Pwndromeda

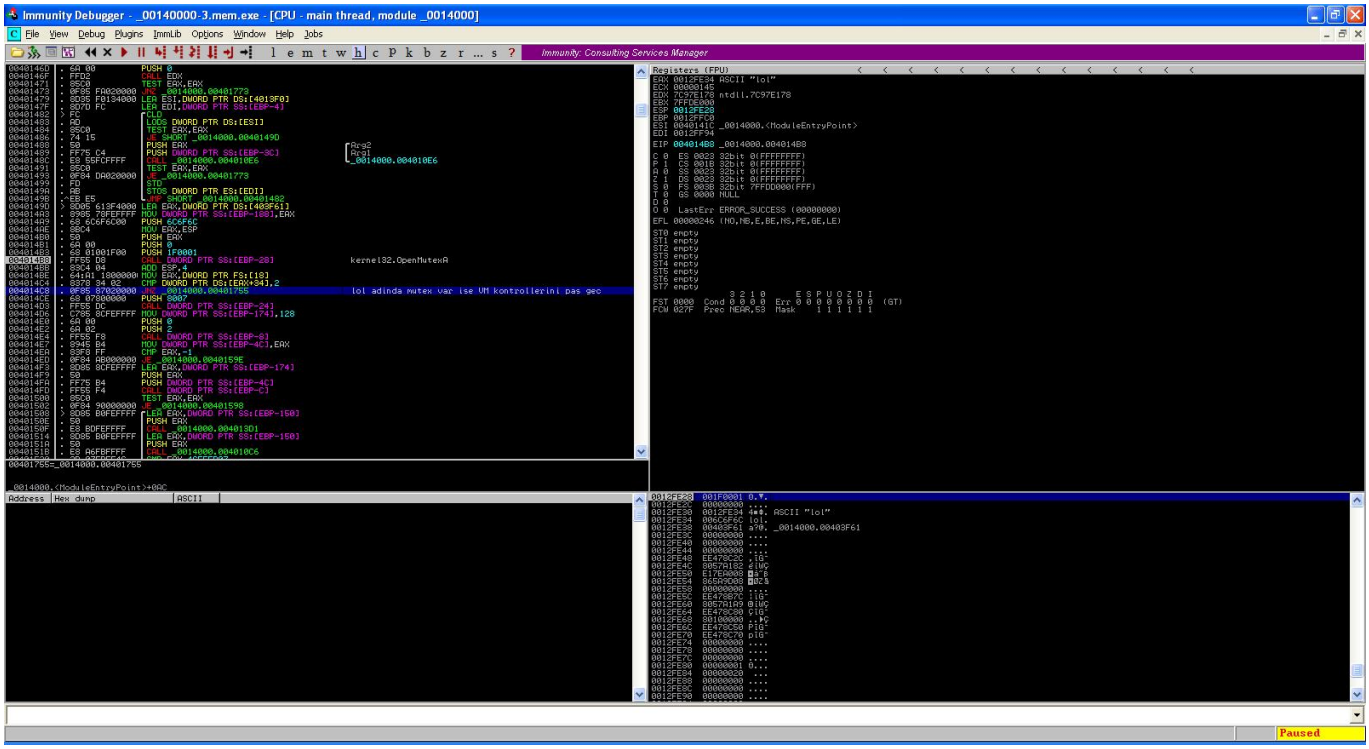
written by Mert SARICA | 2 February 2013

Son yazımdan yani 1 Ocak 2013 tarihinden bu yana geçen zaman zarfında Zemana'dan Emre TINAZTEPE'nin yayınlamış olduğu analiz raporunda sahte e-postalar ile gönderilen bankacılık zararlı yazılımının Andromeda (Symantec'e göre Downloader.Dromedan) zararlı yazılımı olduğunu ve dropper (başka bir zararlı yazılım indiren ve çalıştıran zararlı yazılım) olarak çalışarak Cridex ve/veya Zeus bankacılık zararlı yazılımlarını indirdiğini görmüş olduk. Bir önceki yazımda da Andromeda zararlı yazılımının sanal makinede çalıştırılması durumunda farklı davranışlar sergilediğini ve sadece sistemsel analizler yapılarak hatalı sonuçlara varılabileceğini görmüş olduk.

