

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:

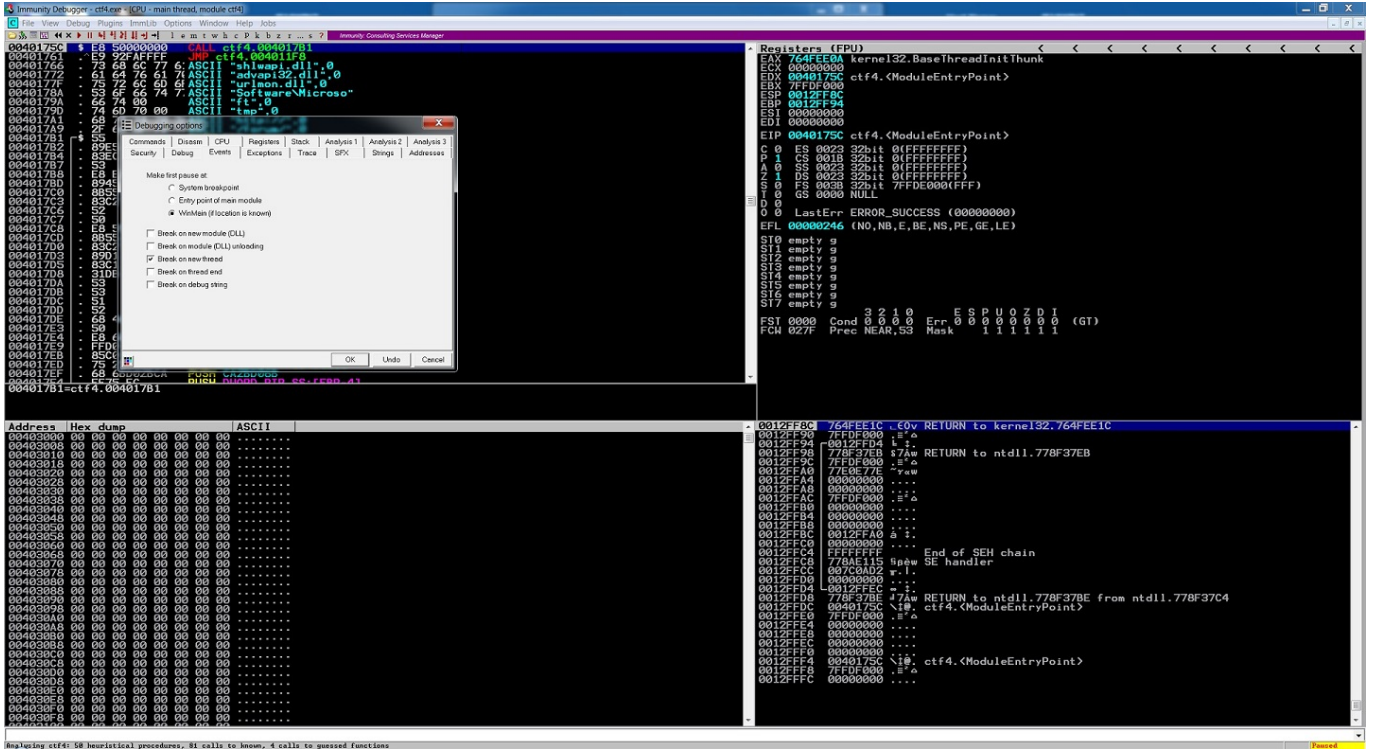
Yapacağınız ilk iş, her zararlı yazılım analizinde olduğu gibi ctf4.exe isimli bu zararlı yazılımı VirusTotal web sitesine yüklemek ve zararlı yazılım ile ilgili olarak olabildiğince bilgi toplamaya çalışmaktır.

