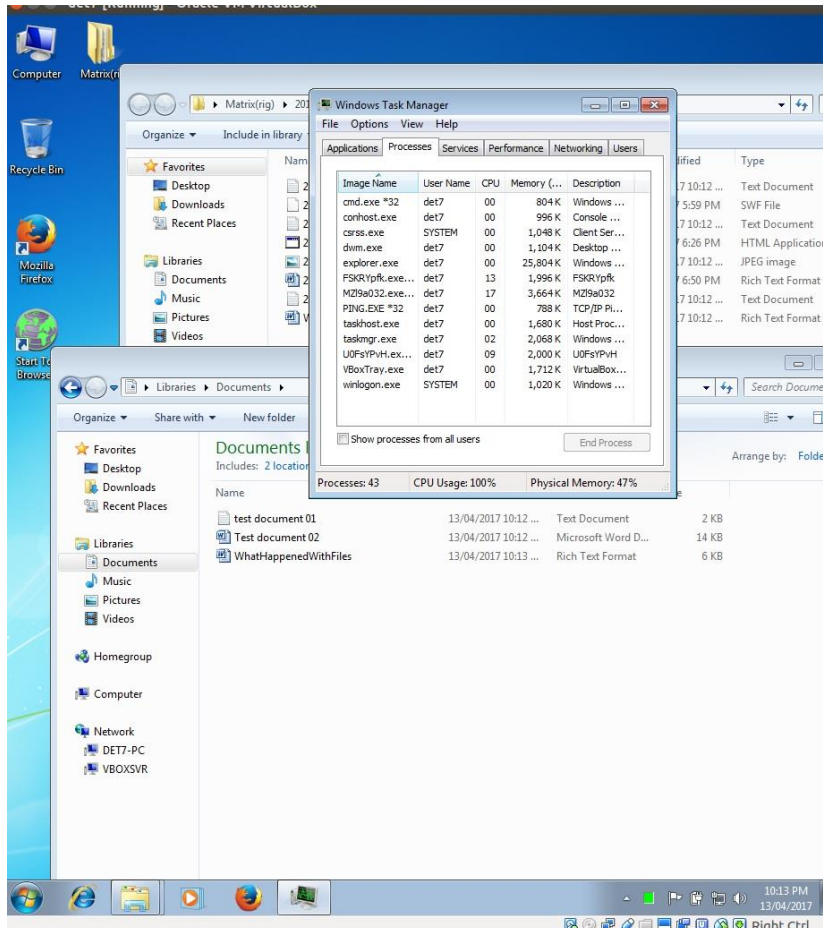


# A look at Matrix(RIG)

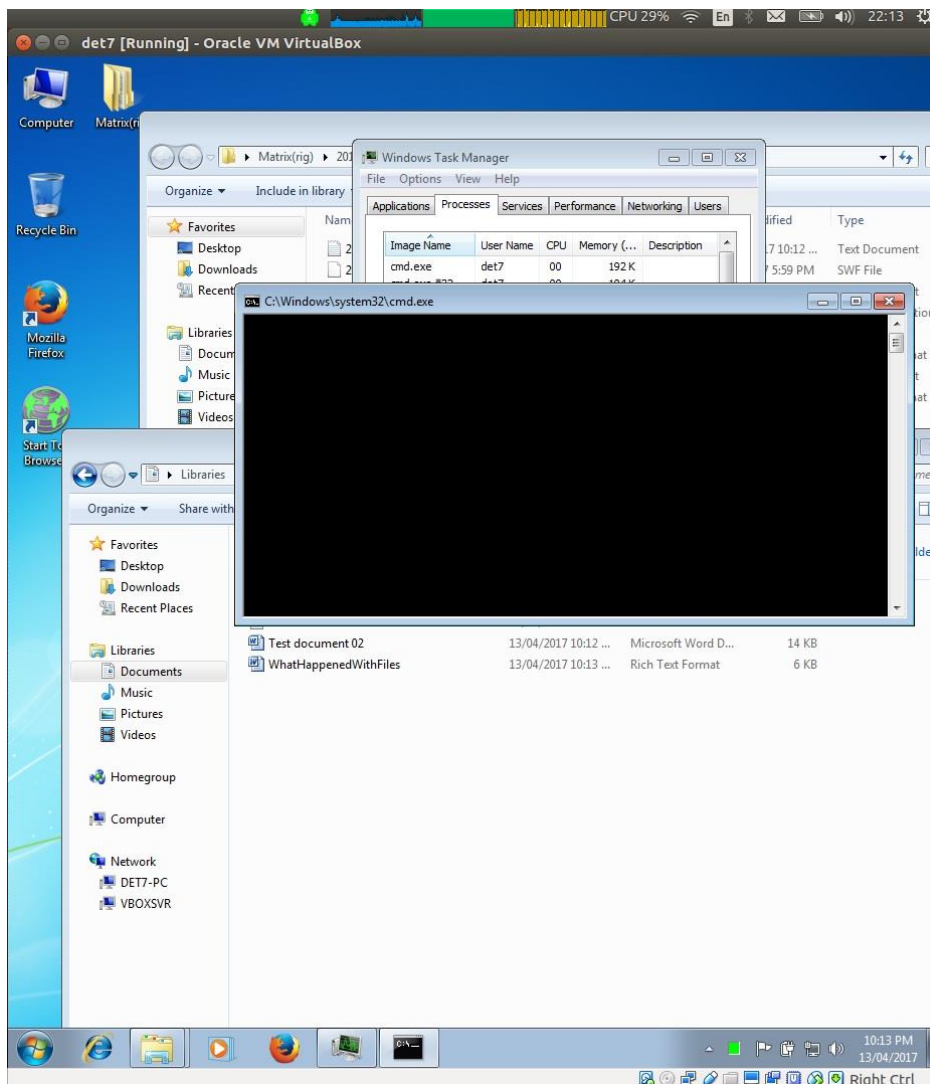
Matrix ransomware was using a waterhole attack from a compromised website.