1 Ocak tarihinden bu yana sahte Turkcell, Kuveyt Türk, Türk Telekom, Garanti Bankası e-postaları ile sayısız defa tekrar ve tekrar gönderilen Andromeda zararlı yazılımı, her defasında olmasa da her iki gönderimde bir, yeni bir komuta kontrol merkez adresi ile gönderiliyordu. Durum böyle olunca da analiz için yazılım seviyesine inemeyen ancak zararlı yazılıma karşı da kurumlarını ve çalışanlarını korumak için komuta kontrol merkezi adreslerini tespit etmek ve güvenlik cihazları üzerinde kara listeye eklemek isteyen çok sayıda sistem/güvenlik yöneticisi olduğunu farkettim ve kendilerine yardımcı olabilmek adına işe koyuldum.

Normalde bu zararlı yazılım sanal makinede çalıştığını kontrol etmiyor ve farklı davranışlar sergilemiyor olsaydı bu zararlı yazılımı sanal makineye kopyalayıp, çalıştırarak ve Wireshark gibi bir trafik izleme aracı ile izleyerek haberleştiği komuta merkezlerini rahatlıkla tespit edebilirdiniz ancak aksi bir durum söz konusu olduğu için her defasında bu zararlı yazılımı, yazılım seviyesine inip analiz etmekten veya zararlı yazılım tarafından tespit edilemeyen özel olarak konfigüre edilmiş bir sanal makinede çalıştırmaktan başka bir çareniz kalmıyordu. Özel olarak konfigüre edilmiş bir sanal makine, tespit edilmemek için ana sistem ile arasındaki kullanımı kolaylaştıran dosya paylaşımı gibi özelliklerden arındırıldığı için sanal makineyi tam randımanlı kullanmak pek mümkün olmuyor. Bu durumda eliniz kolunuz bağlı beklemekten veya zorluklarla mücadele ederek ilerlemekten başka çareniz kalmıyor. Peki gerçekten de öyle mi ? Aslında analiz etmek istediğiniz zararlı yazılım Andromeda olduğu sürece az önce bahsettiğim zorluklarla mücadele etmek zorunda değilsiniz.

Andromeda zararlı yazılımını yazılım seviyesinde analiz ettiğimde dikkatimi çeken lol adında bir mutex nesne kontrolü oldu.



