# Hacking The Hacker

written by Mert SARICA | 1 April 2010

Bir önceki yazımda geçtiğimiz Cumartesi günü Adli Bilişim (Euroforensics) konferansına katıldığımı ve çoğu sunumda memory forensic'in öneminden bahsedildiğini belirtmiştim. Günümüzdeki çoğu keylogger, trojan yazarları ve bu zararlı programları kullanmak isteyen çoğu insan bu programların imza tabanlı antivirüs programlarıı tarafından tespit edilmelerini önleme adına araştırmalar yapıyor (örneğin Google arama motoruna "trojanı t" yazdığınız taktirde "trojanı tanınmaz yapma" cümlesi otomatik olarak tamamlanıyor ki bu bize bu anahtar cümlenin ne kadar çok arandığını gösteriyor) çeşitli yollara başvuruyorlar ve bunların başında packer ile sıkıştırma ve şifreleme geliyor. Paketlenmiş veya şifrelenmiş zararlı program çalıştırılır çalıştırılmaz memory'de kendini açarak orjinal haline bürünüyor. Şifrelenmiş veya paketlenmiş zararlı bir programı incelemek için çok fazla seçeneğiniz yok, ya unpacker yazacaksınız ve bu sayede statik olarak analiz edebileceksiniz ya da programı çalıştıracak ve assembly debugger ile dinamik olarak inceleyeceksiniz.

Yine bir can sıkıntısı ile geçtiğimiz günlerde Türk hacking sitelerine göz atmaya karar verdim. Hemen hemen her sitenin kendisine ait bir forumu var ve her forumda da istisnasız Virus/Trojan/Worm bölümü var. Bu bölüm hem ziyaretçi sayısı açısından ve hem de mesaj sayısı açısından başı çekiyor. Konu başlıklarına hızlıca göz atarsanız hemen hemen her gün yeni bir trojan, keylogger programının paylaşıldığını, bir çok insanın trojanları tanınmaz hale nasıl getirebildiğini öğrenmek için mesaj yazdığını görebilirsiniz.

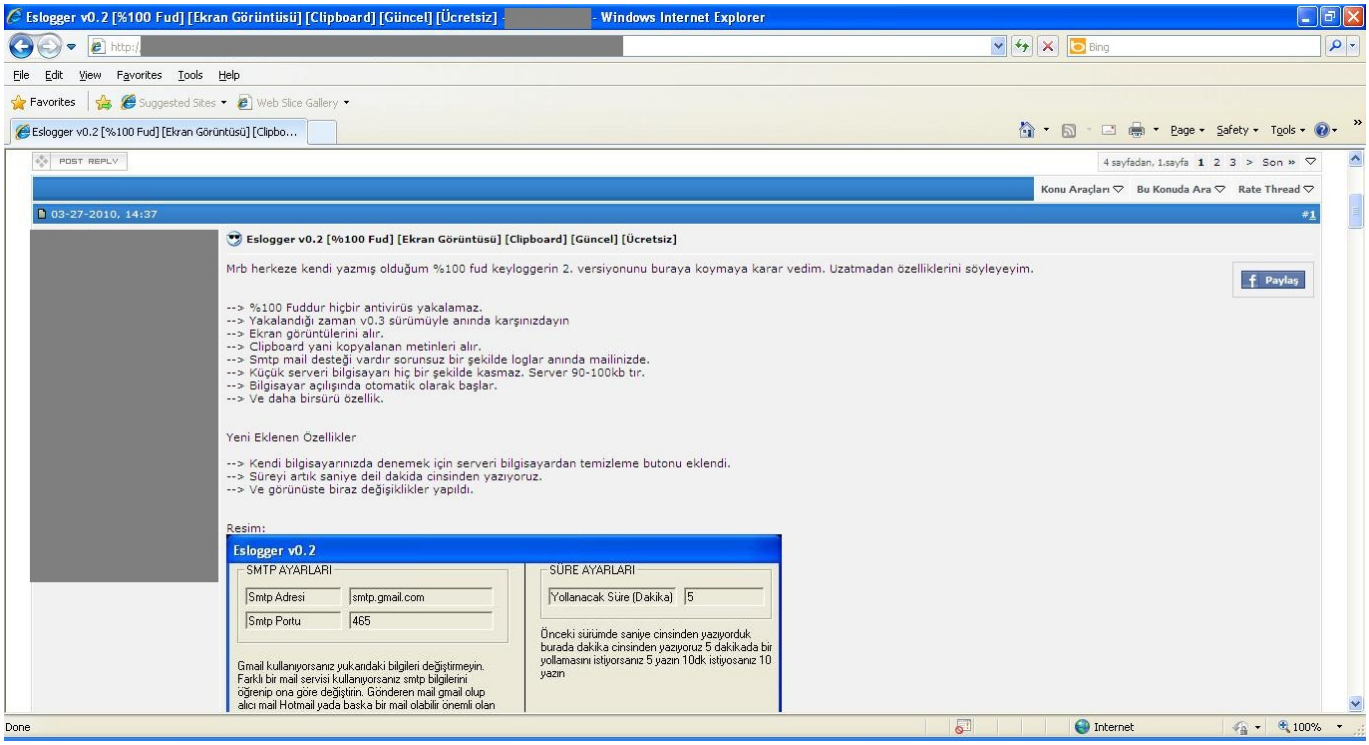
Sitelerden birini gezerken ilk konu başlığına göz atmaya karar verdim, Keylogger ve Stealer Paketi. Forumun moderatörü mesajında 30'dan fazla keylogger programını ziyaretçilerin paylaşımına sunmuş. İnsan ister istemez bu kadar çok zararlı programı ve bu programlara olan yoğun ilgiyi görünce ister istemez biraz üzülüyor malum bu programlar nedeniyle bir çok insan madur oluyor.

