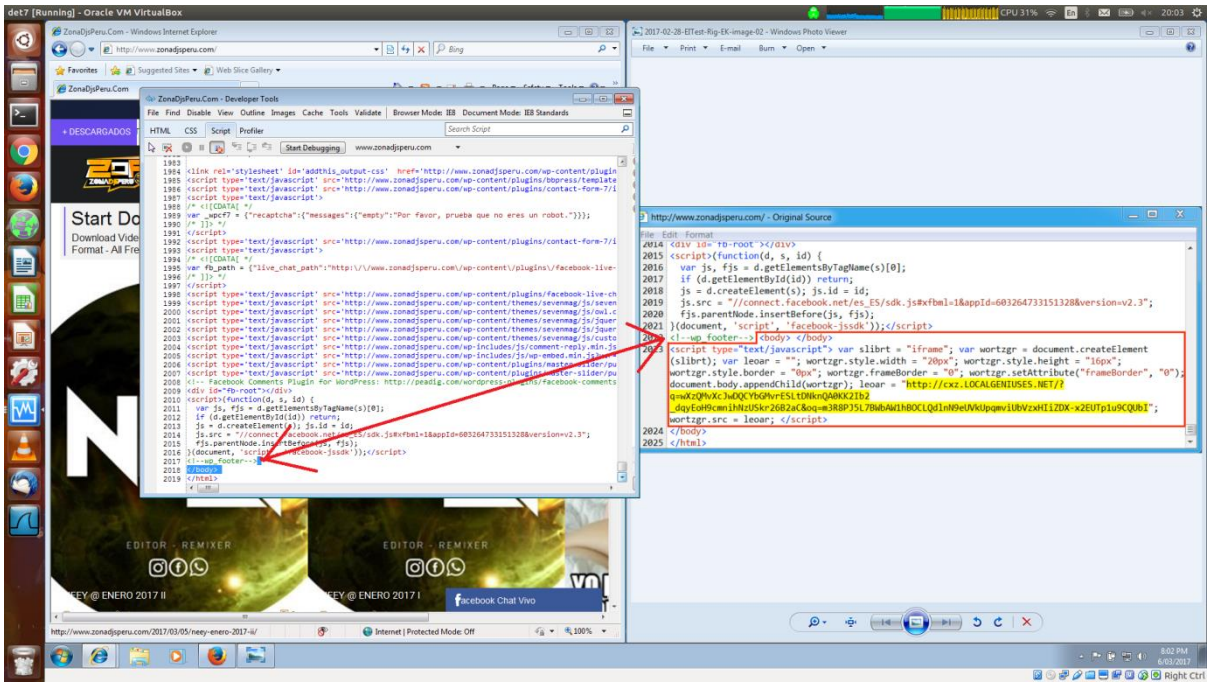
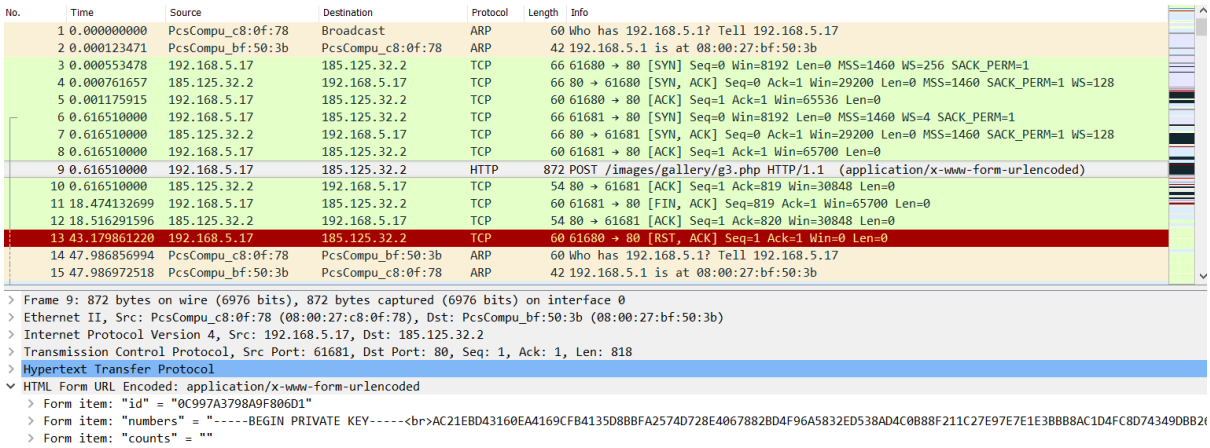
# A look at cryptoshield

Cryptoshield was seen been delivered through RIG EK through web injection, which was clear by the time I looked into the website.