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.

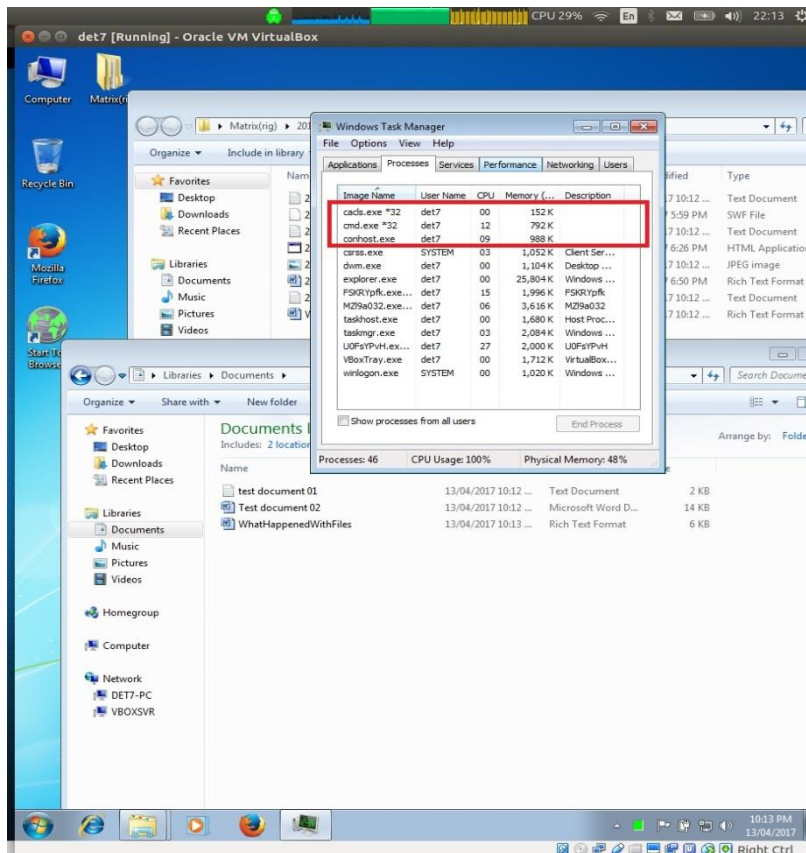


During execution note the FSKR1pfk.exe and MZI9a032.exe along with hidden CMD.exe window