Bu programları indirenlerin bu programları eğitim amacıyla kullanmayacakları göz önünde bulundurulduğunda antivirüs programlarına ve bizlere çok iş düşüyor bu sebeple ufakta olsa birşeyler yapsam diye işe koyuldum ve programların genel özelliklerine bakmaya karar verdim. Örnek ekran görüntülerine baktığımda en çok dikkatimi çekenin hemen hemen her keylogger

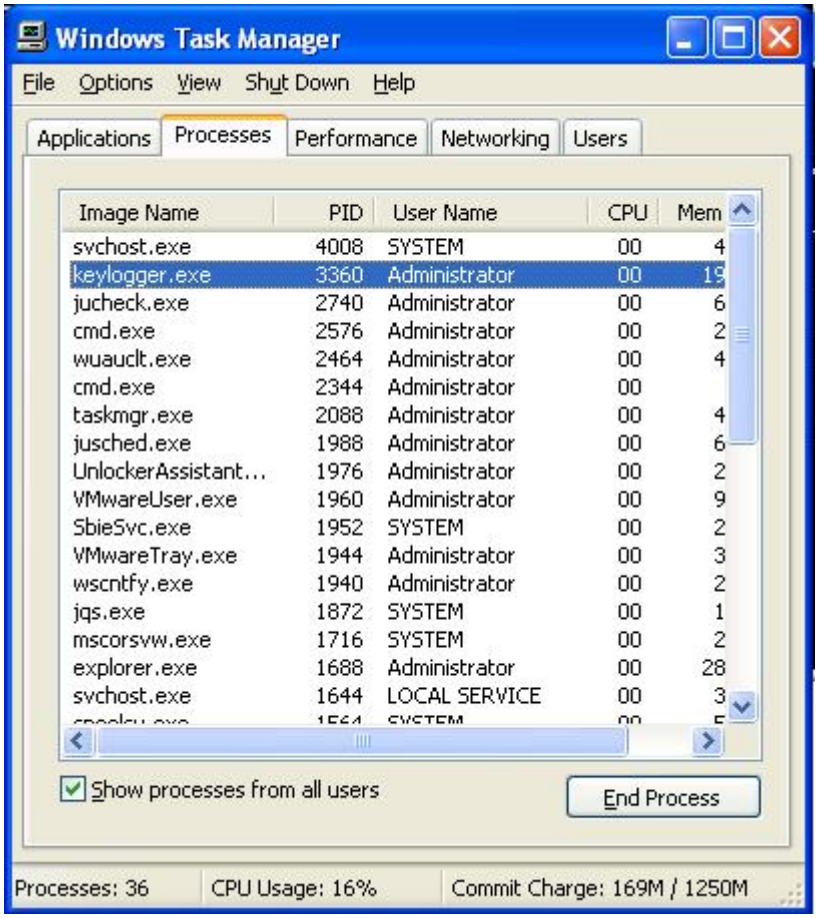
programının çalışabilmesi için bir SMTP sunucusuna ve bu sunucuyu kullanabilecek kullanıcı adı ve şifreye ihtiyaç duyduğunu gördüm ve o anda şimşekler çakıverdi.

