

Pi Hediye Vardı, Verdim, Gitti #4 :)

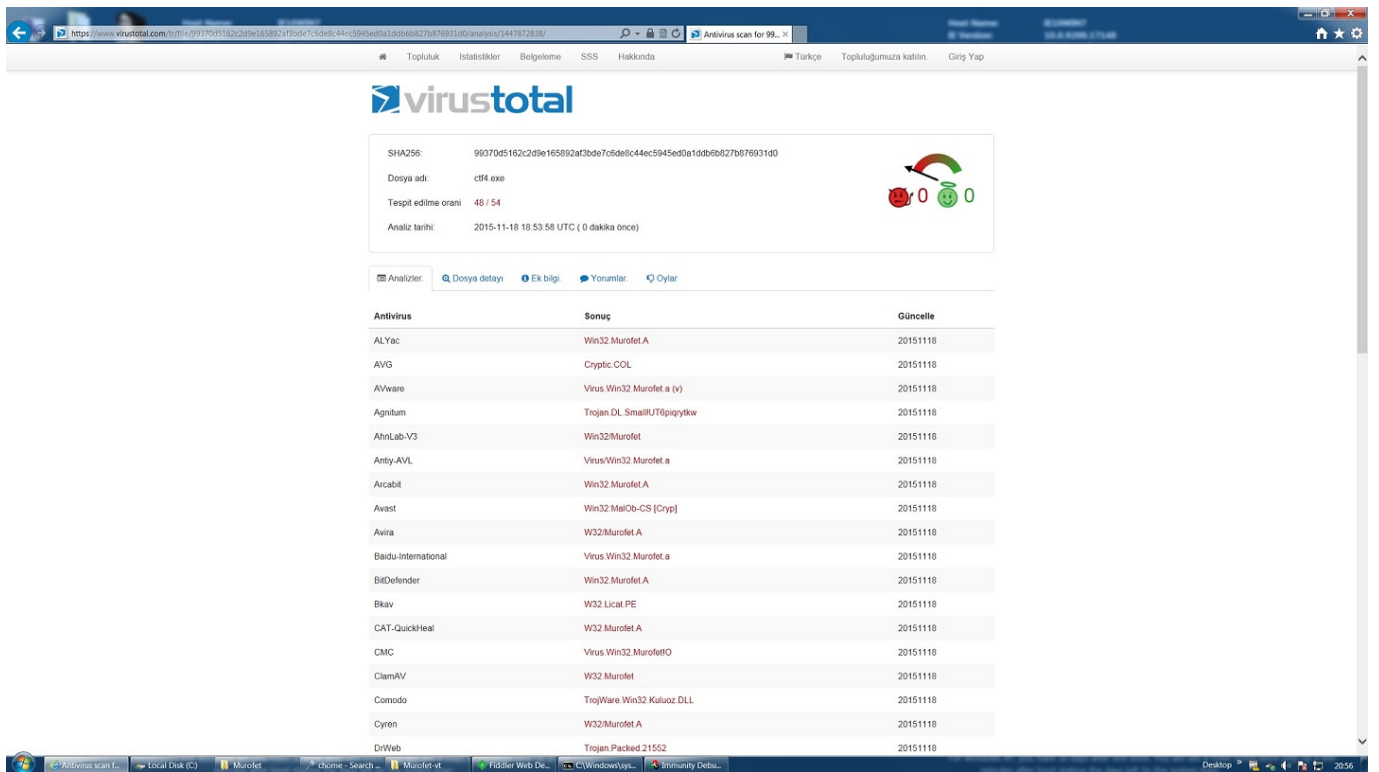
written by Mert SARICA | 30 November 2015

18 Kasım 2015 tarihinde dördüncüsü düzenlenen Pi Hediye Var oyununun çözüm yolu ve Raspberry Pi kazanan talihli karşınızda!

ÇÖZÜM YOLU:

Yapacağınız ilk iş, her zararlı yazılım analizinde olduğu gibi ctf4.exe isimli bu zararlı yazılımı VirusTotal web sitesine yüklemek ve zararlı yazılım ile ilgili olarak olabildiğince bilgi toplamaya çalışmaktır.