Within a windows7 VM we can see on the left where I have gone to the previously infected page and looking through the code you can see where the highlighted (right side window) code was injected within the page to effect delivery of the ransomware.

Looking at the packet capture we can see contact through TCP port 61680/61681 to 185.125.32.2 which appears to be based within Turkey.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | PcsCompu_c8:0f:78 | Broadcast | ARP | 60 | Who has 192.168.5.1? Tell 192.168.5.17 |
| 2 | 0.000123471 | PcsCompu_bf:50:3b | PcsCompu_c8:0f:78 | ARP | 42 | 192.168.5.1 is at 08:00:27:bf:50:3b |
| 3 | 0.000553478 | 192.168.5.17 | 185.125.32.2 | TCP | 66 | 61680 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 4 | 0.000761657 | 185.125.32.2 | 192.168.5.17 | TCP | 66 | 80 → 61680 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 5 | 0.001175915 | 192.168.5.17 | 185.125.32.2 | TCP | 60 | 61680 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 6 | 0.616510000 | 192.168.5.17 | 185.125.32.2 | TCP | 66 | 61681 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 7 | 0.616510000 | 185.125.32.2 | 192.168.5.17 | TCP | 66 | 80 → 61681 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 8 | 0.616510000 | 192.168.5.17 | 185.125.32.2 | TCP | 60 | 61681 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0 |
| 9 | 0.616510000 | 192.168.5.17 | 185.125.32.2 | HTTP | 872 | POST /images/gallery/g3.php HTTP/1.1 (application/x-www-form-urlencoded) |
| 10 | 0.616510000 | 185.125.32.2 | 192.168.5.17 | TCP | 54 | 80 → 61681 [ACK] Seq=1 Ack=819 Win=30848 Len=0 |
| 11 | 18.474132699 | 192.168.5.17 | 185.125.32.2 | TCP | 60 | 61681 → 80 [FIN, ACK] Seq=819 Ack=1 Win=65700 Len=0 |
| 12 | 18.516291596 | 185.125.32.2 | 192.168.5.17 | TCP | 54 | 80 → 61681 [ACK] Seq=1 Ack=820 Win=30848 Len=0 |
| 13 | 43.179861220 | 192.168.5.17 | 185.125.32.2 | TCP | 60 | 61680 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 14 | 47.986856994 | PcsCompu_c8:0f:78 | PcsCompu_bf:50:3b | ARP | 60 | Who has 192.168.5.1? Tell 192.168.5.17 |
| 15 | 47.986972518 | PcsCompu_bf:50:3b | PcsCompu_c8:0f:78 | ARP | 42 | 192.168.5.1 is at 08:00:27:bf:50:3b |

```
> Frame 9: 872 bytes on wire (6976 bits), 872 bytes captured (6976 bits) on interface 0
> Ethernet II, Src: PcsCompu_c8:0f:78 (08:00:27:c8:0f:78), Dst: PcsCompu_bf:50:3b (08:00:27:bf:50:3b)
> Internet Protocol Version 4, Src: 192.168.5.17, Dst: 185.125.32.2
> Transmission Control Protocol, Src Port: 61681, Dst Port: 80, Seq: 1, Ack: 1, Len: 818
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "id" = "0C997A3798A9F806D1"
    > Form item: "numbers" = "-----BEGIN PRIVATE KEY-----<br>AC21EBD43160EA4169CFB4135D8BBFA2574D728E4067882BD4F96A5832ED538AD4C0B88F211C27E97E7E1E3BBB8AC1D4FC8D74349DBB2
    > Form item: "counts" = ""
```

