Şifrelenmiş Zararlı Yazılımlar

written by Mert SARICA | 15 May 2010

Son 2 yazıdır Kanald vakası ile ilişkili yazılar yazıyorum bana kalırsa bu vakadan çıkartılacak çok fazla ders ve geleceğe dair ipuçları var. Takip edenler bilirler daha önceki bir yazımda, yerli ve yabancı hacking sitelerinde, art niyetli yazılımları antivirüs yazılımlarından kaçırmak için hummalı bir çalışma olduğuna dikkat çekmiştim. Kanald vakasındaki tuş kayıt yazılımını, uzaktaki web sitesinden indirmek için kullanılan kodun şifrelenmiş olması ileride bu ve benzer şifrelenmiş zararlı yazılım içeren vakalar ile karşılaşacağımıza dair önemli bir işaretti.

Bu yazımda bu kişilerin bunu nasıl başardıklarından kısaca söz edeceğim fakat öncesinde sizlere yer altı dünyasında kullanılan 4 terimden bahsetmem gerekiyor; packer, crypter, binder ve stub.

Packerlar yani paketleyiciler genel olarak programların içeriğini sıkıştırmak ve bu sayede program içeriğinin hex editör ve benzer programlar ile okunmasını engellemek için kullanılırlar. Çoğunlukla bu programları çalıştırdığınızda, programın akışı normalin aksine öncelikle bu sıkıştırmayı açan ve çoğunlukla programların sonunda yer alan (stub) algoritmaya yönlenir ve sıkıştırılmış içerik açılarak çalışmaya başlar. Paketleyicilere örnek olarak oldukça meşhur olan UPX paketleme programını örnek verebilirim.

Crypterlar yani şifreleyiciler paketleyicilerin aksine içeriği sıkıştırmak yerine şifrelerler ve programın akışı paketleyicilerde olduğu gibi ilerler ve sonunda şifrelenmiş zararlı yazılım çalışma esnasında program içerisinee gömülü olan şifre ile şifresini çözer ve çalışır. Cryptlerlara örnek olarak meşhur olanlardan ASProtect programını örnek verebilirim.

Binderlar yani birleştiriciler ise iki farklı programı alıp tek bir programa dönüştürmek için kullanılırlar bu sayede tek bir program çalıştırdığınızı sanırsınız fakat arkada aslında iki tane farklı program çalışmış olur ve bunlardan biri art niyetli kişinin trojanı olabilir. Binderlara örnek olarak Microsoft'un iexpress uygulamasını (Start -> run -> iexpress) örnek verebilirim.