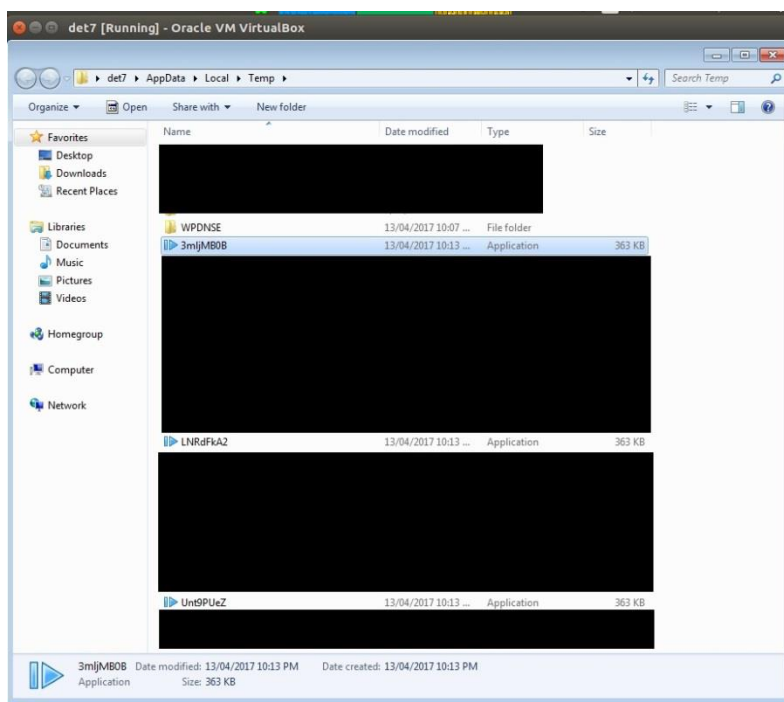
There was also times where it made no attempt to hide its execution (popup command prompt windows) and could be seen working in task manager. I am guessing by that point they consider they have you owned, so no need to hide.



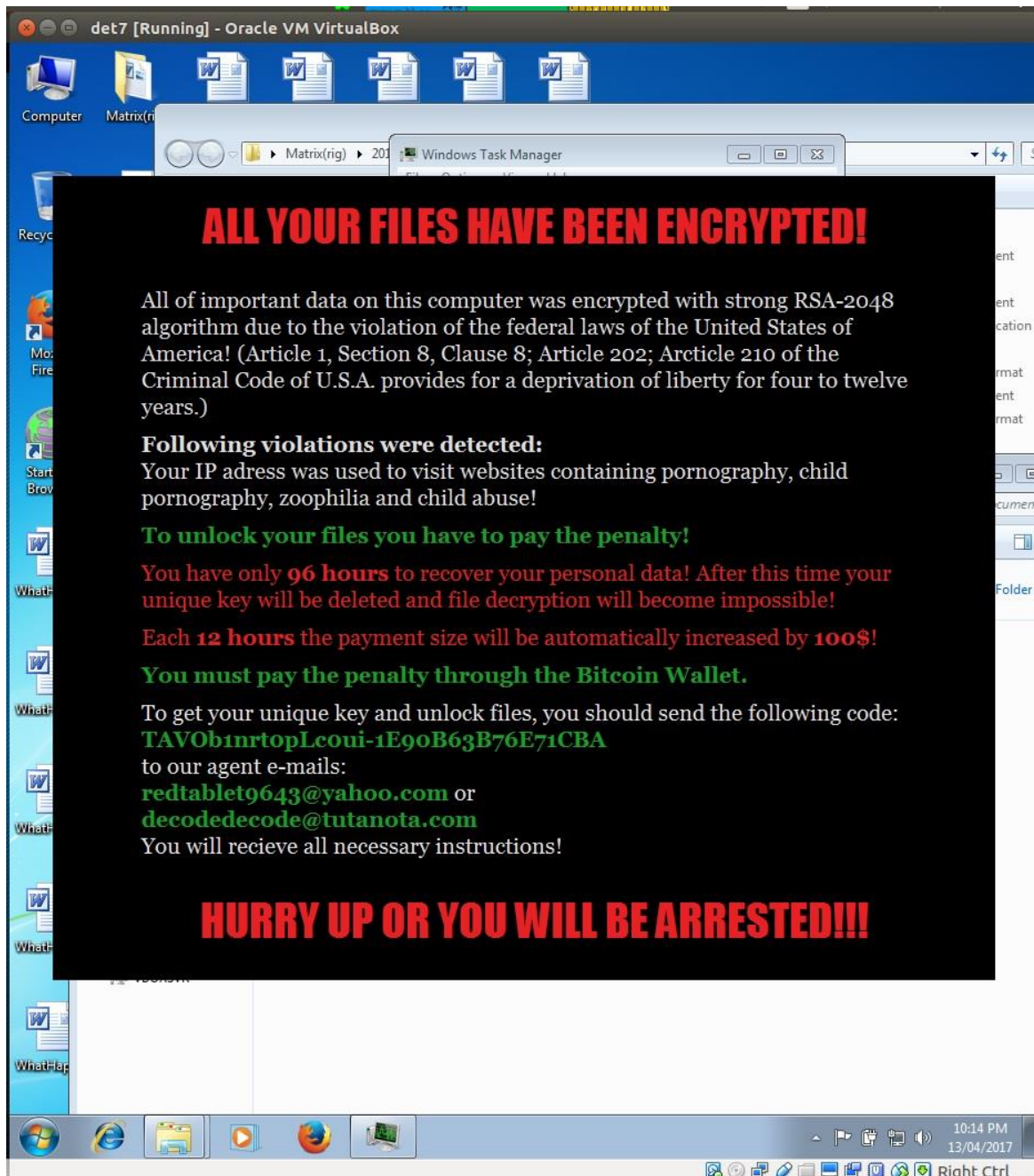
Later in the execution I noted additional executables launching highlighted.



