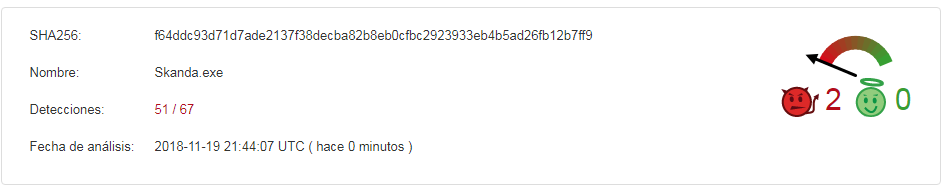
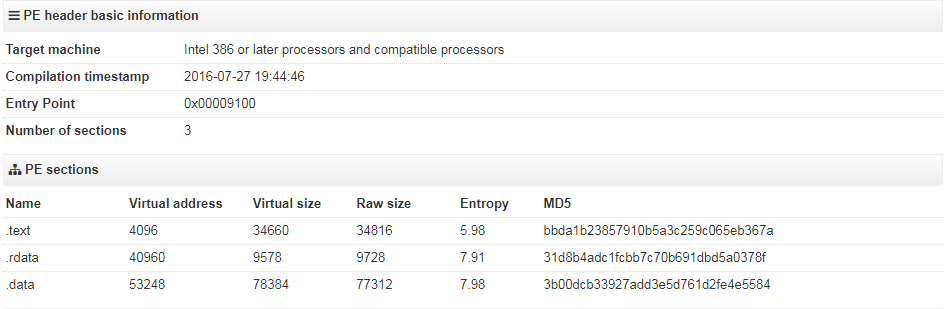
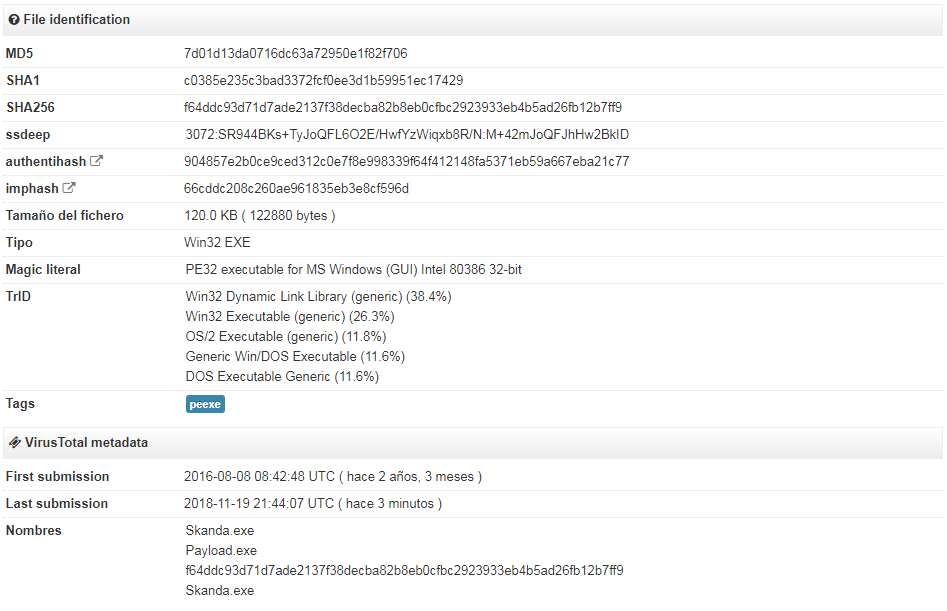
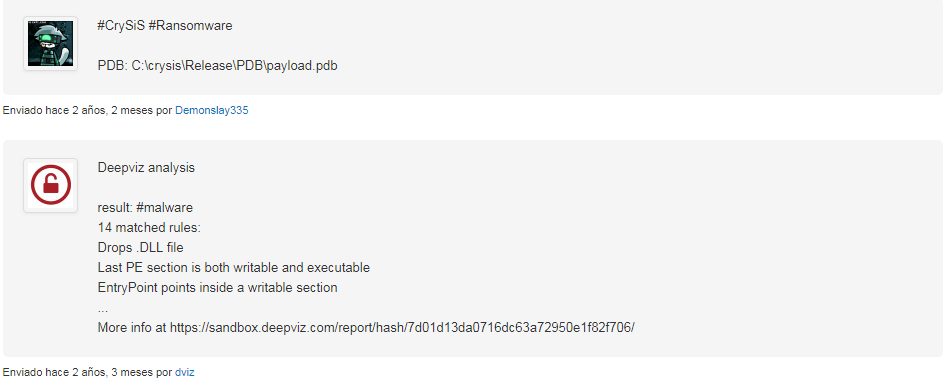
**Análisis del ransomware en virus total**