Kendi kendime acaba ufak bir program yazsam ve bu program memory'den dump edilmiş keylogger process'ine ait olan dump dosyasındaki stringlerden, keylogger programına gömülmüş olan SMTP sunucusunu ve bu sunucuya ait olan kullanıcı adını ve şifreyi ortaya çıkarsa bu sayede madur olan kişi isterse kendisini hacklemede kullanılan e-posta hesabına ulaşabilir, şifresini değiştirebilir veya adli mercilere iletebilir dedim.

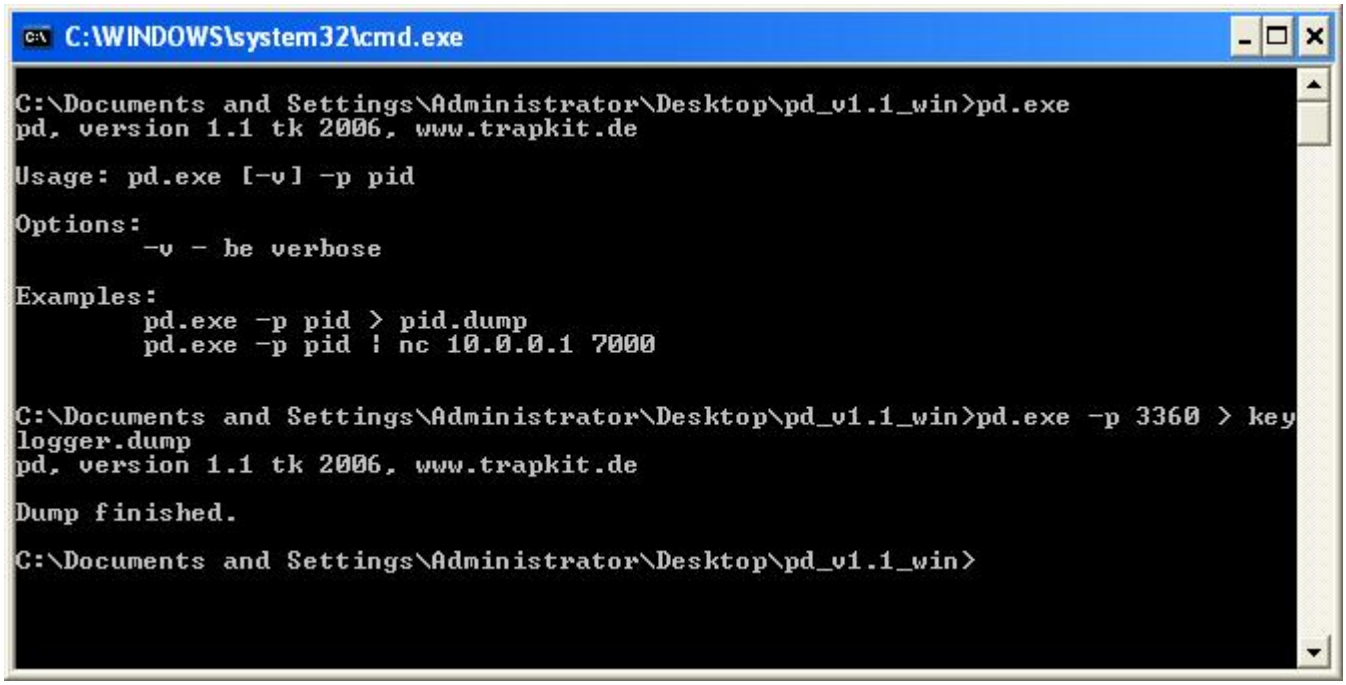
Öncelikle test için forumda paylaşılan Eslogger adındaki keylogger programını indirip kurdum.




Eslogger programını çalıştırdığınızda kurbana göndereceğiniz dosyayı 1 tuş ile hazırlamanıza imkan tanıyor ve default olarak adını svchost.exe olarak diske kaydediyor. Test amacıyla hack4career@gmail.com e-posta hesabını aldım ve deneme1234 olan şifresini Eslogger programına kayıt ettim ve kurbana gönderilecek olan programı oluşturdum. Program çalıştığında işletim sistemi tarafından oluşturulan diğer svchost.exe processleri ile karışmaması için programın adını keylogger.exe olarak değiştirdim ve programı çalıştırdım.