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

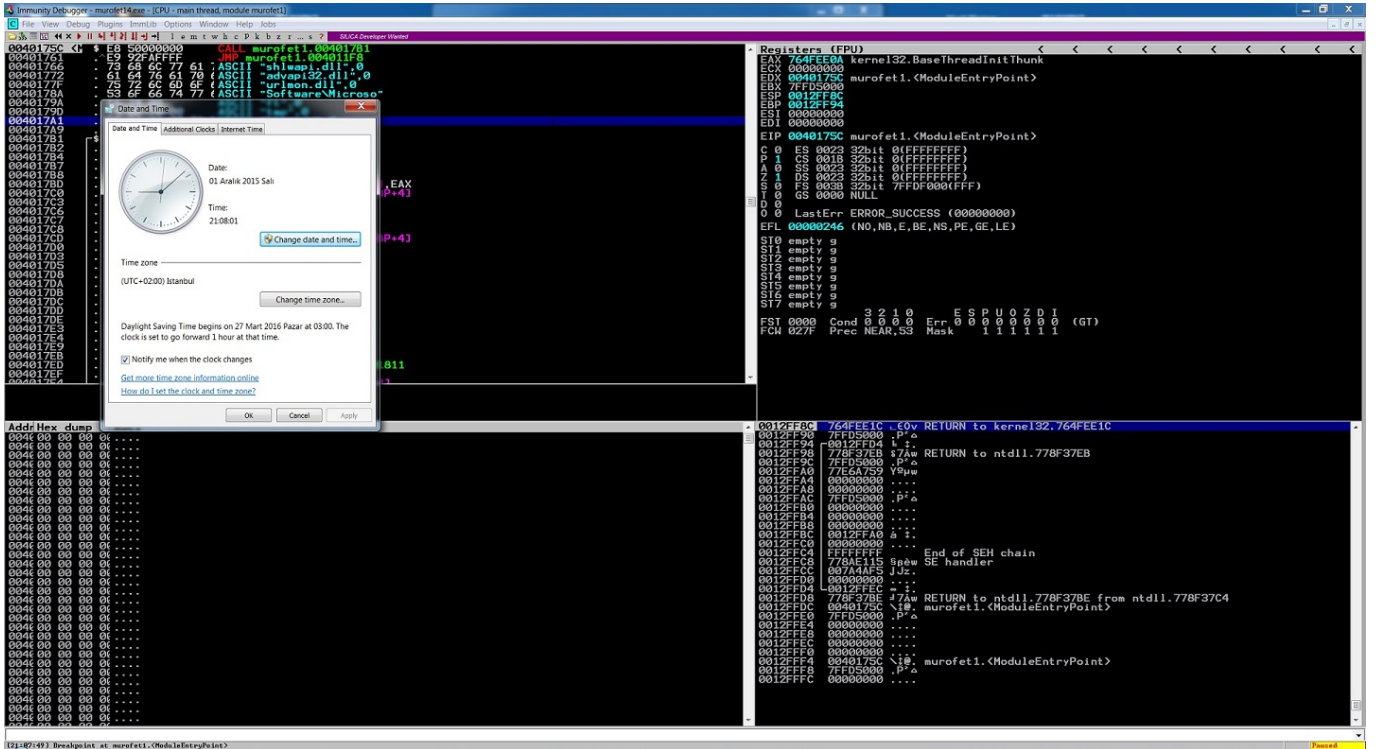
SHA256: 96370d5162c2d9e165892af3bde7c5de8c44ec5945ed0e1ddb8b27b676931d0
Dosya adı: ctf4.exe
Tespit edilme oranı: 48 / 54
Analiz tarihi: 2015-11-18 19:53:58 UTC (0 dakika önce)

Antivirüs	Sonuç	Güncelle
ALYac	Win32/Murofet.A	20151118
AVG	Cryptic.COL	20151118
AVware	Virus Win32/Murofet.a (v)	20151118
Agnitum	Trojan.DL.Small/UT6pqytkw	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.