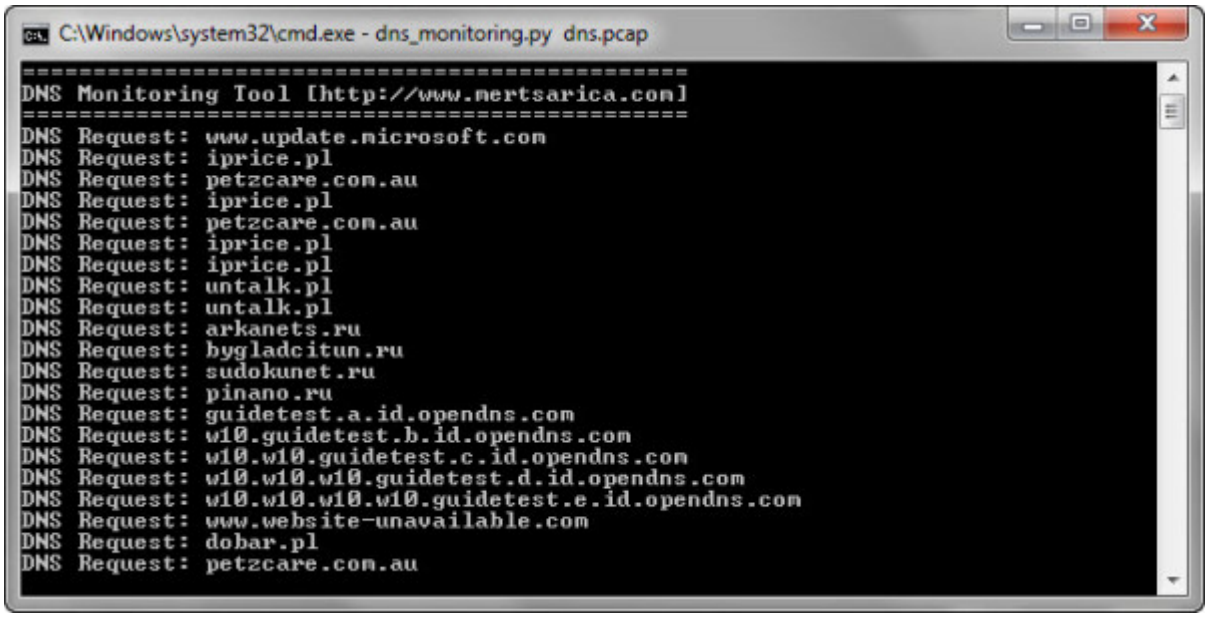
Mutex nesnesini kabaca ve kısaca, bir yazılımın, kopyasının, sistemde çalışmasını engellemek amacıyla kullanılan bir nesne olarak düşünebilirsiniz. Örneğin X yazılımı sistemde çalıştığında Hack4Career mutex nesnesi yaratabilir ve ardından sistemde ikinci defa çalıştırıldığında hali hazırda sistemde çalışıp çalışmadığını kontrol etmek için Hack4Career mutex nesnesini kontrol ederek bu sonuca göre sistemde tekrar çalışıp çalışmayacağına karar verebilir.

Bu kontrol sayesinde eğer lol adındaki bu mutex nesnesi sistemde yaratılmış ise Andromeda zararlı yazılımı, tüm VM kontrollerini atlayarak, pas geçerek sanal makine içinde çalışmaktaydı. Kısacası Andromeda zararlı yazılımının geliştiricisi muhtemelen sanal makinede zararlı yazılımı test edilebilmek için zararlı yazılımına bir nevi arka kapı koymuştu. Bu sayede biz de bu arka kapıdan faydalanarak Andromeda zararlı yazılımının sanal makinede çalışmasını sağlayabilir ve rahatlıkla trafiğini analiz edebilirdik.

Bunun için Python ile Andromeda Anti VM adında işletim sisteminde lol adında bir mutex nesnesi oluşturan ufak bir program hazırladım. Bu sayede Andromeda zararlı yazılımını analiz etmek için yapmanız gereken tek şey Andromeda zararlı yazılımı ile birlikte Andromeda Anti VM programını sanal makineye kopyalamak, önce Andromeda Anti VM programını daha sonra ise Andromeda

zararlı yazılımını çalıştırmak ve sanal makinenin ürettiği trafiği izleyerek kara listeye ekleyeceğiniz adresleri rahatlıkla tespit etmektedir.

Hatta benim gibi işi gereği komuta kontrol merkezlerini anlık olarak takip etmek isteyenler aşağıdaki resimde ve videoda yer aldığı gibi Andromeda Anti VM programını izleme mekanizmalarının kilit bir parçası olarak da kullanabilirler.



Analizinizi kolaylaştıracak Andromeda Anti VM programını buradan indirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Aşağıdaki video, 30 Ocak tarihinde gönderilen sahte Garanti Bankası e-postası ile gönderilen Andromeda zararlı yazılımı üzerinde yapılan çalışmayı içermektedir. (Andromeda zararlı yazılımlarının temin edilmesinde göstermiş olduğu yardımseverlik nedeniyle Kemal Karakaya'ya teşekkürü bir borç bilirim.)