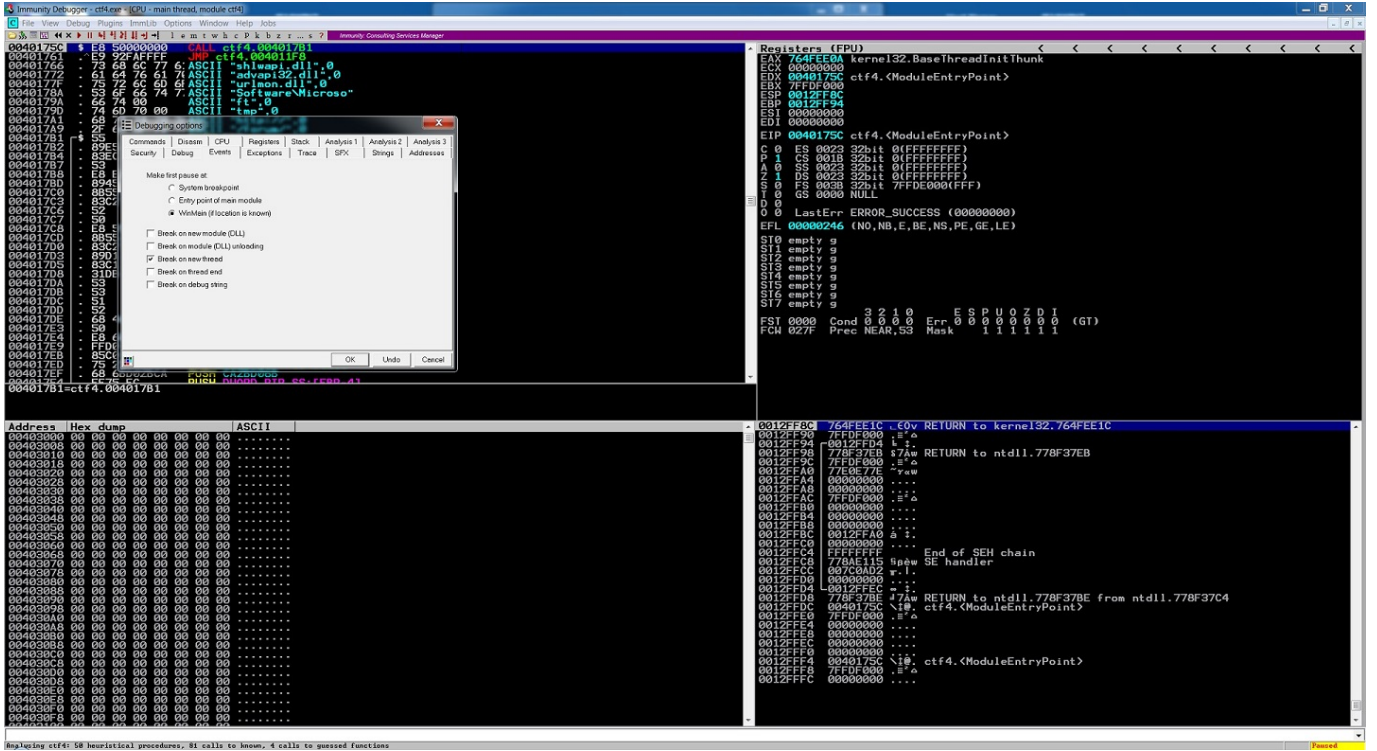
VirusTotal'a dosyayı yüklediğinizde karşınıza çıkan Antivirüs çıktılarından bunun Murofet isimli bir zararlı yazılım olduğunu anlayabilirdiniz.



