

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.

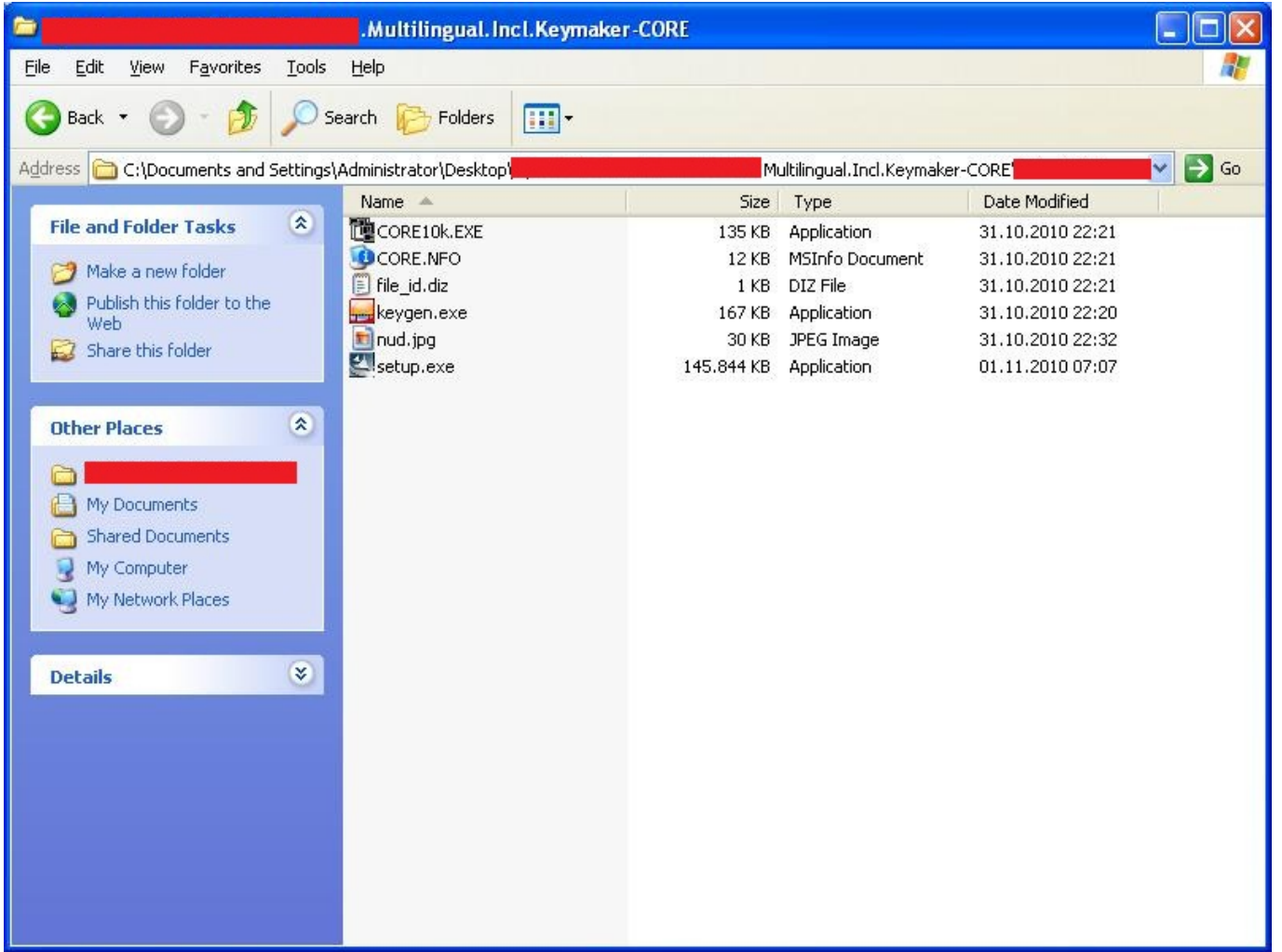
Her ne kadar günümüzde korsanla mücadelede büyük adımlar atılıyorsa da eski yıllara kıyasla bağlantı hızlarının yüksek olması, dosya paylaşım sitelerinin çokluğu ve torrent programlarının neredeyse işletim sistemleri ile kurulu geliyor olması nedeniyle paylaşım kolaylaşıyor, mücadele ise zorlaşıyor.