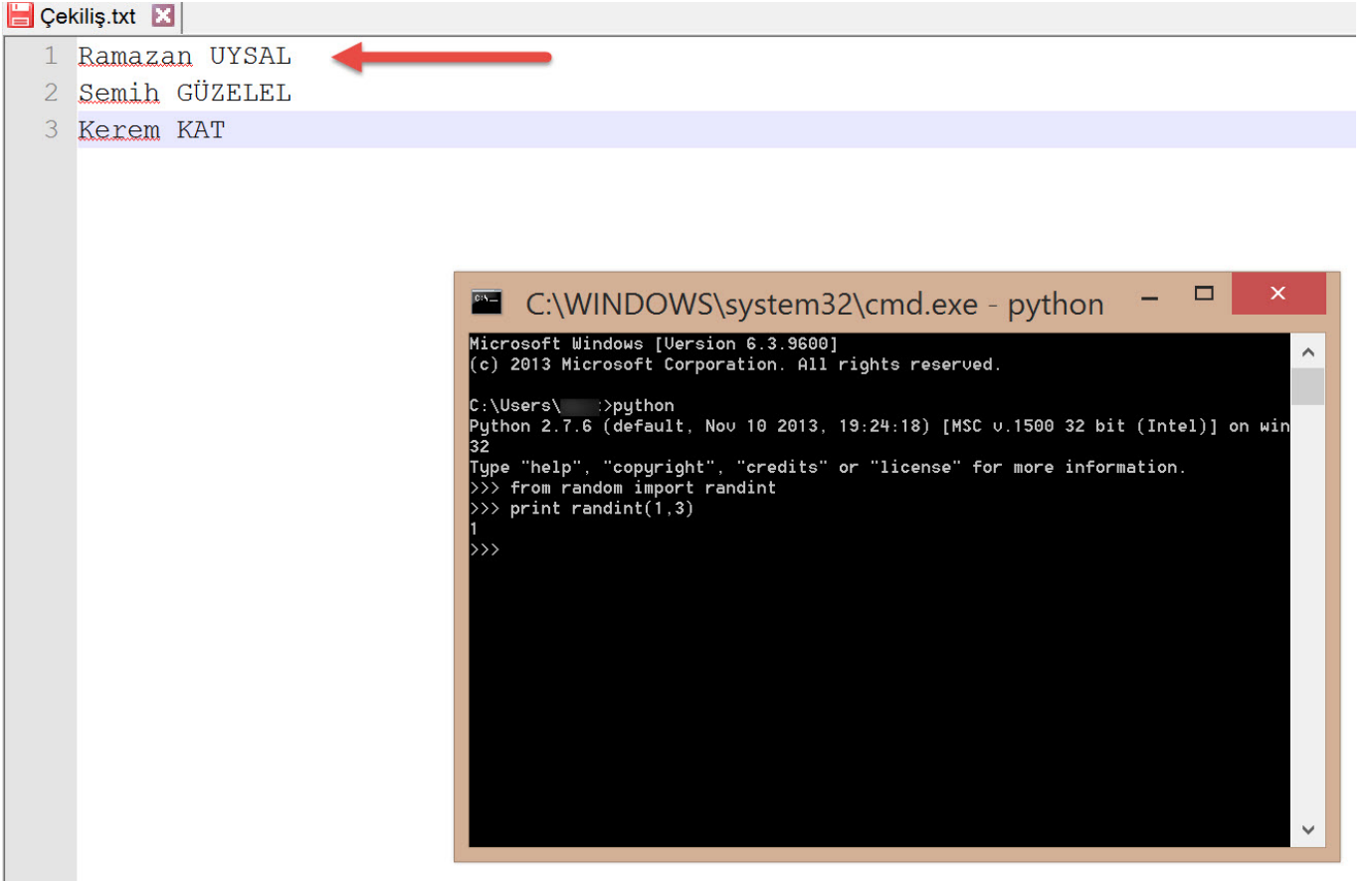


Adım adım ilgili komutların üzerinden ilerlediğinizde, zararlı yazılımın GetSystemTime API'sini çağırdığını görebilirdiniz. Hata ayıklamaya devam ettiğinizde, 00401B80 fonksiyonu (subroutine) çağırıldıktan sonra alan adının oluşturulduğunu görebilirdiniz.

