Korsan Yazılımlardaki Tehlike

written by Mert SARICA | 20 November 2010

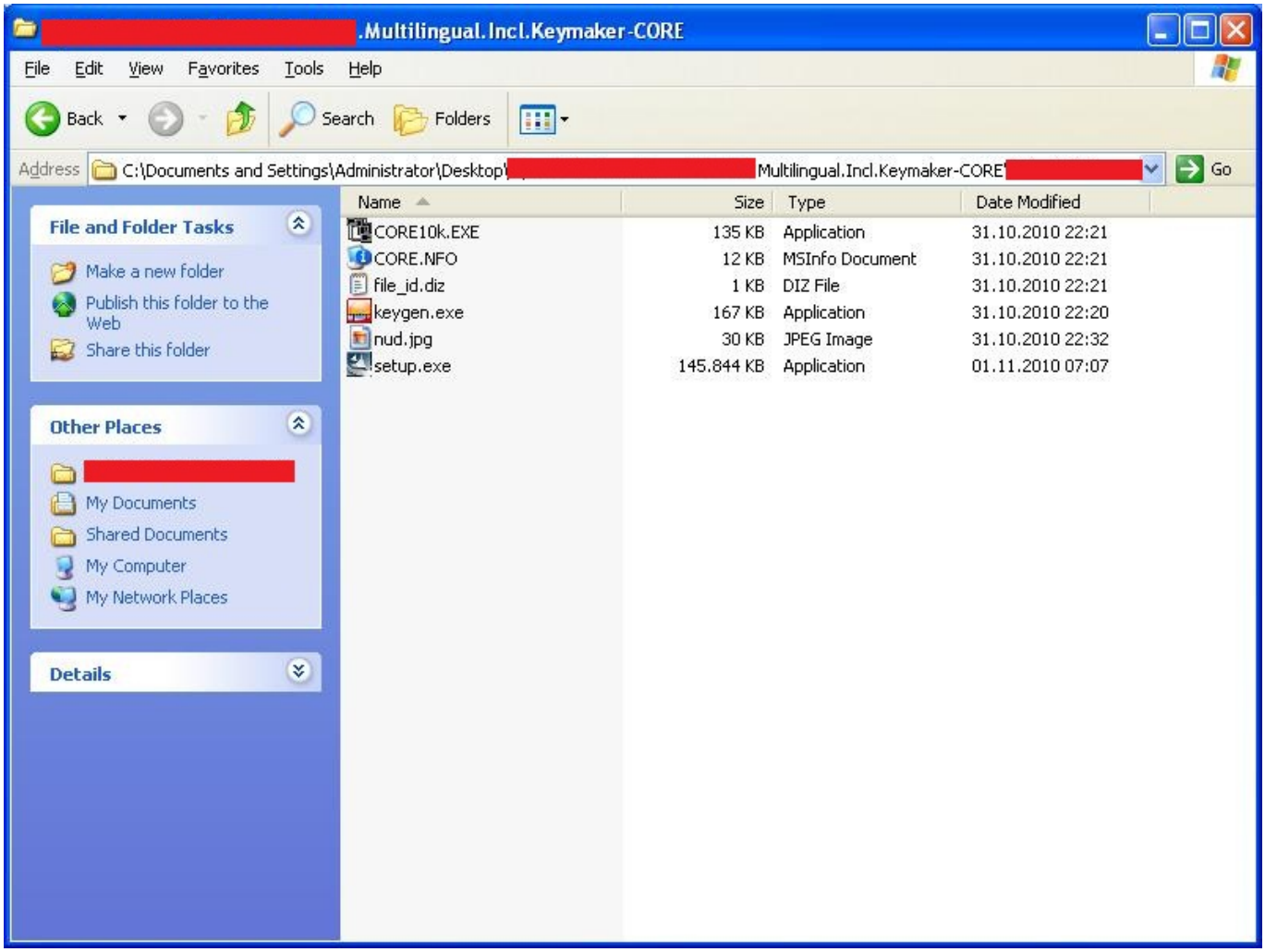
Nedense korsan yazılım denilince aklıma hemen Kadıköy Yazıcıoğlu İşhanı gelir. Orta okul yıllarında (1996-1998) usanmadan sıkılmadan her haftasonu arkadaşlarla buluşup yeni oyun almak için oraya giderdik. Önüne koca koca tezgahlar kurulur, yazılım, oyun, video ne ararsak bulurduk. O zamanlar ne bittorrent ne de başka p2p programları vardı. Warez sitelerden dial-up bağlantı ve 28k modem ile indirmekte peygamber sabrı gerektirirdi. Aradan yıllar geçtikçe öğrendik korsanın ne demek olduğunu, neden emek hırsızlığı olduğunu, neden ülke ekonomisine ve sektöre zarar verdiğini.