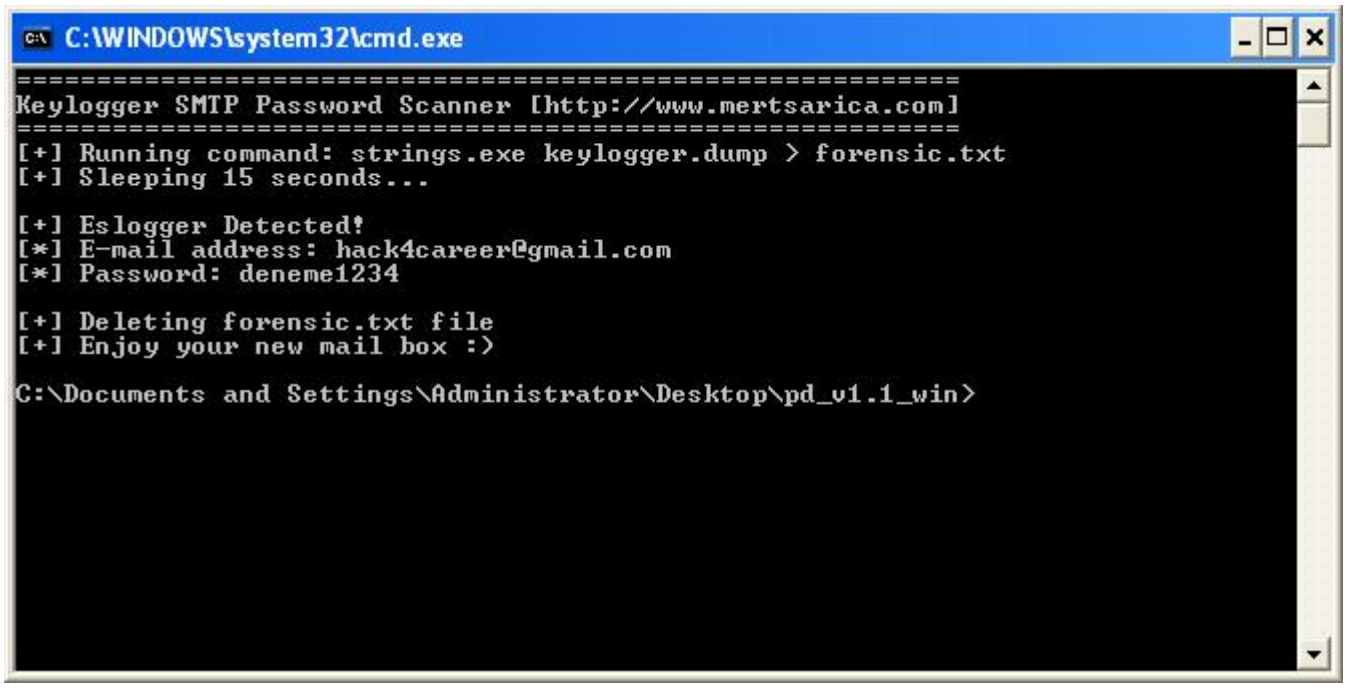



Ardından PD programı ile memory'den keylogger.exe process'ini diske keylogger.dump adı ile kayıt ettim. (PD programı, memory forensic analizlerinde kullanılan ve çalışan processi diske kayıt etmenize imkan tanıyan oldukça faydalı bir program.)




Gelelim yazmış olduğum programa, ksps (Keylogger SMTP Password Scanner). Öncelikle bu program şuan için sadece iki keylogger programını (Eslogger ve

Perfect Keylogger) destekliyor. KSPS programını şüphelendiğiniz process'e ait olan dump üzerinde çalıştırdığınızda eğer bu dump Eslogger ve Perfect Keylogger programlarından birine ait ise size içerisinde yer alan SMTP sunucu adını, kullanıcı adını ve şifreyi gösteriyor.




KSPS programının kaynak koduna bakacak olursanız ufak bir geliştirme ile başka keylogger programlarınıda tespit etmesini sağlatabilirsiniz. KSPS programına buradan ulaşabilirsiniz.

That's all folks :)