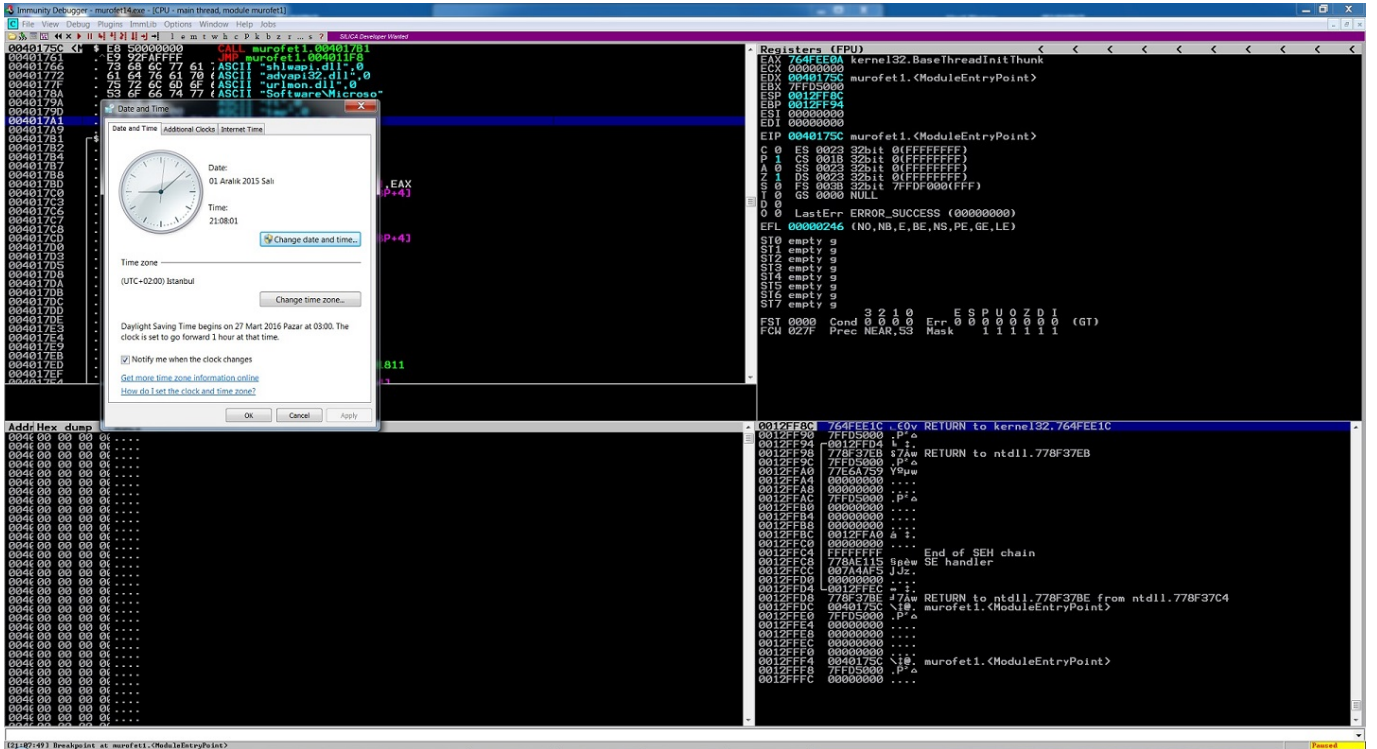
SHA256: 96370d5162c2d9e165892af3bde7c5de8c44ec5945ed0e1ddb8b27b679931d0
Dosya adı: ctf4.exe
Tespit edilme oranı: 48 / 54
Analiz tarihi: 2015-11-18 19:53:58 UTC (0 dakika önce)

Antivirüs	Sonuç	Güncelle
ALYac	Win32/Murofet.A	20151118
AVG	Cryptic.COL	20151118
AVware	Virus Win32/Murofet.a (v)	20151118
Agnitum	Trojan.DL.SmallUT6pqytkw	20151118
AhnLab-V3	Win32/Murofet	20151118
Antiy-AVL	Virus/Win32/Murofet.a	20151118
Arcabit	Win32/Murofet.A	20151118
Avast	Win32/MalOb-CS [Cryp]	20151118
Avira	W32/Murofet.A	20151118
Baidu-International	Virus Win32/Murofet.a	20151118
BitDefender	Win32/Murofet.A	20151118
Bkav	W32/Lcal.PE	20151118
CAT-QuickHeal	W32/Murofet.A	20151118
CMC	Virus Win32/Murofet.O	20151118
ClimAV	W32/Murofet	20151118
Comodo	Trojan/W32/Kuluoz.DLL	20151118
Cyren	W32/Murofet.A	20151118
DrWeb	Trojan.Packed.21552	20151118