Her ne kadar günümüzde korsanla mücadelede büyük adımlar atılıyorda olsa eski yıllara kıyasla bağlantı hızlarının yüksek olması, dosya paylaşım sitelerinin çokluğu ve torrent programlarının neredeyse işletim sistemleri ile kurulu geliyor olması nedeniyle paylaşım kolaylaşıyor, mücadele ise zorlaşıyor.

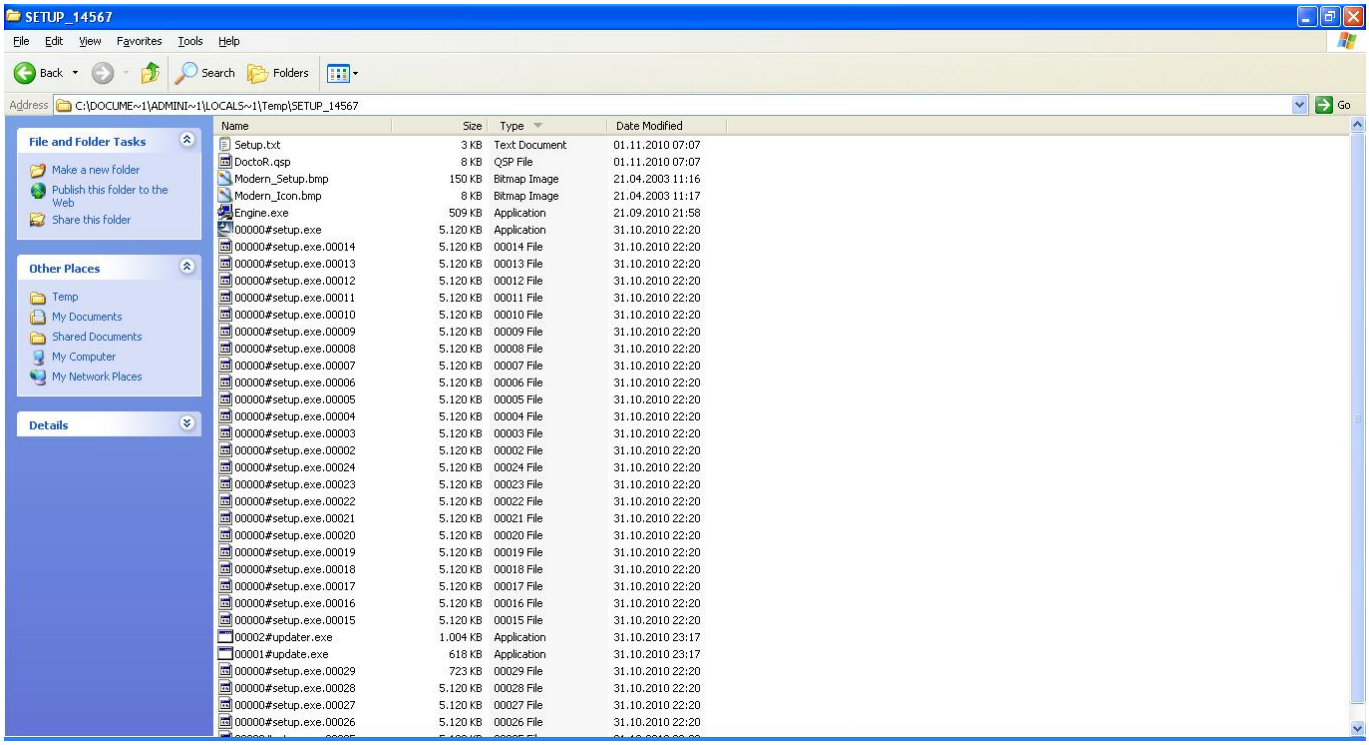
Emek hırsızlığıydı, ekonomiye zararıydı bir kenara, günümüzde korsan yazılım kullanmamanız için çok büyük bir neden daha var, korsan yazılımla gelen zararlı yazılımlar.