File View Debug Plugins ImmLib Options Window Jobs

00401805 61 PUSH ECX
00401806 65 CS9508A7 PUSH 87A995C5
0040180B FF85 DCDFDFFF PUSH DWORD PTR SS:[EBP-224]
0040180C 65 C0100000 CALL murefet1.00401A54
0040180E FF80 PUSH EDI
0040180F 0F87B5 F2DFDFFF MOVZX EAX, DWORD PTR SS:[EBP-20E]
00401812 680C 11 MOV EAX, EAX, 11
0040181F 8B 20030000 MOV EBX, 320
0040181F 8B FC030000 MOV ECX, 3FC
00401820 7F1 J1 ECX
00401900 52 PUSH EDX
00401901 FF85 E0DFDFFF PUSH DWORD PTR SS:[EBP-220]
00401902 52 PUSH EDX
00401908 8D95 E8DFDFFF PUSH EDI, DWORD PTR SS:[EBP-218]
00401909 52 PUSH EDX
0040190F 8D95 FFDFFDFFF PUSH EDI, DWORD PTR SS:[EBP-201]
00401910 7F1 J1 ECX
00401912 EB 65020000 CALL murefet1.00401B80
0040191B 8D8C65 FFDFFDFFF LEA EDI, DWORD PTR SS:[EBP-FAX-201]
00401922 83C6 48 MOV ESI, DWORD PTR SS:[EBP-8]
00401923 83C6 48 ADD ESI, 48
00401924 59 POP ECX
00401925 83C6 48 MOV ESI, BYTE PTR ES:[EDI], BYTE PTR DS:[ESI]
00401926 59 POP ECX
00401927 59 POP ECX
00401928 59 POP ECX
00401929 59 POP ECX
0040192A 59 POP ECX
0040192B 59 POP ECX
0040192C 59 POP ECX
0040192D 59 POP ECX
0040192E 59 POP ECX
0040192F 59 POP ECX
00401930 59 POP ECX
00401931 59 POP ECX
00401932 59 POP ECX
00401933 59 POP ECX
00401934 59 POP ECX
00401935 59 POP ECX
00401936 59 POP ECX
00401937 59 POP ECX
00401938 59 POP ECX
00401939 59 POP ECX
0040193A 59 POP ECX
0040193B 59 POP ECX
0040193C 59 POP ECX
0040193D 59 POP ECX
0040193E 59 POP ECX
0040193F 59 POP ECX
00401940 59 POP ECX
00401941 59 POP ECX
00401942 59 POP ECX
00401943 59 POP ECX
00401944 59 POP ECX
00401945 59 POP ECX
00401946 59 POP ECX
00401947 59 POP ECX
00401948 59 POP ECX
00401949 59 POP ECX
0040194A 59 POP ECX
0040194B 59 POP ECX
0040194C 59 POP ECX
0040194D 59 POP ECX
0040194E 59 POP ECX
0040194F 59 POP ECX
00401950 59 POP ECX
00401951 59 POP ECX
00401952 59 POP ECX
00401953 59 POP ECX
00401954 59 POP ECX
00401955 59 POP ECX
00401956 59 POP ECX
00401957 59 POP ECX
00401958 59 POP ECX
00401959 59 POP ECX
0040195A 59 POP ECX
0040195B 59 POP ECX
0040195C 59 POP ECX
0040195D 59 POP ECX
0040195E 59 POP ECX
0040195F 59 POP ECX
00401960 59 POP ECX
00401961 59 POP ECX
00401962 59 POP ECX
00401963 59 POP ECX
00401964 59 POP ECX
00401965 59 POP ECX
00401966 59 POP ECX
00401967 59 POP ECX
00401968 59 POP ECX
00401969 59 POP ECX
0040196A 59 POP ECX
0040196B 59 POP ECX
0040196C 59 POP ECX
0040196D 59 POP ECX
0040196E 59 POP ECX
0040196F 59 POP ECX
00401970 59 POP ECX
00401971 59 POP ECX
00401972 59 POP ECX
00401973 59 POP ECX
00401974 59 POP ECX
