# Dikkat Malware!!!

written by Mert SARICA | 10 December 2009

Bugün öğlen saatlerinde bir arkadaşım, kendisine gelen şüpheli bir e-postayı benimle paylaştı. E-posta, popüler bir kariyer sitesindeki iş ilanına yanıt şeklinde hazırlanmıştı ve bu e-postada adı geçen adaya ait C.V detaylarının bir web sitesinden indirilebileceği belirtilmişti. İlk izlenimim bu kariyer sitesindeki iş verenlerin hedef alındığı yönündeydi. Malum mesai saatleri içerisinde bu sitede yer alan şüpheli dosyayı detaylı inceleme fırsatım olmadığı için evde inceleyebilmek için diskime kayıt edip işimin başına döndüm.

Akşam saatlerinde dosyayı incelemeye başladığımda ve dosyanın içerisinde Türkçe stringlerin yer alması, yerli yapımı olduğu ihtimalini güçlendirdi. Dosyayı debugger ile incelemeye devam ettiğimde zararlı koda ait payload'un blowfish ile encrypt edildiğini bu nedenle antivirüsler tarafından tespit edilmesinin pek mümkün olmadığını (3/41 başarı ve 7/41) gördüm.

Trojan çalıştırıldıktan hemen sonra kendisini silerek windows/system32/wins/setup klasörü altına msmgrs.exe adı altında kopyalıyordu. Trojanın yarattığı trafiği yakından incelediğimde ise yurt dışındaki bir ftp adresine bağlandığını gördüm.

ISC2 code of ethics'in altına imza atmış bir güvenlik uzmanı olarak bu konu karşısında duyarsız kalmam mümkün değildi o nedenle keşfettiğim ve analiz ettiğim malware ile ilgili olarak insanları ve kurumları bilgilendirdim. Ön analizler neticesinde trojanın keylogger özelliğine sahip olduğunu, ek olarak 10'dan fazla Türk bankasının internet bankacılığı sayfasına girişi esnasında kullanıcının ekran görüntülerini kayıt ettiğini gördüm. İlerleyen zamanlarda malware analizi ile ilgili bir makale yayınlayarak nasıl tespit ettiğimi ve analiz ettiğimi sizlerle paylaşmayı düşünüyorum.

Code of Ethics Canons:
Protect society, the commonwealth, and the infrastructure.
Act honorably, honestly, justly, responsibly, and legally.
Provide diligent and competent service to principals.
Advance and protect the profession.