Art niyetli kişiler çoğunlukla zararlı yazılımlarını yaymak için o gün için popüler olan sistemleri (misal facebook üzerinden yayılan trojan), insanlanları kandırmak için popüler isimleri veya güncel olayları kullanmayı severler. Korsan yazılım kullanımın yüksek olduğu son yıllarda bu yazılımların art niyetli kişilerin ciddi anlamda hedefi haline ne zaman geleceğini merak eder dururdum.

Yine bir rutin zararlı yazılım kontrolü amacıyla göz attığım popüler paylaşım sitesinden rastgele bir paket indirdim.
Paketi açtığımda her zamanki gibi içinden 1 kurulum dosyası ve bir de keygen dosyası çıktı.



Kurulum dosyasını çalıştırdığımda güvenlik duvarı GoogleUpdate.exe programının bir ip adresi ile haberleşmek istediği uyarısını verdi. Şüpheli bu durum karşısında kurulum paketi tarafından oluşturulan kurulum paketlerine göz atmaya karar verdim. %temp% klasörü içinde oluşturulan ve bu pakete ait olan klasörün içine baktığımda dosya isimleri şüphe duymama yetti.



Kurulumu tekrar başlatıp Procmon ile setup.exe, update.exe, updater.exe ve googleupdate.exe için filtrele hazırladıktan sonra updategillerin davranışlarını yakından inceledim.