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

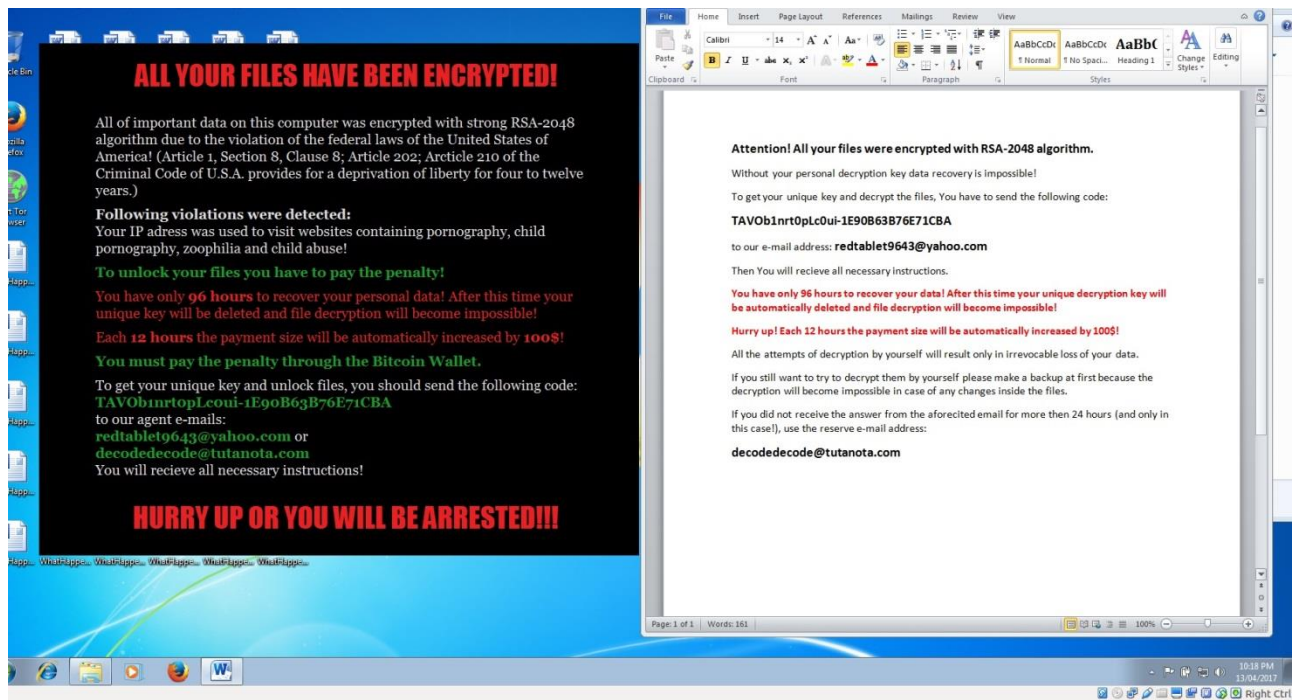


The image shows a Windows 7 desktop environment. In the background, there is a window titled 'det7 [Running] - Oracle VM VirtualBox' and another window titled 'Matrix(rig)'. The desktop has several icons, including 'Computer', 'Matrix(rig)', 'Recycle Bin', 'Mozilla Firefox', 'Start Menu', and 'What's New'. A large black overlay with red and green text is centered on the screen. The text reads: 'ALL YOUR FILES HAVE BEEN ENCRYPTED! All of important data on this computer was encrypted with strong RSA-2048 algorithm due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.) Following violations were detected: Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse! To unlock your files you have to pay the penalty! You have only 96 hours to recover your personal data! After this time your unique key will be deleted and file decryption will become impossible! Each 12 hours the payment size will be automatically increased by 100\$! You must pay the penalty through the Bitcoin Wallet. To get your unique key and unlock files, you should send the following code: TAVOb1nrtpLcoui-1E9oB63B76E71CBA to our agent e-mails: redtablet9643@yahoo.com or decodedecode@tutanota.com You will receive all necessary instructions! HURRY UP OR YOU WILL BE ARRESTED!!!'. The taskbar at the bottom shows the Start button, several application icons, and the system clock displaying '10:14 PM 13/04/2017'.

