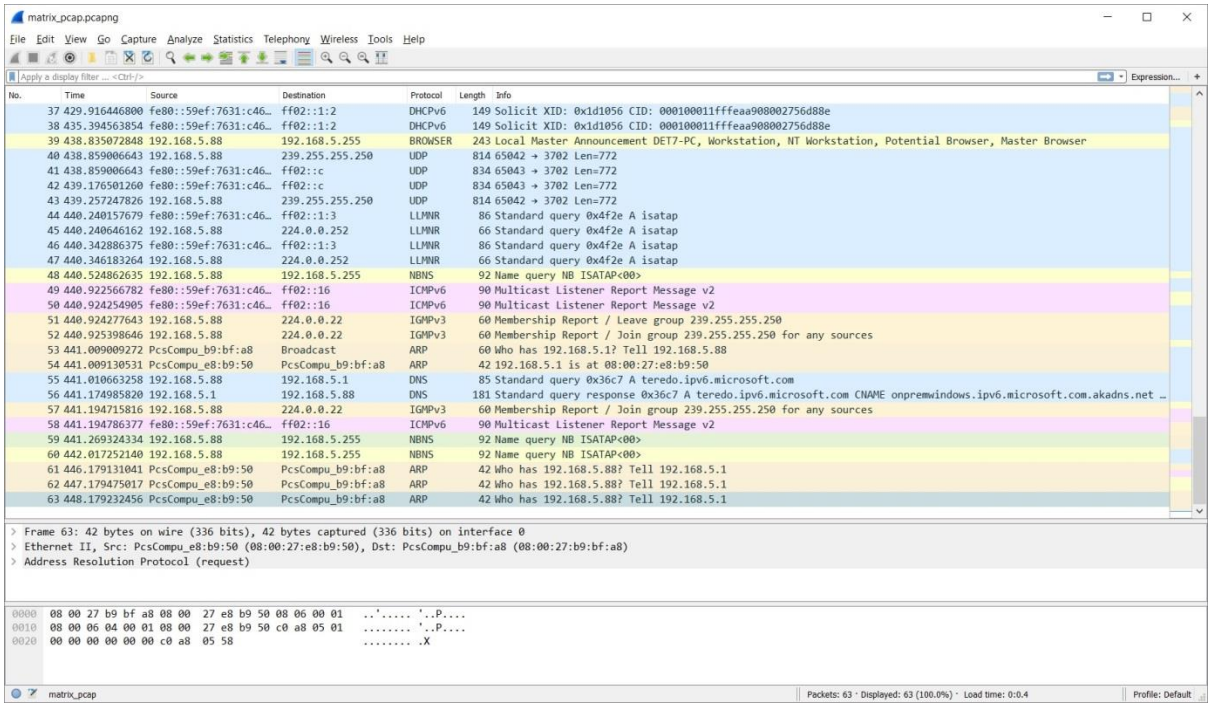
Another master browser declaration and domain enumeration



A pile of UDP traffic using what looks to be ipv6, packet inspection points mostly to

schemas.xmlsoap.org

`Domain Name: XMLSOAP.ORG`
Upon domain lookup I can see ICANN & MARKMONITOR are already here by this point.



end of packet capture.

I found matrix to be slow clunky and “does the job” but fortunately would be easily detected however I am not sure how successful a decryption process would be, there is talk online of using shadow explorer to browse prior shadow copies of your windows environment which matrix tries to delete, there are also references to programs designed to try recover encrypted files which I may look to trial in future “look ats” that I do.

Otherwise the packet capture and ipv6 traffic use is presenting new challenges in following the bread trail back.

Thankyou

MBYX