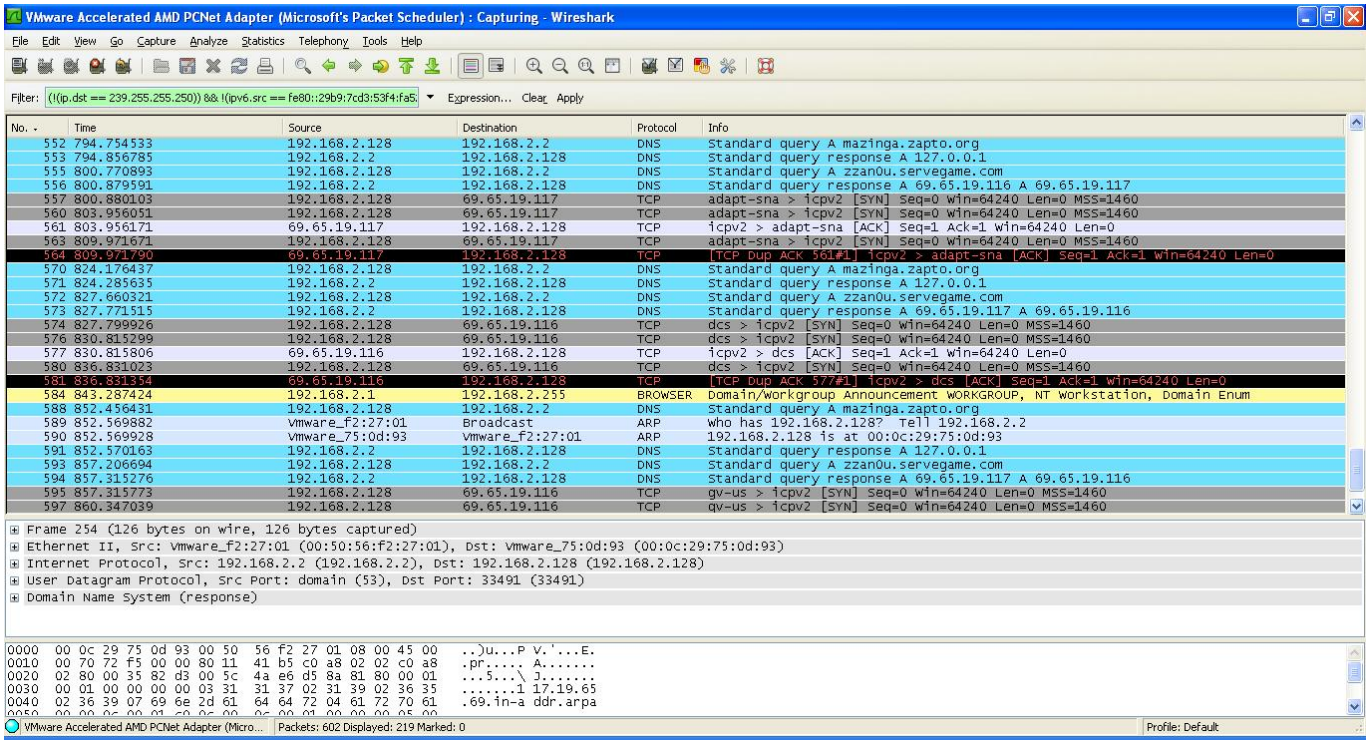
```
updater.exe 196 CreateFile C:\Documents and
Settings\Administrator\Application Data\GoogleUpdate.exe
updater.exe 196 RegSetValue
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\GoogleUpdate

update.exe 3224 CreateFile C:\Program Files\Trillian\users\default\msn.ini
update.exe 3224 CreateFile C:\Program Files\Trillian\users\default\aim.ini
update.exe 3224 CreateFile C:\Program Files\Trillian\users\default\yahoo.ini
update.exe 3224 CreateFile C:\Documents and
Settings\Administrator\Application Data\.purple\accounts.xml
update.exe 3224 CreateFile C:\Documents and Settings\All Users\Application
Data\DynDNS\Updater\config.dyndns
update.exe 3224 QueryEaInformationFile C:\Documents and
Settings\Administrator\Local Settings\Application Data\Google\Chrome\User
Data\Default\Web Data
update.exe 3224 CreateFile C:\Documents and
Settings\Administrator\Application Data\chrtmp
update.exe 3224 CreateFile C:\Documents and
Settings\Administrator\Application Data\Opera\Opera\wand.dat
update.exe 3224 CreateFile C:\Documents and
```

Settings\Administrator\Application Data\FileZilla\recentservers.xml
update.exe 3224 CreateFile C:\Documents and Settings\All Users\Application Data\FlashFXP\3\Sites.dat
update.exe 3224 CreateFile C:\Documents and Settings\Administrator\Application Data\GlobalSCAPE\CuteFTP Pro\8.0\sm.dat
update.exe 3224 CreateFile C:\Documents and Settings\Administrator\Application Data\GlobalSCAPE\CuteFTP Home\8.0\sm.dat
update.exe 3224 CreateFile C:\Documents and Settings\Administrator\Application Data\GlobalSCAPE\CuteFTP Lite\8.0\sm.dat

GoogleUpdate.exe 320 CreateFile C:\Documents and Settings\Administrator\Local Settings\Temp\dclogs.sys
GoogleUpdate.exe 320 CreateFile C:\Documents and Settings\Administrator\Cookies\index.dat
GoogleUpdate.exe 320 CreateFile C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat