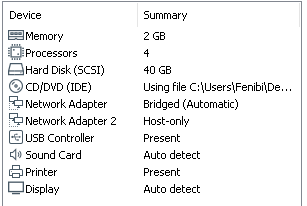




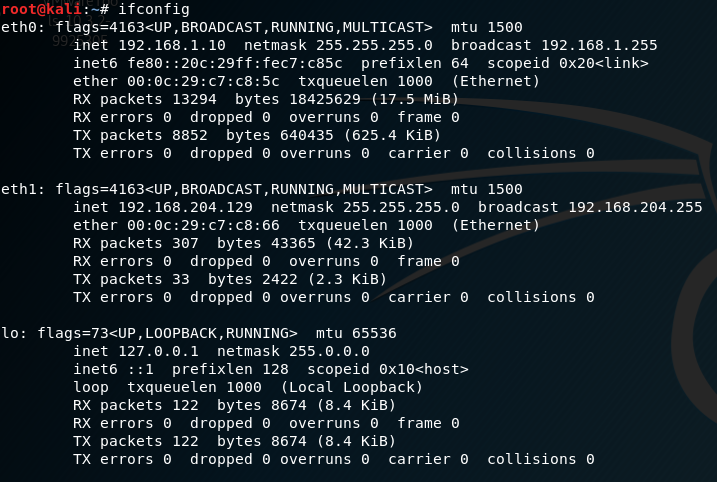
El verdadero nombre del ransomware es Crysis.

**Configuración del setup**

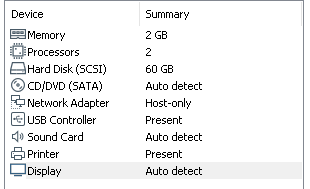
* Máquina con Kali Linux:

****

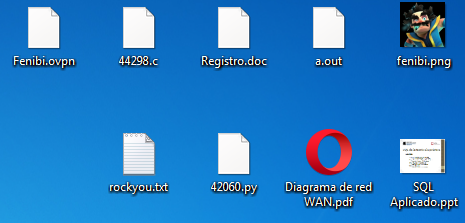
Donde se configuraron dos adaptadores de red, uno en modo ‘host-only’ (eth1) y el otro en modo bridge (eth0) con salida hacia internet.



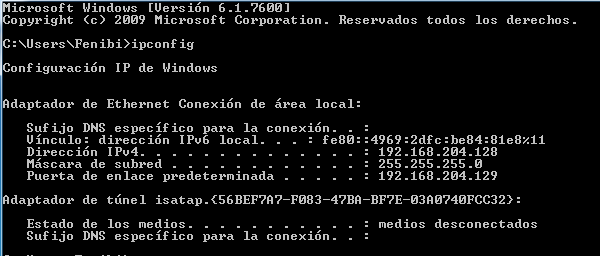
* Máquina con W7 en donde se va a correr la aplicación, en una máquina virtual con las siguientes características.



En el escritorio se colocan archivos con diferentes formatos para ver si a todos los archivos los cifra o no.

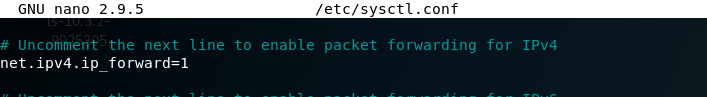


La conexión de red está configurada como ‘Host-only’ en donde tiene configurado como puerta de enlace una de las IPs asignadas a el Kali.