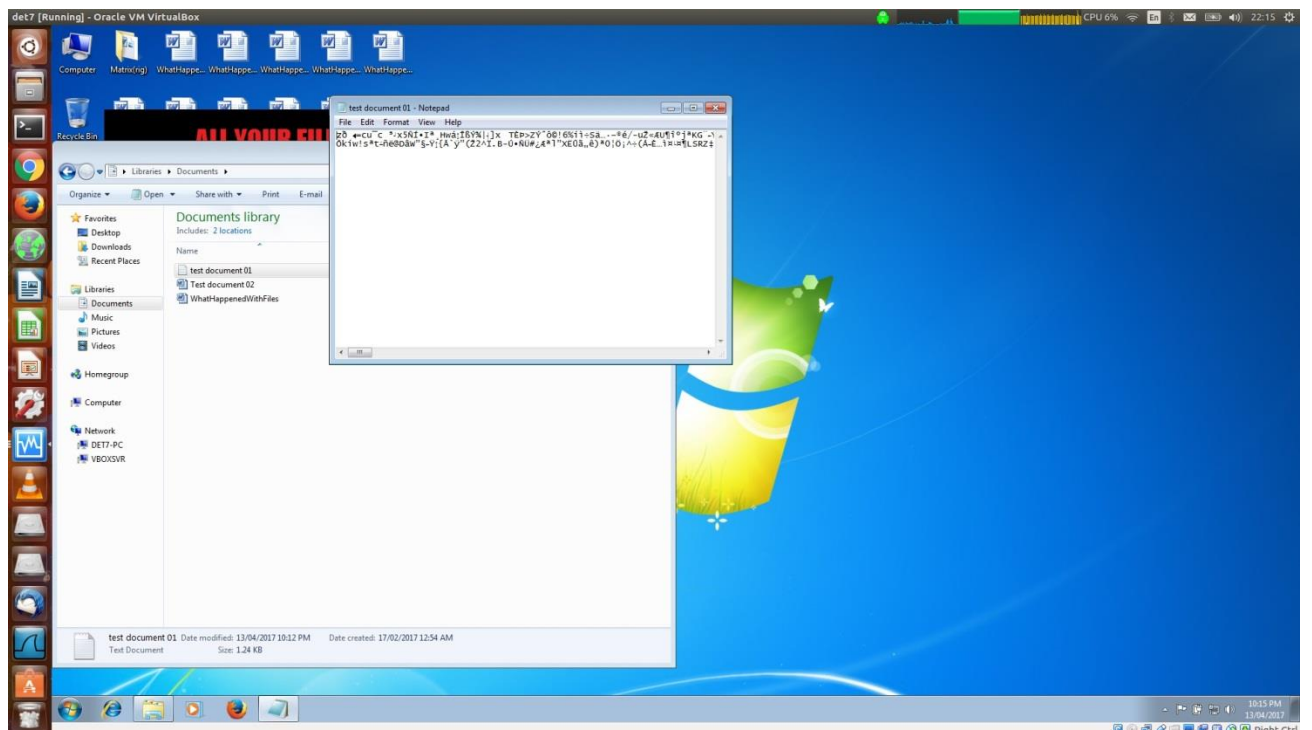




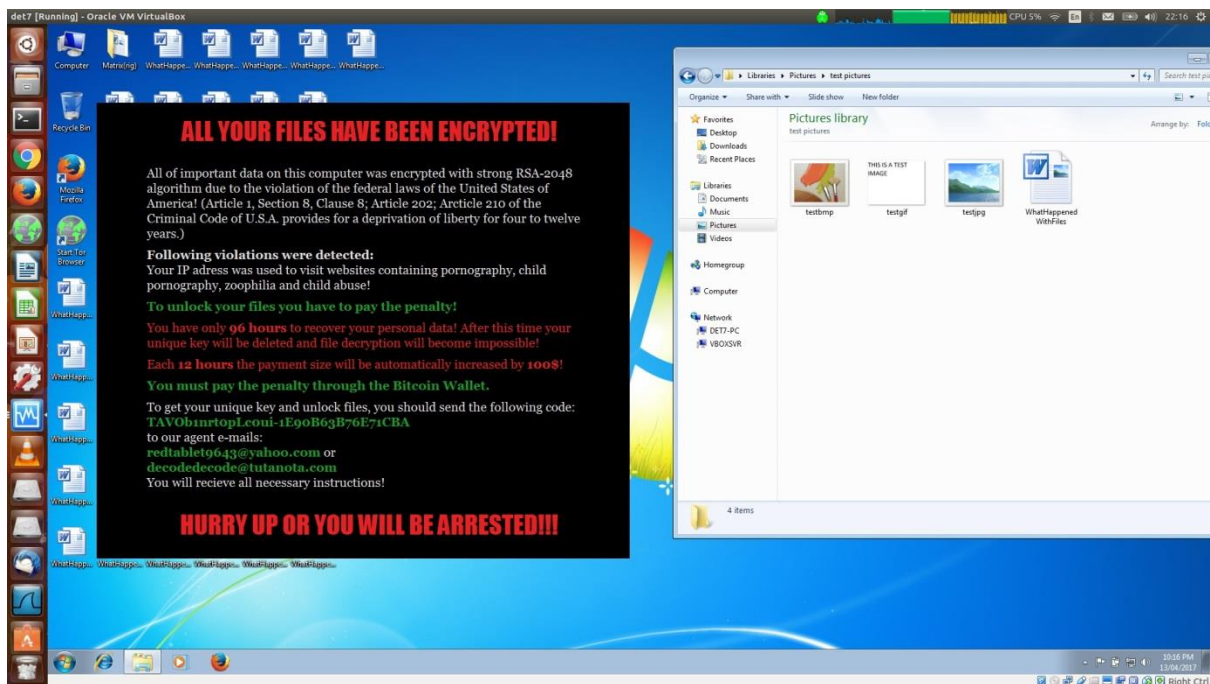
Word documents were generated and dropped just about everywhere, an example of one here which repeats parts of the ransom demand.



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.