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

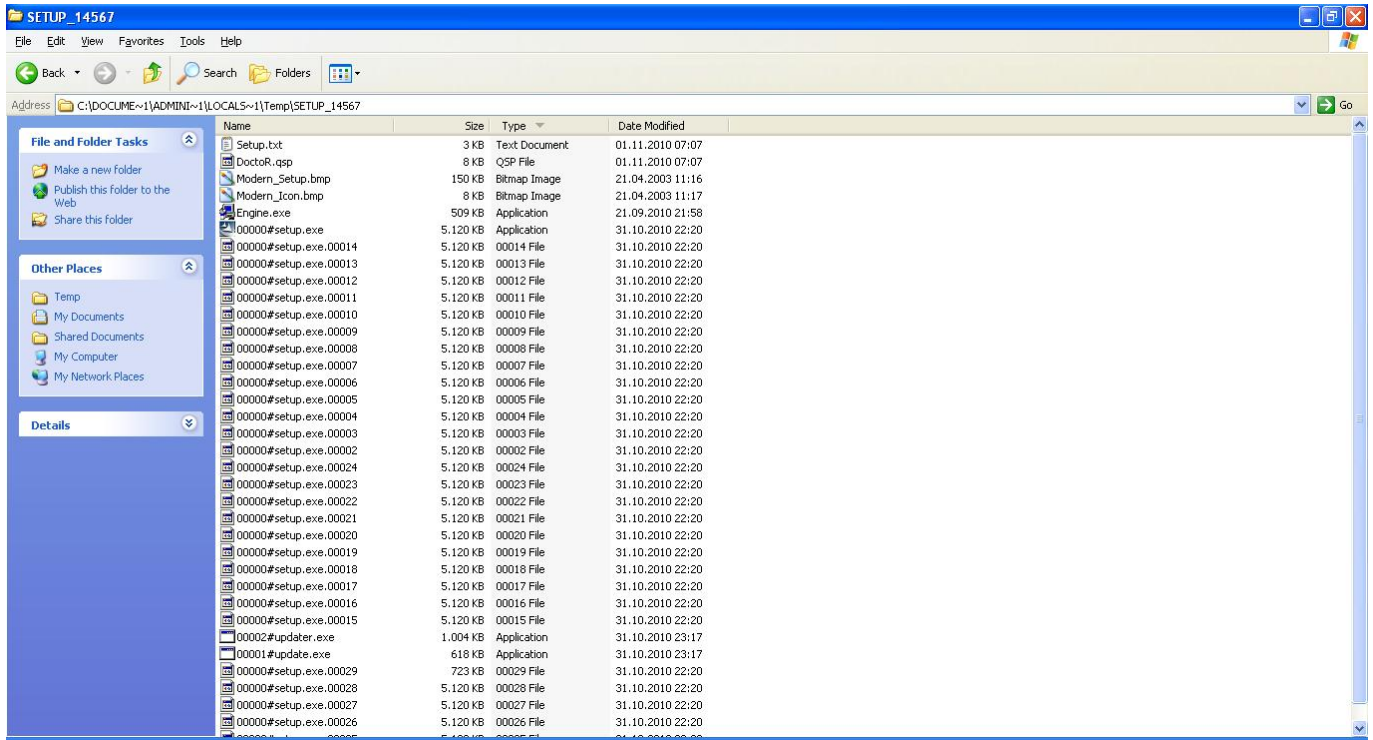
Art niyetli kişiler çoğunlukla zararlı yazılımlarını yaymak için o gün için popüler olan sistemleri (misal facebook üzerinden yayılan trojan), insanları kandırmak için popüler isimleri veya güncel olayları kullanmayı severler. Korsan yazılım kullanımının yüksek olduğu son yıllarda bu yazılımların art 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\FIashFXP\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\dcllogs.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.

VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark

Filter: ((ip.dst == 239.255.255.250) && ! (ipv6.src == fe80::29b9:7cd3:53f4:fa5)) Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
552	794.754533	192.168.2.128	192.168.2.2	DNS	Standard query A mazinga.zapto.org
553	794.856785	192.168.2.2	192.168.2.128	DNS	Standard query response A 127.0.0.1
555	800.770893	192.168.2.128	192.168.2.2	DNS	Standard query A zzan0u.servgame.com
556	800.879591	192.168.2.2	192.168.2.128	DNS	Standard query response A 69.65.19.116 A 69.65.19.117
557	800.880103	192.168.2.128	69.65.19.117	TCP	adapt-sna > icpv2 [SYN] Seq=0 win=64240 Len=0 MSS=1460
560	803.956051	192.168.2.128	69.65.19.117	TCP	adapt-sna > icpv2 [SYN] Seq=0 win=64240 Len=0 MSS=1460
561	803.956171	69.65.19.117	192.168.2.128	TCP	icpv2 > adapt-sna [ACK] Seq=1 Ack=1 win=64240 Len=0
563	809.971671	192.168.2.128	69.65.19.117	TCP	adapt-sna > icpv2 [SYN] Seq=0 win=64240 Len=0 MSS=1460
564	809.971790	69.65.19.117	192.168.2.128	TCP	[TCP dup ACK 561#1] icpv2 > adapt-sna [ACK] Seq=1 Ack=1 win=64240 Len=0
570	824.176437	192.168.2.128	192.168.2.2	DNS	Standard query A mazinga.zapto.org
571	824.285635	192.168.2.2	192.168.2.128	DNS	Standard query response A 127.0.0.1
572	827.660321	192.168.2.128	192.168.2.2	DNS	Standard query A zzan0u.servgame.com
573	827.771515	192.168.2.2	192.168.2.128	DNS	Standard query response A 69.65.19.117 A 69.65.19.116
574	827.799926	192.168.2.128	69.65.19.116	TCP	dcs > icpv2 [SYN] Seq=0 win=64240 Len=0 MSS=1460
576	830.815299	192.168.2.128	69.65.19.116	TCP	dcs > icpv2 [SYN] Seq=0 win=64240 Len=0 MSS=1460
577	830.815806	69.65.19.116	192.168.2.128	TCP	icpv2 > dcs [ACK] Seq=1 Ack=1 win=64240 Len=0
580	836.831023	192.168.2.128	69.65.19.116	TCP	dcs > icpv2 [SYN] Seq=0 win=64240 Len=0 MSS=1460
581	836.831354	69.65.19.116	192.168.2.128	TCP	[TCP dup ACK 577#1] icpv2 > dcs [ACK] Seq=1 Ack=1 win=64240 Len=0
584	843.287424	192.168.2.1	192.168.2.255	BROWSER	Domain/workgroup Announcement WORKGROUP, NT workstation, Domain Enum
588	852.436431	192.168.2.128	192.168.2.2	DNS	Standard query A mazinga.zapto.org
589	852.569882	vmware_f2:27:01	Broadcast	ARP	who has 192.168.2.128? Tell 192.168.2.2
590	852.569928	vmware_75:0d:93	vmware_f2:27:01	ARP	192.168.2.128 is at 00:0c:29:75:0d:93
591	852.570163	192.168.2.2	192.168.2.128	DNS	Standard query response A 127.0.0.1
593	857.206694	192.168.2.128	192.168.2.2	DNS	Standard query A zzan0u.servgame.com
594	857.315276	192.168.2.2	192.168.2.128	DNS	Standard query response A 69.65.19.117 A 69.65.19.116
595	857.315773	192.168.2.128	69.65.19.116	TCP	gv-us > icpv2 [SYN] Seq=0 win=64240 Len=0 MSS=1460
597	860.347039	192.168.2.128	69.65.19.116	TCP	qv-us > icpv2 [SYN] Seq=0 win=64240 Len=0 MSS=1460