* Luego configuramos el IpTables para que todo lo que salga del w7, entre al eth1 del Kali y se fordwardee al eth0 y viceversa. De esta manera el Kali funciona como una especie de proxy.

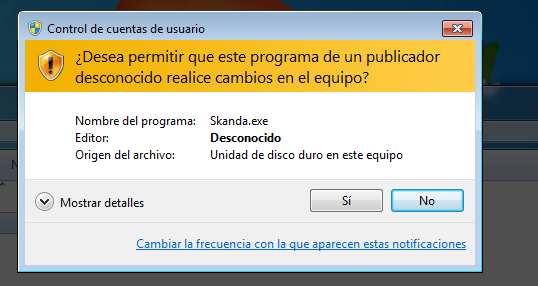
Fuente: https://unix.stackexchange.com/questions/126595/iptables-forward-all-traffic-to-interface







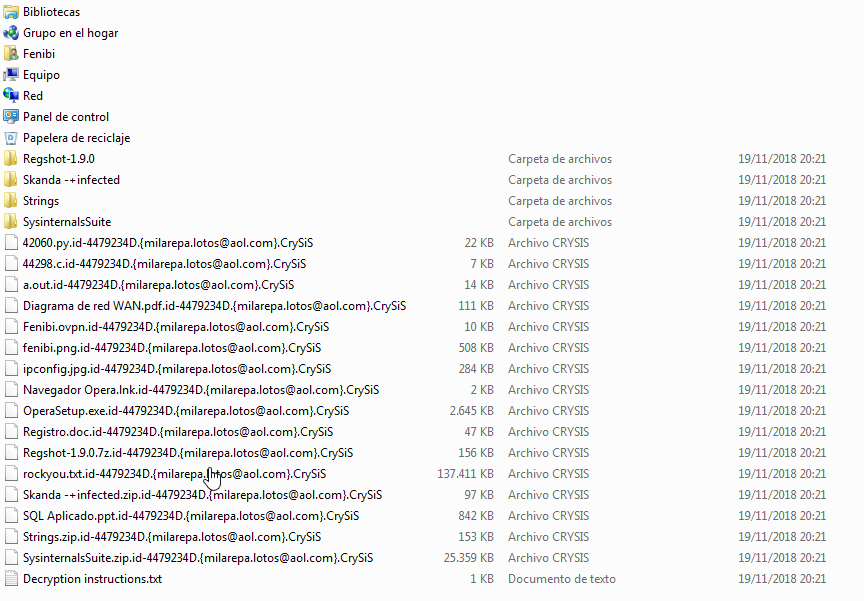
**Corriendo el malware**



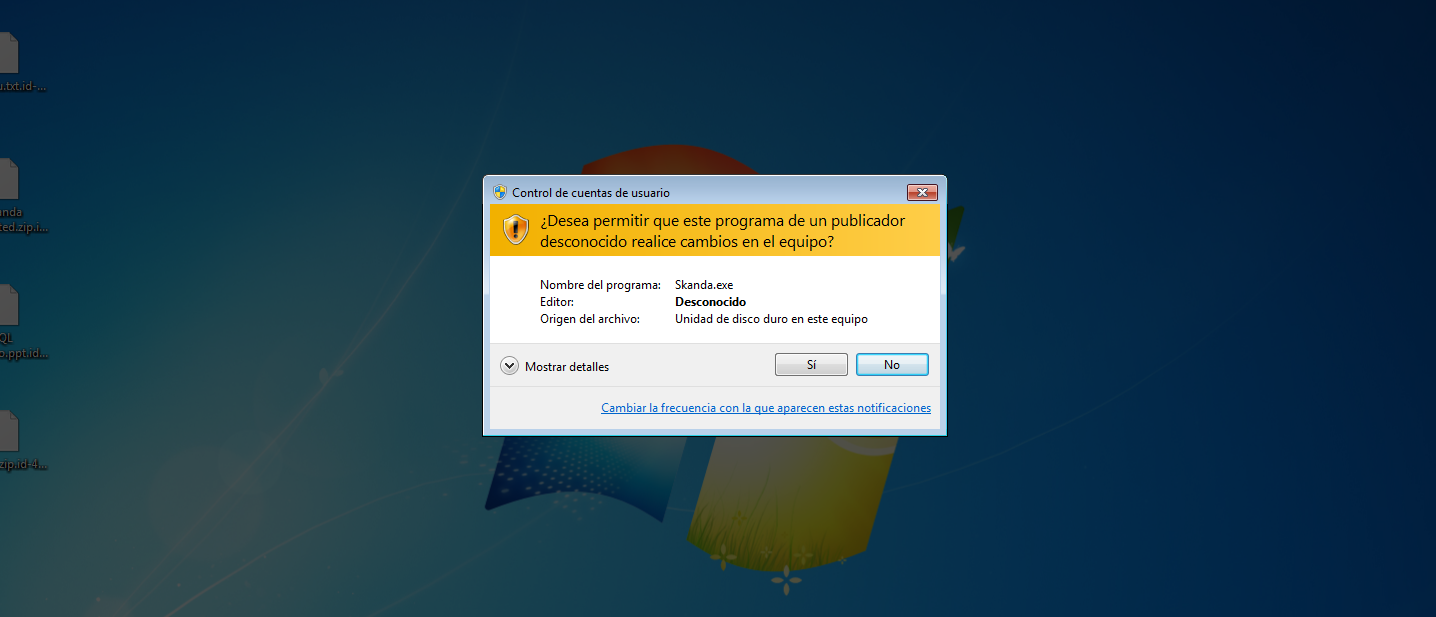
Se cambió el fondo de escritorio con una imagen de la milicia con un mensaje y también se creó un file txt con un mensaje para ‘salvar’ los datos.



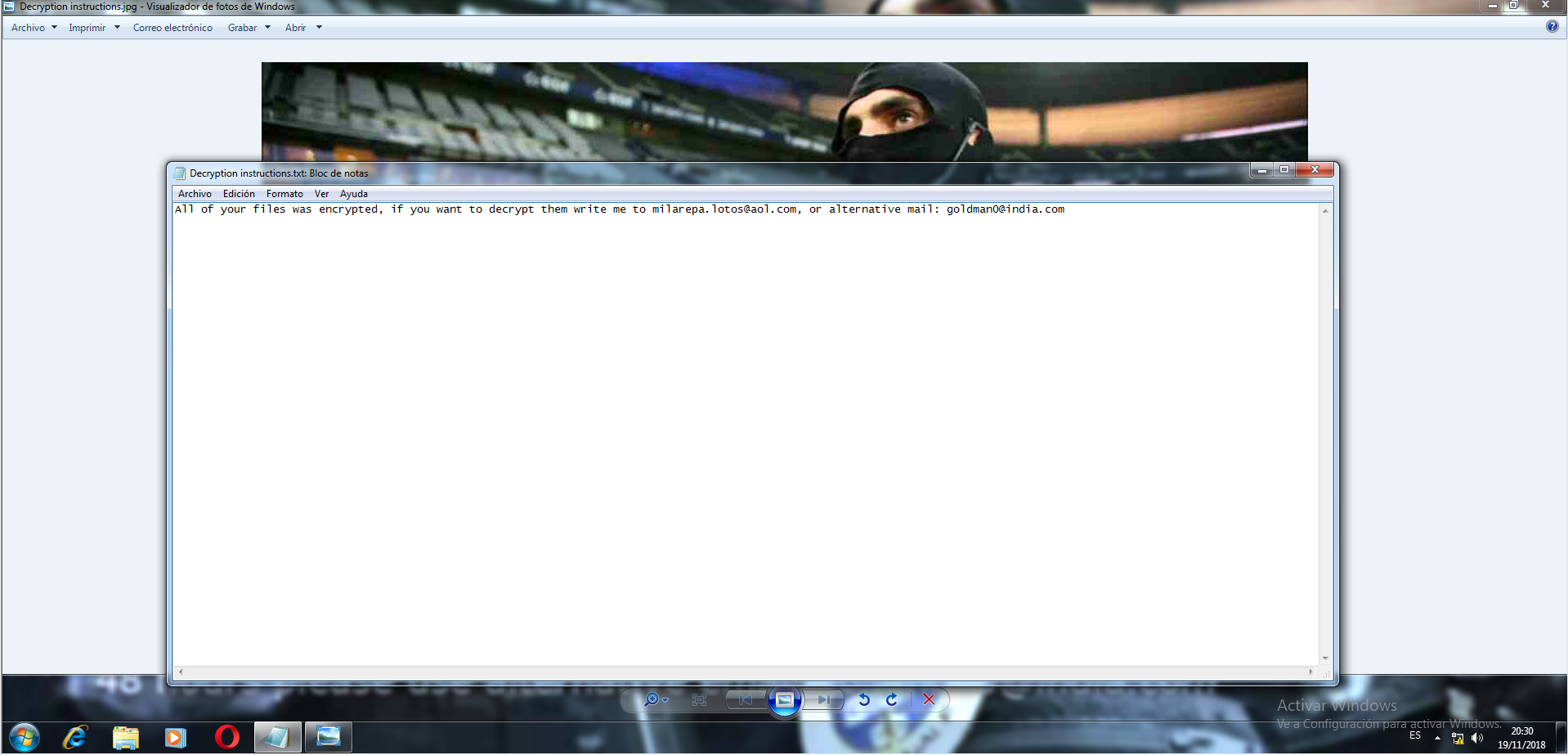
Todos los files de prueba fueron encriptados.