Lookup of the IP address 185.125.32.2

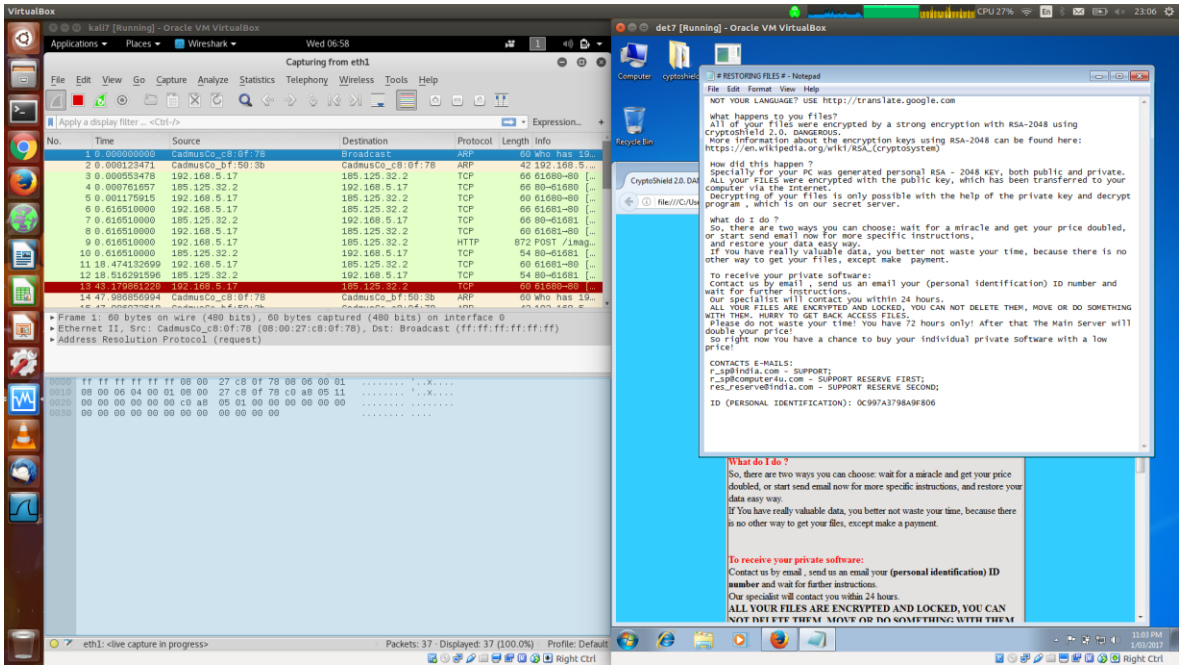
```
% Abuse contact for '185.125.32.0 - 185.125.35.255' is 'legal@hosthink.net'

inetnum:        185.125.32.0 - 185.125.35.255
netname:        TR-HOSTHINKIS-20151106
country:        TR
org:            ORG-SIHV2-RIPE
admin-c:        HIS63-RIPE
tech-c:         HIS63-RIPE
status:         ALLOCATED PA
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      tr-hosthinkis-1-mnt
mnt-routes:     tr-hosthinkis-1-mnt
created:        2015-11-06T07:49:33Z
last-modified:  2016-04-14T10:24:07Z
source:         RIPE

organisation:   ORG-SIHV2-RIPE
org-name:       Sembol Internet Hizmetleri ve Dis Ticaret Ltd
org-type:       LIR
address:        Seyrantepe Nato St. No 2 / 2 Kagithane
address:        34418
address:        Istanbul
address:        TURKEY
e-mail:         seref@hosthink.net
admin-c:        HIS62-RIPE
tech-c:         HIS62-RIPE
abuse-c:        AR34102-RIPE
mnt-ref:        tr-hosthinkis-1-mnt
mnt-by:         RIPE-NCC-HM-MNT
mnt-ref:        RIPE-NCC-HM-MNT
created:        2015-11-03T14:05:27Z
last-modified:  2016-06-14T07:48:50Z
source:         RIPE
phone:          +908503023025

role:           Hosthink Internet Services
address:        Seyrantepe Nato Cad. Nato Cikmazi No:2/2 Kagithane Istanbul
e-mail:         info@hosthink.net
abuse-mailbox:  legal@hosthink.net
nic-hdl:        HIS63-RIPE
```

Once deployed, queries of the local network are done looking for additional points to encrypt. Contact is also made with