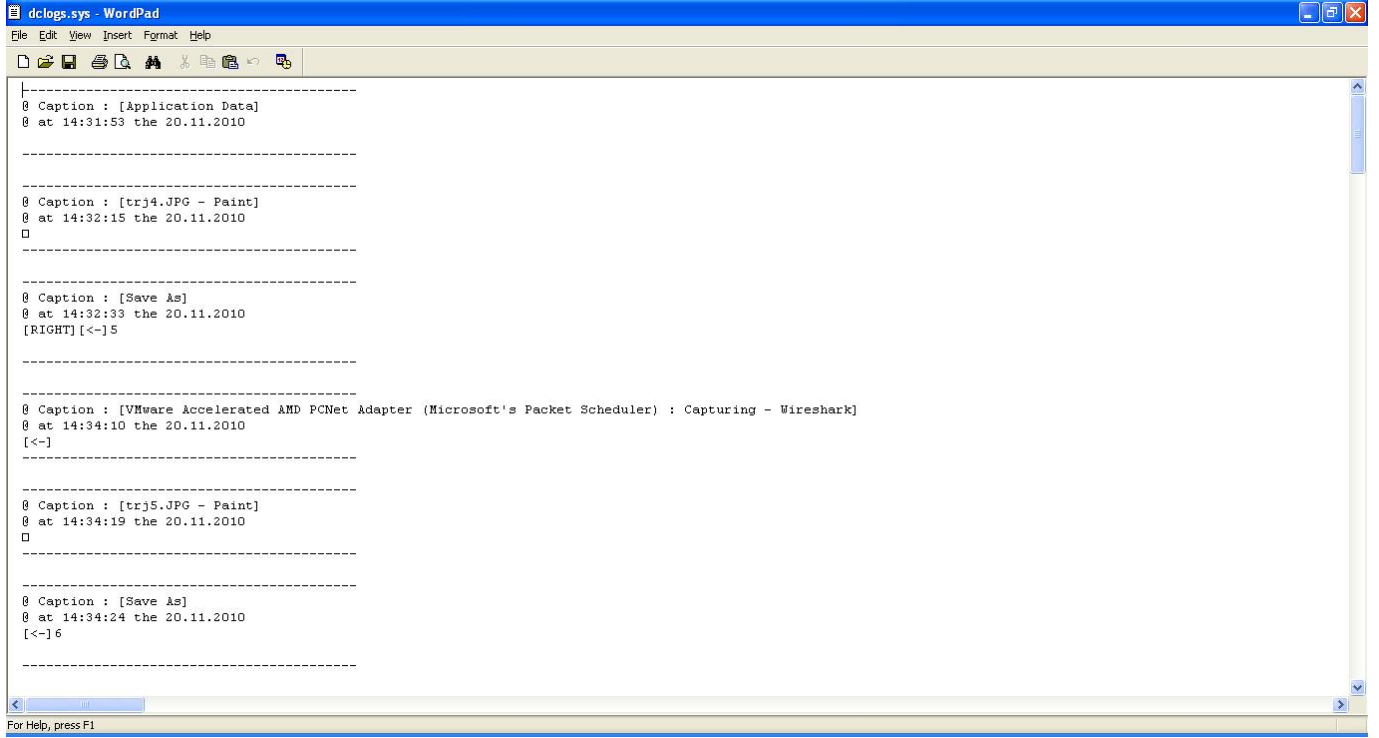
Frame 254 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: vmware_f2:27:01 (00:50:56:f2:27:01), Dst: vmware_75:0d:93 (00:0c:29:75:0d:93)
Internet Protocol, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.2.128 (192.168.2.128)
User Datagram Protocol, Src Port: domain (53), Dst Port: 33491 (33491)
Domain Name System (response)

0000 00 0c 29 75 0d 93 00 50 56 f2 27 01 08 00 45 00 ..)u...P V...E.
0010 00 70 72 f5 00 00 80 11 41 b5 c0 a8 02 02 c0 a8 .p....A.....
0020 02 80 00 35 82 d3 00 5c 4a e6 d5 8a 81 80 00 01 ...5...J.....
0030 00 01 00 00 00 03 31 31 37 02 31 39 02 36 351 17.19.65
0040 02 36 39 07 69 6e 2d 61 64 64 72 04 61 72 70 61 .69.in-a ddr.arpa

VMware Accelerated AMD PCNet Adapter (Micro... Packets: 602 Displayed: 219 Marked: 0 Profile: Default

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

açtığında tuş kayıtlarım ile karşılaştığıma hiç şaşırmadım.