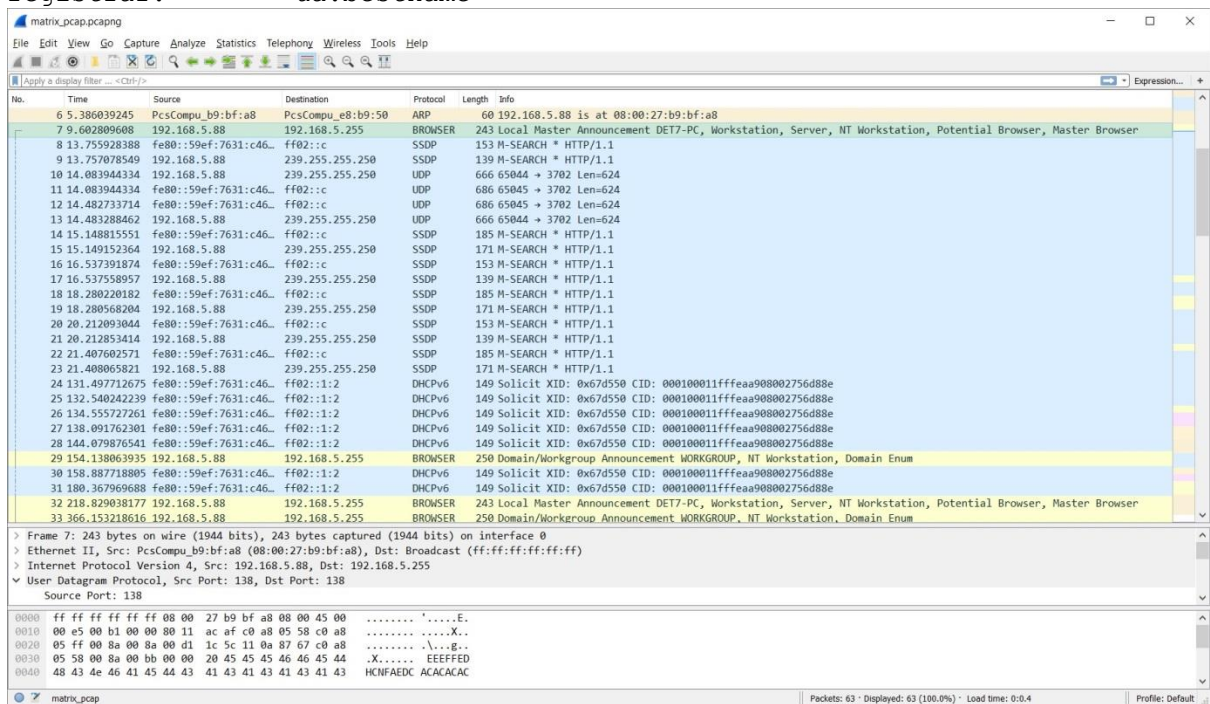
## Packet capture

Starts by quiring the gateway

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

r53.com.ua

registrar: ua.bestname

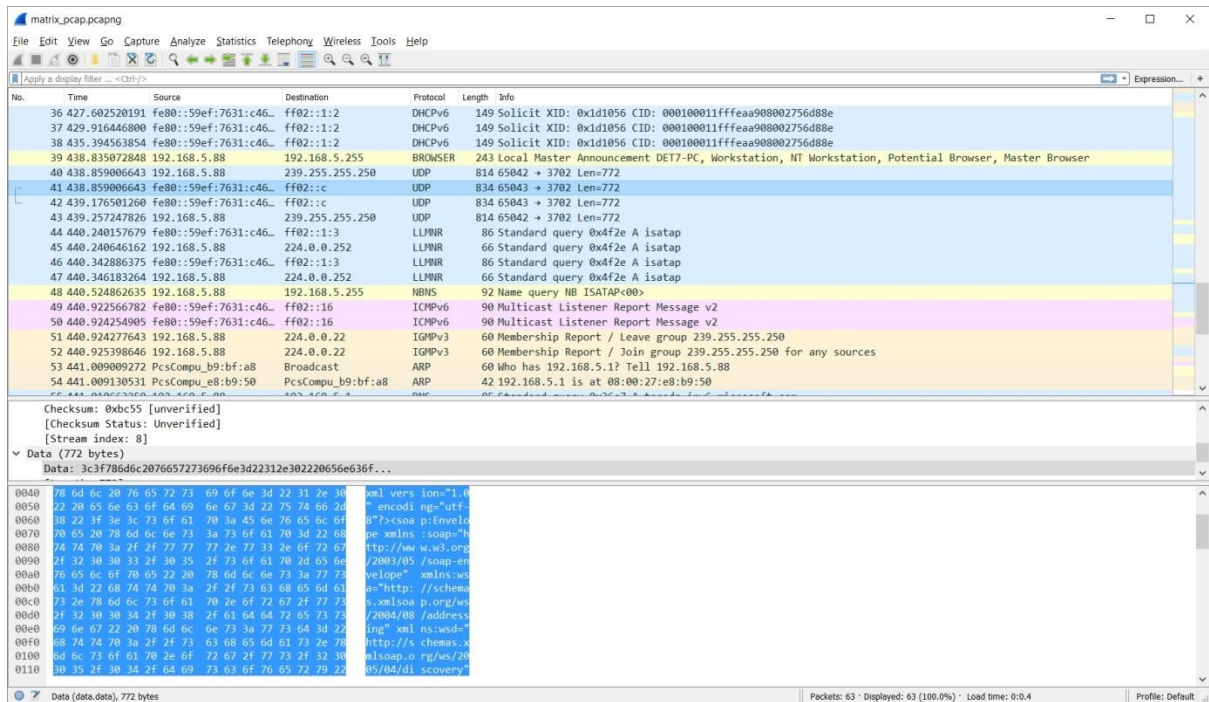


the victim machine then escalates to become the master browser.

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.