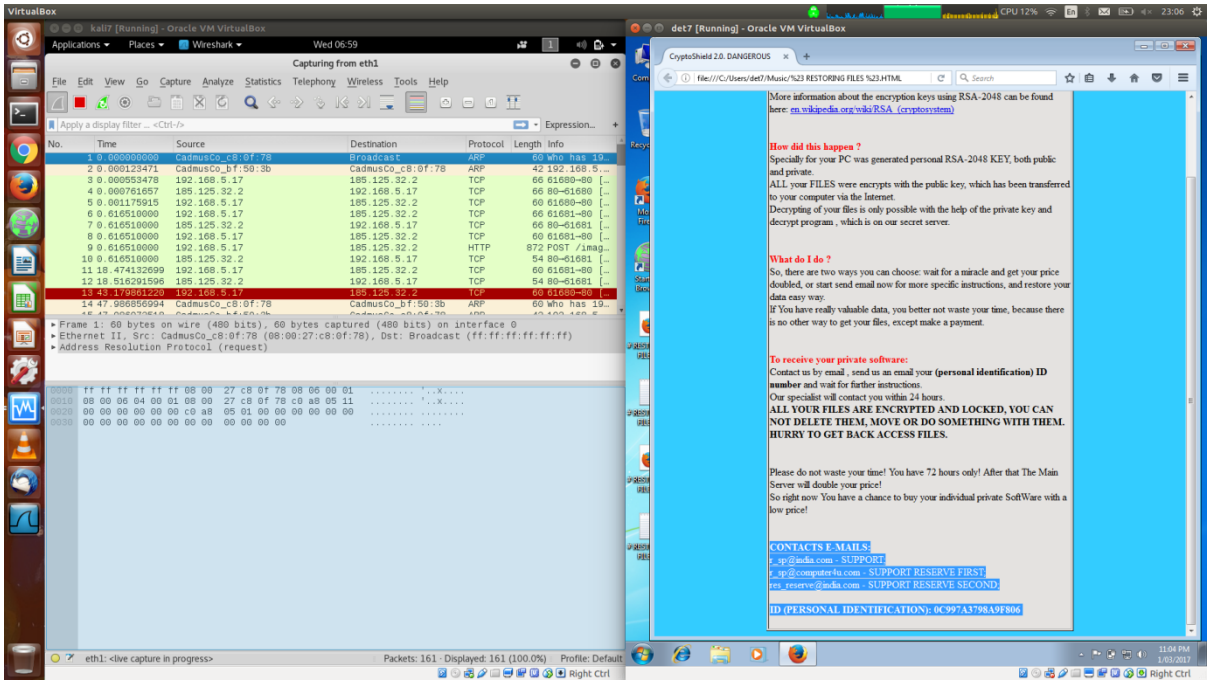
- 52.25.169.254 amazon hosting TCP 61686.
- 54.192.139.169 cloudfront hosting TCP 61687

Further communication noted on other IP's but not recorded here.

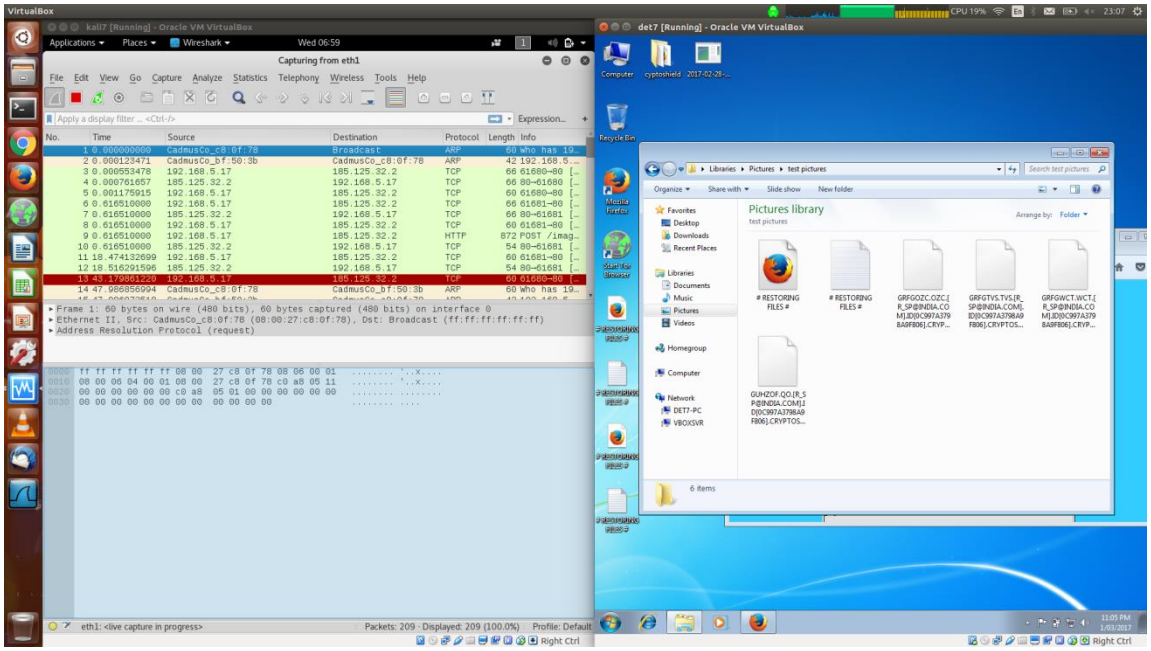
The payload itself is very quick to function and is simple and no nonsense in design. Here we can see the payload start to function with the left window showing the traffic and right window displaying the ransom demand.