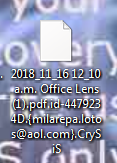
Luego de reiniciar el programa busca iniciarse nuevamente.



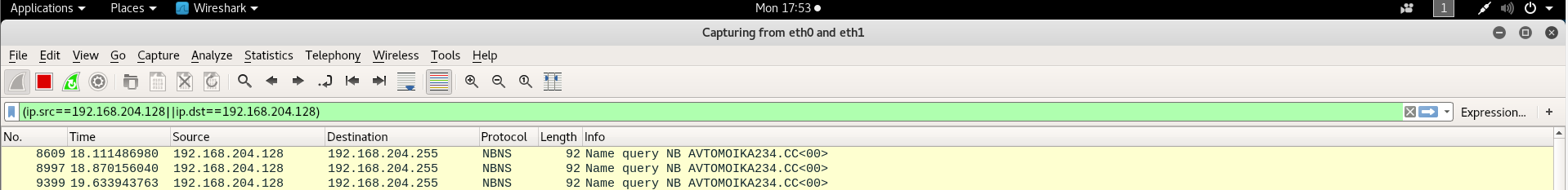
Por más que le dé no, el programa cambia de fondo y abre el archivo de imagen y el txt antes descripto.



Había agregado un file antes del reinicio y lo encriptó.