No.	Time	Source	Destination	Protocol	Length	Info
37	429.916446800	fe80::59ef:7631:c46...	ff02::1:2	DHCPv6	149	Solicit XID: 0x1d1056 CID: 00010001ffffaa908002756d88e
38	435.394563854	fe80::59ef:7631:c46...	ff02::1:2	DHCPv6	149	Solicit XID: 0x1d1056 CID: 00010001ffffaa908002756d88e
39	438.835072848	192.168.5.88	192.168.5.255	BROWSER	243	Local Master Announcement DET7-PC, Workstation, NT Workstation, Potential Browser, Master Browser
40	438.859006643	192.168.5.88	239.255.255.250	UDP	814	65042 → 3702 Len=772
41	438.859006643	fe80::59ef:7631:c46...	ff02::c	UDP	834	65043 → 3702 Len=772
42	439.176501260	fe80::59ef:7631:c46...	ff02::c	UDP	834	65043 → 3702 Len=772
43	439.257247826	192.168.5.88	239.255.255.250	UDP	814	65042 → 3702 Len=772
44	440.240157679	fe80::59ef:7631:c46...	ff02::1:3	LLMNR	86	Standard query 0x4f2e A isatap
45	440.240646162	192.168.5.88	224.0.0.252	LLMNR	66	Standard query 0x4f2e A isatap
46	440.342886375	fe80::59ef:7631:c46...	ff02::1:3	LLMNR	86	Standard query 0x4f2e A isatap
47	440.346183264	192.168.5.88	224.0.0.252	LLMNR	66	Standard query 0x4f2e A isatap
48	440.524862635	192.168.5.88	192.168.5.255	NBNS	92	Name query NB ISATAP<00>
49	440.922566782	fe80::59ef:7631:c46...	ff02::1:6	ICMPv6	90	Multicast Listener Report Message v2
50	440.924254905	fe80::59ef:7631:c46...	ff02::1:6	ICMPv6	90	Multicast Listener Report Message v2
51	440.924277643	192.168.5.88	224.0.0.22	IGMPv3	60	Membership Report / Leave group 239.255.255.250
52	440.925398646	192.168.5.88	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
53	441.009009272	PcsCompu_b9:bf:a8	Broadcast	ARP	60	Who has 192.168.5.1? Tell 192.168.5.88
54	441.009130531	PcsCompu_e8:b9:50	PcsCompu_b9:bf:a8	ARP	42	192.168.5.1 is at 08:00:27:e8:b9:50
55	441.010663258	192.168.5.88	192.168.5.1	DNS	85	Standard query 0x36c7 A teredo.ipv6.microsoft.com
56	441.174985820	192.168.5.1	192.168.5.88	DNS	181	Standard query response 0x36c7 A teredo.ipv6.microsoft.com CNAME onpremiwindows.ipv6.microsoft.com.akadns.net ...
57	441.194715816	192.168.5.88	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
58	441.194786377	fe80::59ef:7631:c46...	ff02::1:6	ICMPv6	90	Multicast Listener Report Message v2
59	441.209324334	192.168.5.88	192.168.5.255	NBNS	92	Name query NB ISATAP<00>
60	442.017252140	192.168.5.88	192.168.5.255	NBNS	92	Name query NB ISATAP<00>
61	446.179131041	PcsCompu_e8:b9:50	PcsCompu_b9:bf:a8	ARP	42	Who has 192.168.5.88? Tell 192.168.5.1
62	447.179475017	PcsCompu_e8:b9:50	PcsCompu_b9:bf:a8	ARP	42	Who has 192.168.5.88? Tell 192.168.5.1
63	448.179232456	PcsCompu_e8:b9:50	PcsCompu_b9:bf:a8	ARP	42	Who has 192.168.5.88? Tell 192.168.5.1

> Frame 63: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 > Ethernet II, Src: PcsCompu\_e8:b9:50 (08:00:27:e8:b9:50), Dst: PcsCompu\_b9:bf:a8 (08:00:27:b9:bf:a8)  
 > Address Resolution Protocol (request)

```

0000  08 00 27 b9 bf a8 08 00 27 e8 b9 50 08 06 00 01  ..'.....'.P....
0010  08 00 06 04 00 01 08 00 27 e8 b9 50 c8 a8 05 01  ....P.....'.P....
0020  00 00 00 00 00 00 c0 a8 05 58  ....X

```

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