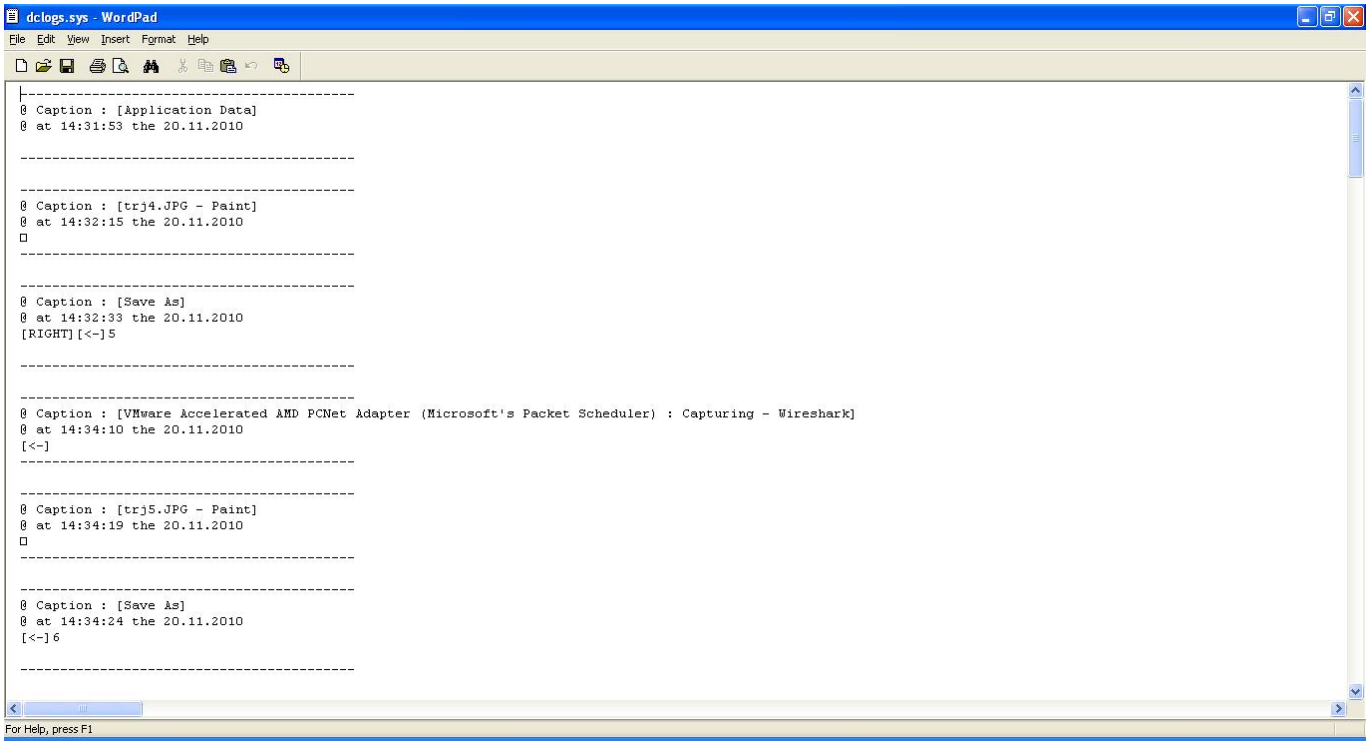
Daha kurulum penceresi gelmeden sistemimdeki bir çok programa bu kadar ilgi ve alaka göstermesi ve başlangıçta çalışmak sistemde değişiklik yapması kurulum dosyasının zararsız olmadığını kanıtlıyor gibiydi.

Wireshark ile trafiği incelediğimde program şüpheli iki alan adı ile iletişime geçmeye çalışıyordu.