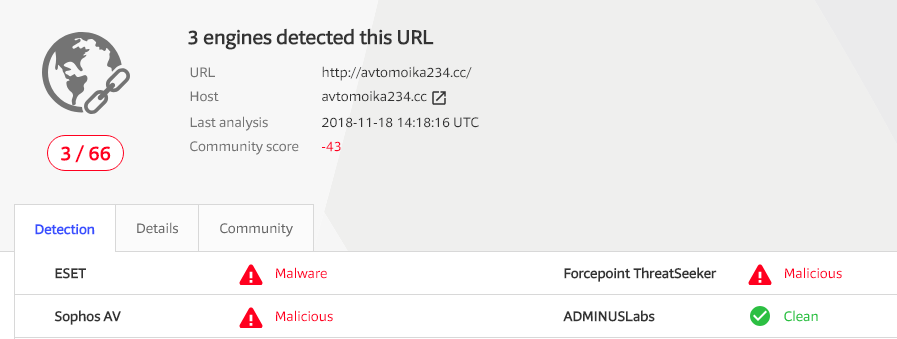


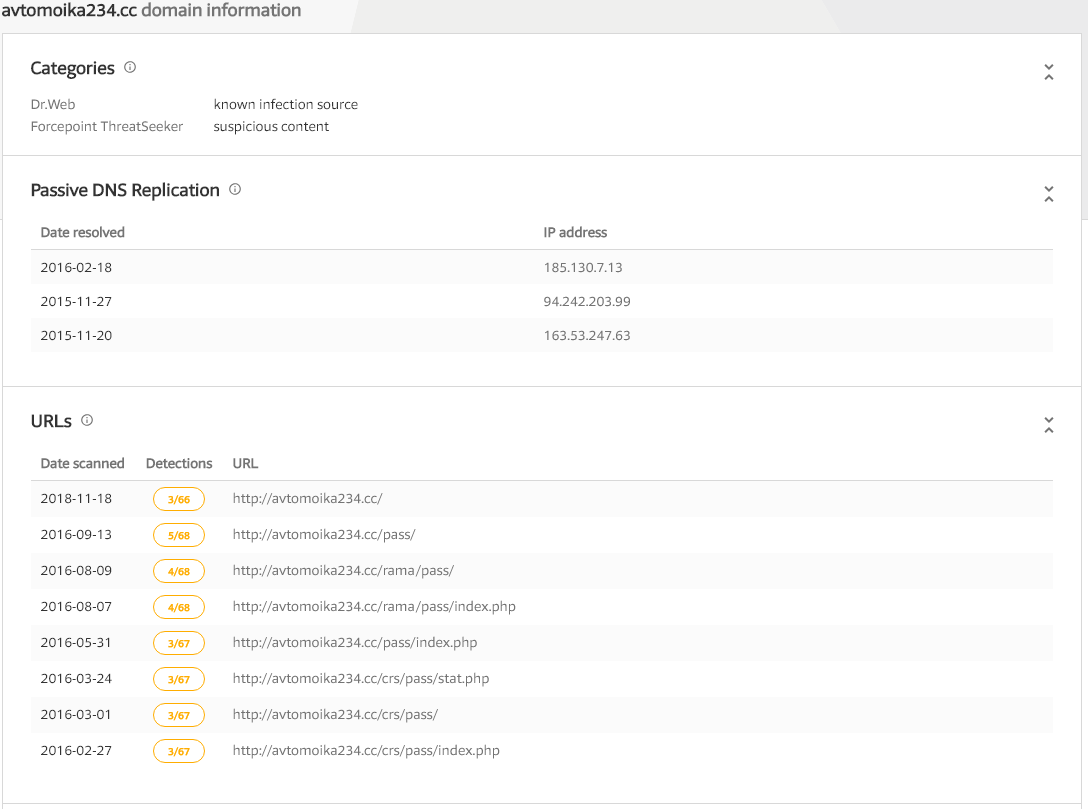
**Dejando un wireshark escuchando en el Kali, y filtrando por la IP del w7, se pueden destacar dos líneas:**