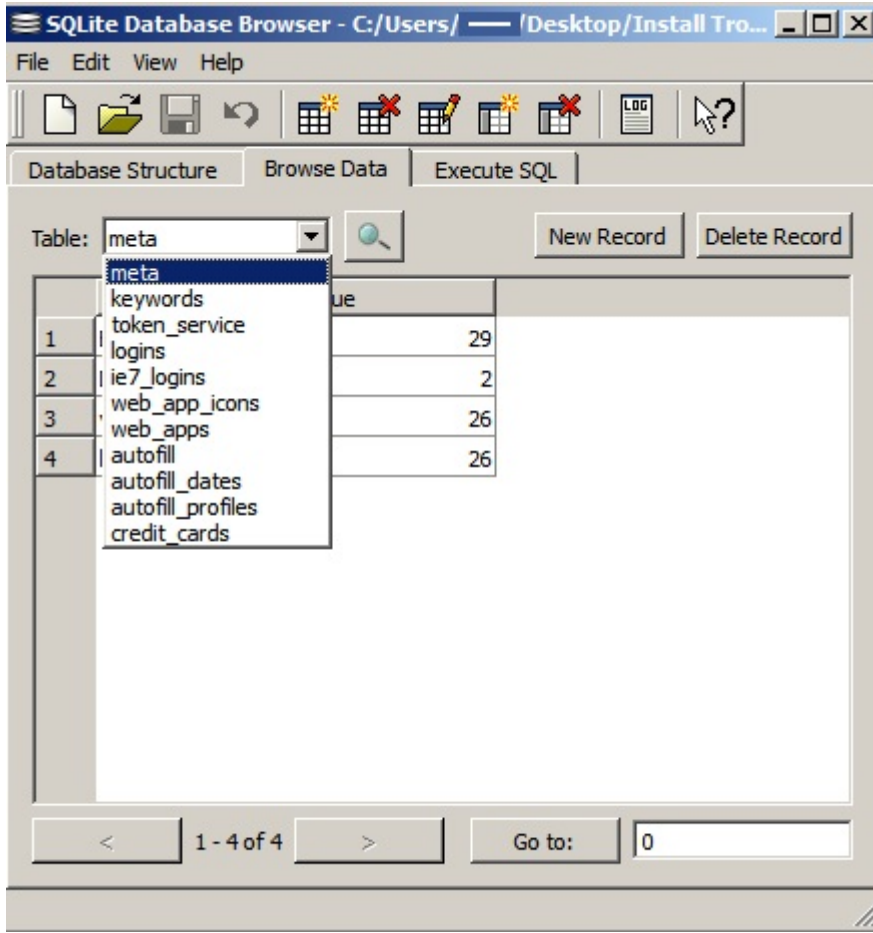


```
-----  
@ Caption : [Application Data]  
@ at 14:31:53 the 20.11.2010  
-----  
-----  
@ Caption : [trj4.JPG - Paint]  
@ at 14:32:15 the 20.11.2010  
@  
-----  
-----  
@ Caption : [Save As]  
@ at 14:32:33 the 20.11.2010  
[RIGHT] [<-]5  
-----  
-----  
@ Caption : [VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark]  
@ at 14:34:10 the 20.11.2010  
[<-]  
-----  
-----  
@ Caption : [trj5.JPG - Paint]  
@ at 14:34:19 the 20.11.2010  
@  
-----  
-----  
@ Caption : [Save As]  
@ at 14:34:24 the 20.11.2010  
[<-]6  
-----  
-----
```

Kurulum dosyası tarafından oluşturulan klasör içinde yer alan DoctoR.qsp dosyasını açtığında 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.