Stub'ı ise paketlenmiş bir programda, paketin açılmasından sorumlu algoritma

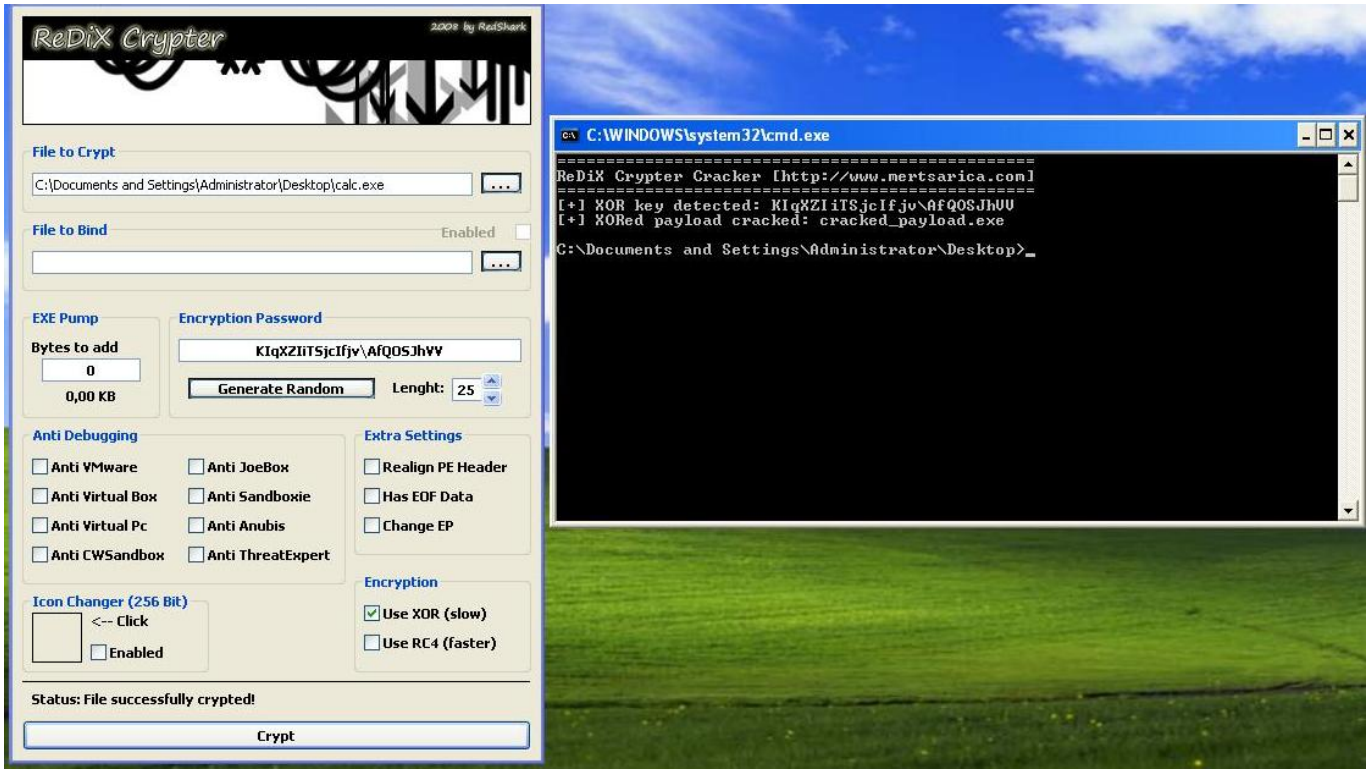
olarak, şifrelenmiş bir programda ise şifrenin çözülmesinden sorumlu algoritma olarak düşünebilirsiniz.

Stub hazırlama programlarına bakıldığında şifreleme algoritması olarak Blowfish, Twofish, Aes, RC4, XOR ve daha bir çok algoritma destekleyebiliyorlar fakat temel düzeyde bakıldığında en çok karşılaşılan algoritmalar RC4 ve XOR oluyor. Malum şifreleme için simetrik algoritma kullanıldığı içinde binary üzerinde yer alan şifreye ulaşmak ve statik olarak bunu tespit etmek mümkün.

Bir malware analist için ilk yapılacak iş trojan paketlenmiş ise paketten çıkartmak, şifrelenmiş ise şifresini çözmektir. Piyasada kullanılan bir çok paketleyici program için paket çözücü programlar hazırlandığı için zararlı yazılımı paketten çıkartmak aslında artık büyük bir sorun değil fakat şifrelenmiş olanlar için bunu söylemek biraz güç çünkü kullanılan şifreleme anahtarını ve algoritmayı tespit edecek programı otomatize etmek crypterın tasarımı nedeniyle güç olabiliyor. Peki basit olanları yok mu ? Otomatize etmek mümkün mü ? sorularının yanıtını bende merak ettiğim için geçtiğimiz günlerde bir forumdaki crypterlara göz atmaya karar verdim ve rastgele bir crypter programını indirip incelemeye karar verdim.

Redix Crypter adındaki şifreleme aracına göz attığımda desteklenen şifreleme algoritmaları RC4 ve XOR'dan oluşuyordu. Şifreleme anahtarını program üzerinde nerede tuttuğuna hex editör ile baktığımda ise şifrenin programın son satırlarında yer aldığını gördüm. Ayrıca şifreleme programı tüm parametreleri (payload, aktif anti vm özellikleri, şifreleme anahtarı) _<>_ ayracı kullanarak tutuyordu. Bu üç ipucu bize şifrelenmiş bir programı çözecek otomatik bir araç tasarlamanın mümkün olabileceğini işaret ediyordu.

Python, python, python diyerek hemen bir program hazırlamaya başladım ve ortaya Redix şifreleme aracı ile şifrelenmiş bir programın şifresini (sadece XOR için) çözen ufak bir program ortaya çıkıverdi. XOR'u çözen programı ben hazırladım, RC4'u çözenide siz hazırlayın diyerek bu haftanın yazısına burada son veriyorum. Bir sonraki yazıda görüşmek dileğiyle…



Redix Crypter Cracker programına buradan ulaşabilirsiniz.