Bunun üzerine ek olarak %temp% klasörü altında bulunan dclogs.sys dosyasını

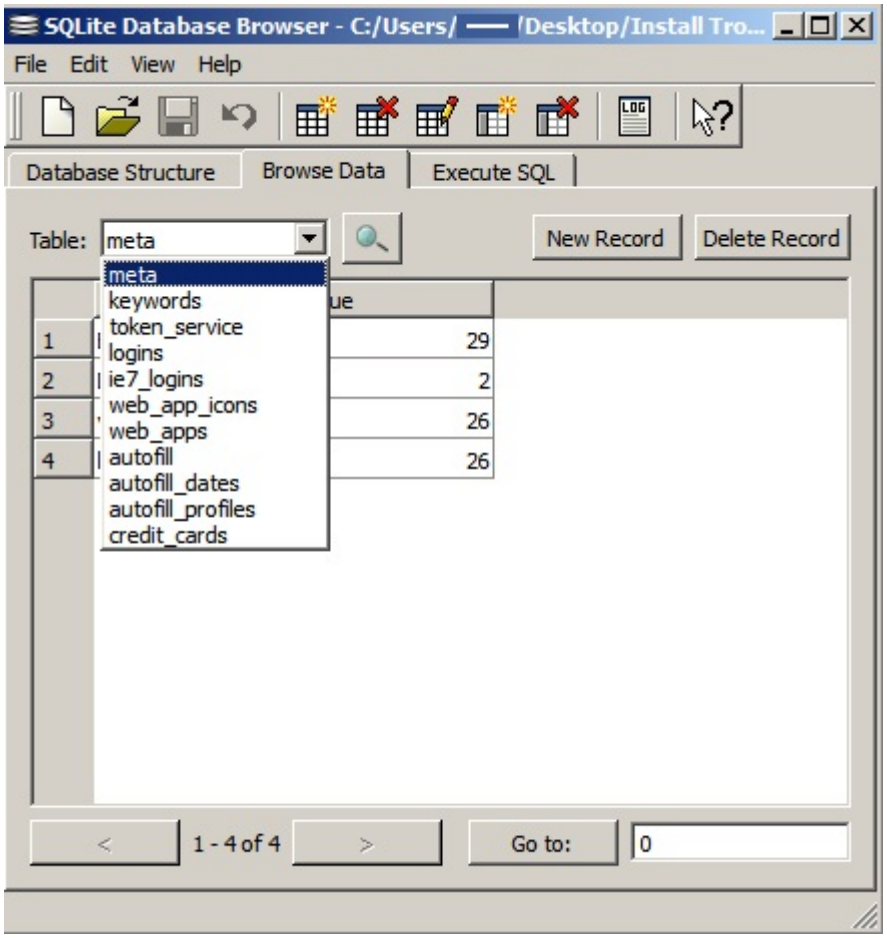
açtığımda tuş kayıtlarım ile karşılaştığıma hiç şaşırmadım.



Kurulum dosyası tarafından oluşturulan klasör içinde yer alan DoctoR.qsp dosyasını açtığımda ise kurulum dosyasının (setup.exe) özel olarak oluşturulduğunu ve kurulumda orjinal programa ilave olarak tuş kayıt bilgilerini çalmak üzere hazırlanmış olan update.exe ve updater.exe adındaki iki trojanıda çalıştırmak üzere hazırlanmış olduğunu gördüm.

Arg-000-13=setup.exe
Arg-000-16=update.exe
Arg-000-25=updater.exe

C:\Documents and Settings\Administrator\Application Data\chrtmp dosyasına SQLite Database Browser ile göz attığımda internet tarayıcısı tarafından kayıt altına alınan bilgileride çaldığını öğrenmiş oldum.



Son olarak Virustotal sonuçlarına baktığımda ise bunların zararlı yazılım oldukları konusunda artık hiç şüphem kalmamıştı. (update.exe , updater.exe , googleupdate.exe)

Sonuç olarak günümüzde korsan yazılımlarında art niyetli kişilerin hedefi haline geldiğini, ülke ekonomisini düşünmeyenlerin en azından kendi sistemlerinin, verilerinin güvenliği için lisanslı yazılımlar kullanmaları gerektiğinin altını bu vesileyle çizmek isterim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli haftalar dilerim.