00401975 59 POP ECX
00401976 59 POP ECX
00401977 59 POP ECX
00401978 59 POP ECX
00401979 59 POP ECX
0040197A 59 POP ECX
0040197B 59 POP ECX
0040197C 59 POP ECX
0040197D 59 POP ECX
0040197E 59 POP ECX
0040197F 59 POP ECX
00401980 59 POP ECX
00401981 59 POP ECX
00401982 59 POP ECX
00401983 59 POP ECX
00401984 59 POP ECX
00401985 59 POP ECX
00401986 59 POP ECX
00401987 59 POP ECX
00401988 59 POP ECX
00401989 59 POP ECX
0040198A 59 POP ECX
0040198B 59 POP ECX
0040198C 59 POP ECX
0040198D 59 POP ECX
0040198E 59 POP ECX
0040198F 59 POP ECX
00401990 59 POP ECX
00401991 59 POP ECX
00401992 59 POP ECX
00401993 59 POP ECX
00401994 59 POP ECX
00401995 59 POP ECX
00401996 59 POP ECX
00401997 59 POP ECX
00401998 59 POP ECX
00401999 59 POP ECX
0040199A 59 POP ECX
0040199B 59 POP ECX
0040199C 59 POP ECX
0040199D 59 POP ECX
0040199E 59 POP ECX
0040199F 59 POP ECX
004019A0 59 POP ECX
004019A1 59 POP ECX
004019A2 59 POP ECX
004019A3 59 POP ECX
004019A4 59 POP ECX
004019A5 59 POP ECX
004019A6 59 POP ECX
004019A7 59 POP ECX
004019A8 59 POP ECX
004019A9 59 POP ECX
004019AA 59 POP ECX
004019AB 59 POP ECX
004019AC 59 POP ECX
004019AD 59 POP ECX
004019AE 59 POP ECX
004019AF 59 POP ECX
004019B0 59 POP ECX
004019B1 59 POP ECX
004019B2 59 POP ECX
004019B3 59 POP ECX
004019B4 59 POP ECX
004019B5 59 POP ECX
004019B6 59 POP ECX
004019B7 59 POP ECX
004019B8 59 POP ECX
004019B9 59 POP ECX
004019BA 59 POP ECX
004019BB 59 POP ECX
004019BC 59 POP ECX
004019BD 59 POP ECX
004019BE 59 POP ECX
004019BF 59 POP ECX
004019C0 59 POP ECX
004019C1 59 POP ECX
004019C2 59 POP ECX
004019C3 59 POP ECX
004019C4 59 POP ECX
004019C5 59 POP ECX
004019C6 59 POP ECX
004019C7 59 POP ECX
004019C8 59 POP ECX
004019C9 59 POP ECX
004019CA 59 POP ECX
004019CB 59 POP ECX
004019CC 59 POP ECX
004019CD 59 POP ECX
004019CE 59 POP ECX
004019CF 59 POP ECX
004019D0 59 POP ECX
004019D1 59 POP ECX
004019D2 59 POP ECX
004019D3 59 POP ECX
004019D4 59 POP ECX
004019D5 59 POP ECX
004019D6 59 POP ECX
004019D7 59 POP ECX
004019D8 59 POP ECX
004019D9 59 POP ECX
004019DA 59 POP ECX
004019DB 59 POP ECX
004019DC 59 POP ECX
004019DD 59 POP ECX
004019DE 59 POP ECX
004019DF 59 POP ECX
004019E0 59 POP ECX
004019E1 59 POP ECX
004019E2 59 POP ECX
004019E3 59 POP ECX
004019E4 59 POP ECX
004019E5 59 POP ECX
004019E6 59 POP ECX
004019E7 59 POP ECX
004019E8 59 POP ECX
004019E9 59 POP ECX
004019EA 59 POP ECX
004019EB 59 POP ECX
004019EC 59 POP ECX
004019ED 59 POP ECX
004019EE 59 POP ECX

[illegible]



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.