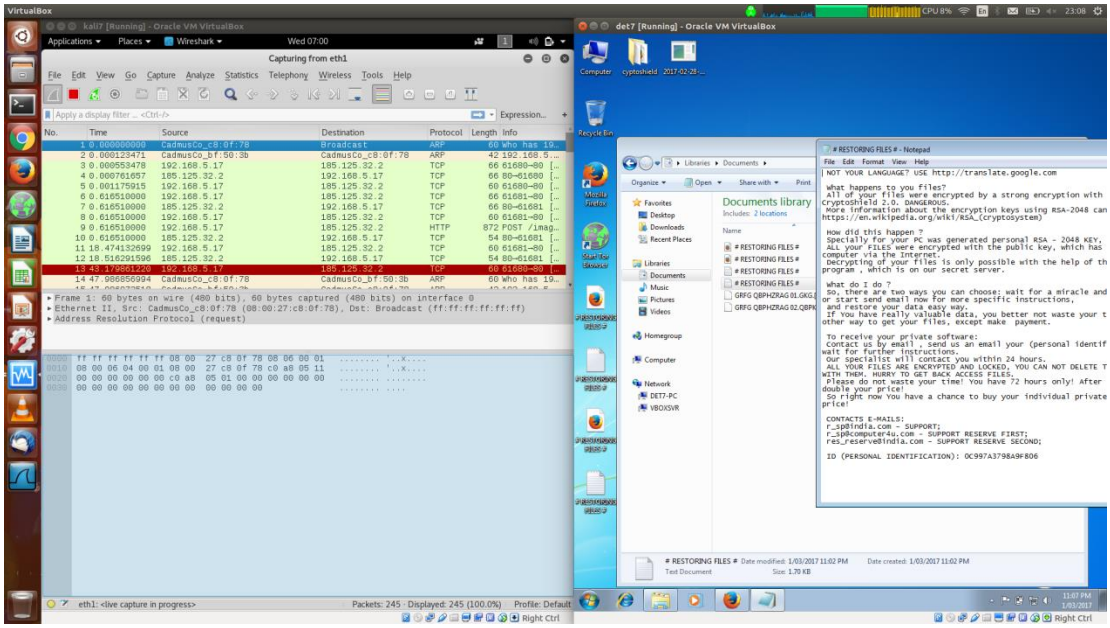


The webpage and text file provides simple instruction on what has occurred and provides contact information and a 72 hour window with which to “unlock your files”




Observing my test documents and pictures shows successful encryption of all the file types including text files which I have noted other ransomware avoids encrypting.





A look at my documents folder right side.