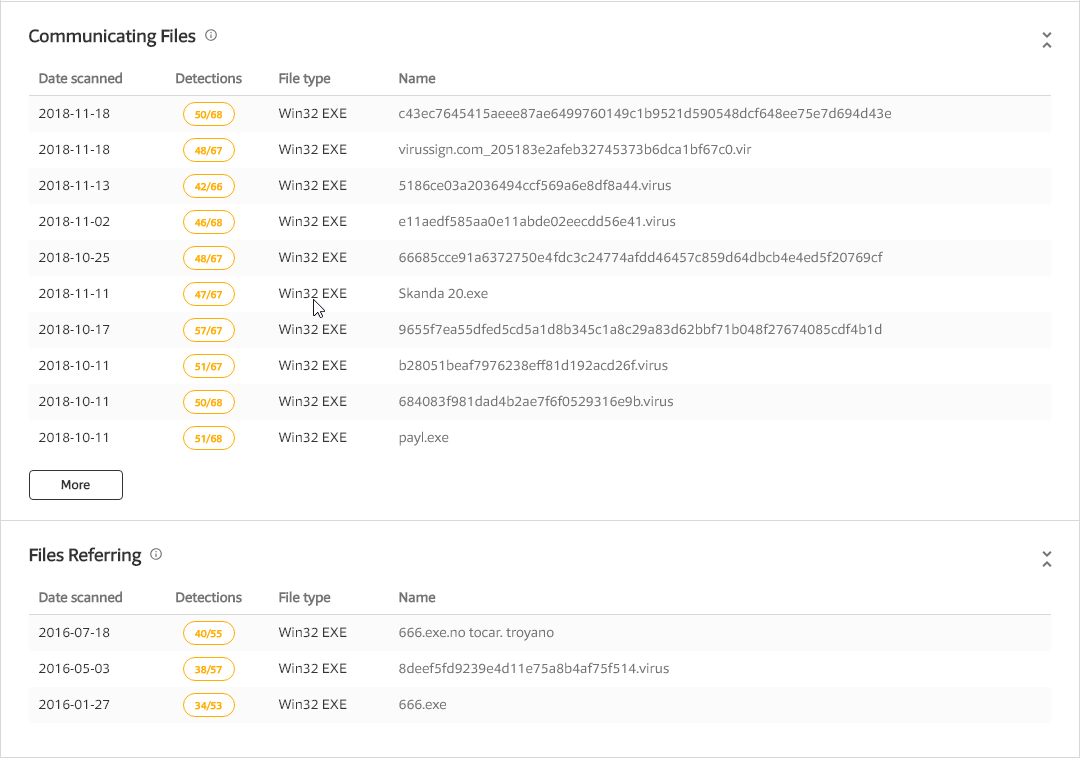
****

****

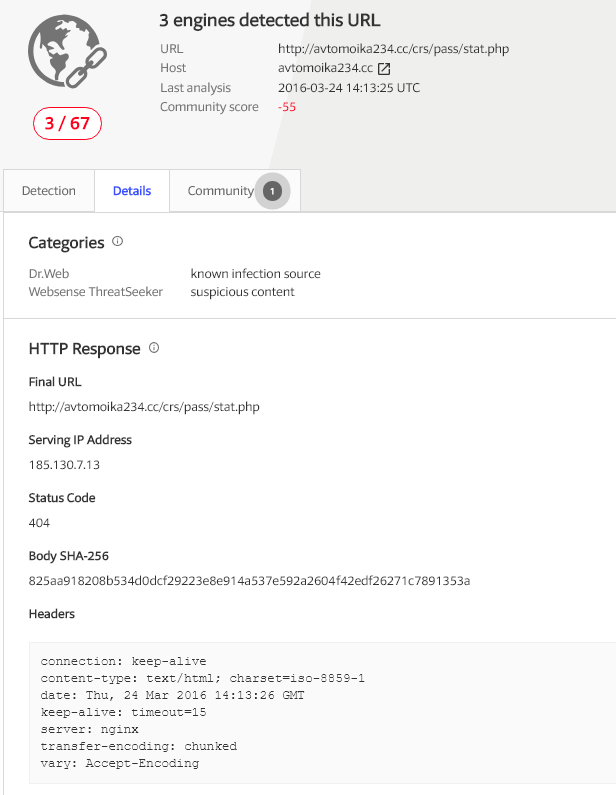
Por ende, podemos analizar esta nueva url en virus total:







Evidentemente, las diferentes versiones del virus buscan el mismo DNS. Si vamos al detalle de una de las URL específicas que está queriendo acceder:



Claramente queda en evidencia que envía solamente un texto plano. (Podría ser la key de desbloqueo con el id)

* Volvemos atrás la VM pero esta vez utilizamos unos programas de análisis dinámico. (ApateDNS, RegShot, ProcMonitor)