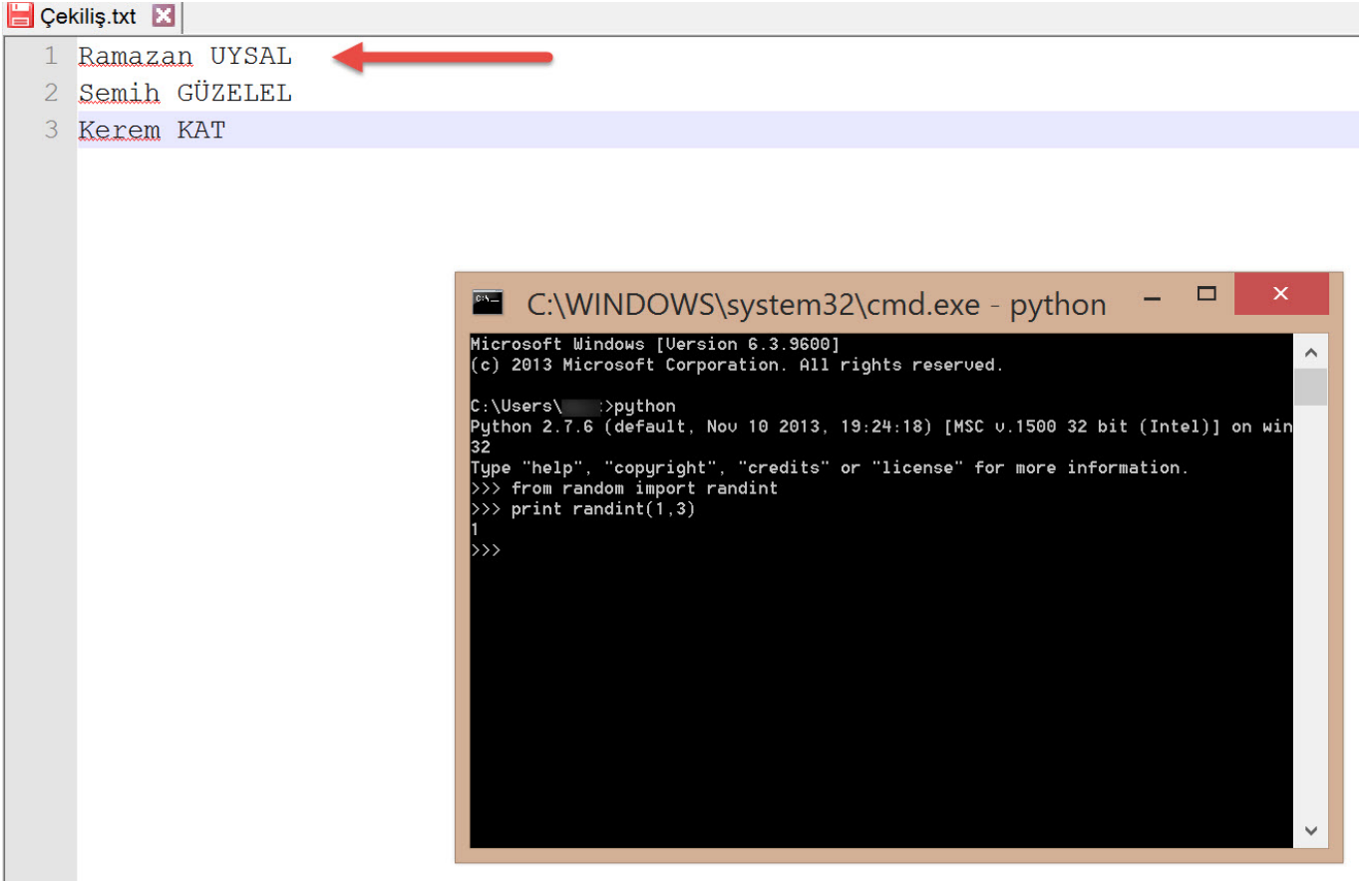
Ardından ctf4.exe zararlı yazılımını Windows XP işletim sistemi üzerinde çalıştırsaydınız, zararlı yazılımın göçtüğünü ancak yazılımı kapatmadığınız takdirde arka planda çalışmaya devam ettiğini görebilirdiniz. Zararlı yazılımı Immunity Debugger aracı ile analiz ettiğinizde, programın akışının çalıştıktan kısa bir süre sonra işlem parçacığı (thread) üzerinden ilerlediğini görebilirdiniz. İşlem parçacığı üzerinden analizi devam ettirmek için ise Immunity Debugger aracının hata ayıklama ayarlarında, "break on new thread" ayarının aktif olması yeterliydi.



Size 1 Aralık 2015 tarihinde zararlı yazılım tarafından oluşturulacak 10 tane alan adının neler olduğunu sorduğum için de, sistem tarihini 1 Aralık 2015 yapmanız gerekiyordu.



Adım adım ilgili komutların üzerinden ilerlediğinizde, zararlı yazılımın GetSystemTime API'sini çağırdığını görebilirdiniz. Hata ayıklamaya devam ettiğinizde, 00401B80 fonksiyonu (subroutine) çağırıldıktan sonra alan adınının oluşturulduğunu görebilirdiniz.



Başta kazanan talihli Ramazan UYSAL olmak üzere oyunu başarıyla çözen, katılan, destekleyen, sponsor olan herkese teşekkür eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Murofet'in DGA'sı hakkında detaylı bilgi almak için bu sayfayı ziyaret edebilirsiniz.