Cuckoo analysis showed a LARGE number of python files, which would take pages to list. I noted a few registry entries

**Registry keys opened**

- HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\RunOnce

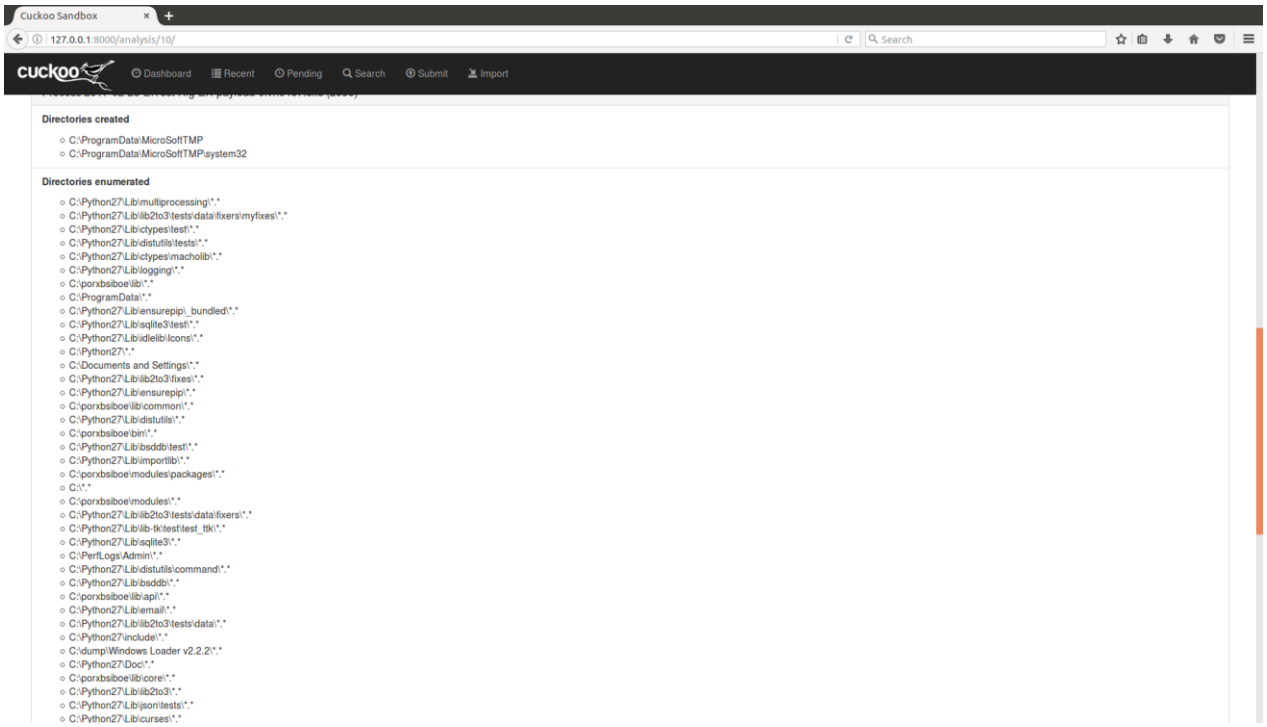
**Registry keys written**

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Oracle Microsoft
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Oracle Microsoft Updater
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce*Oracle Microsoft Updater
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce*Oracle Microsoft

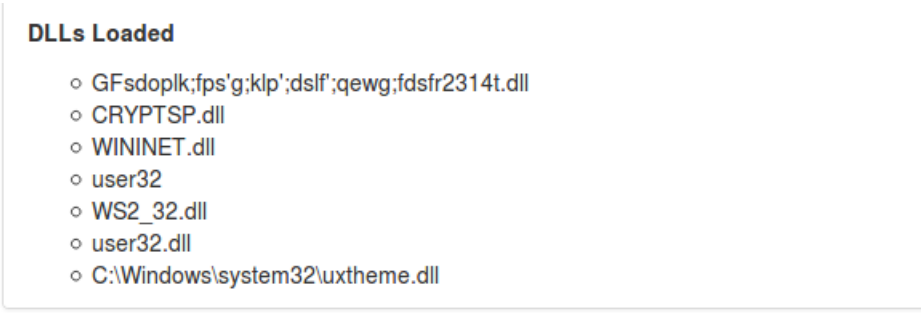
**Registry keys read**

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags

There was also a large number of folders enumerated which I believe has to do with the encryption process been they all are *.*, I also noted the two folders created likely for persistence.




Processes loaded




There is talk online of decryption processes for Cryptoshield however I did not find out how effective these are. It's also rumoured that it may not work on newer versions such as this.

Thankyou

mbyx