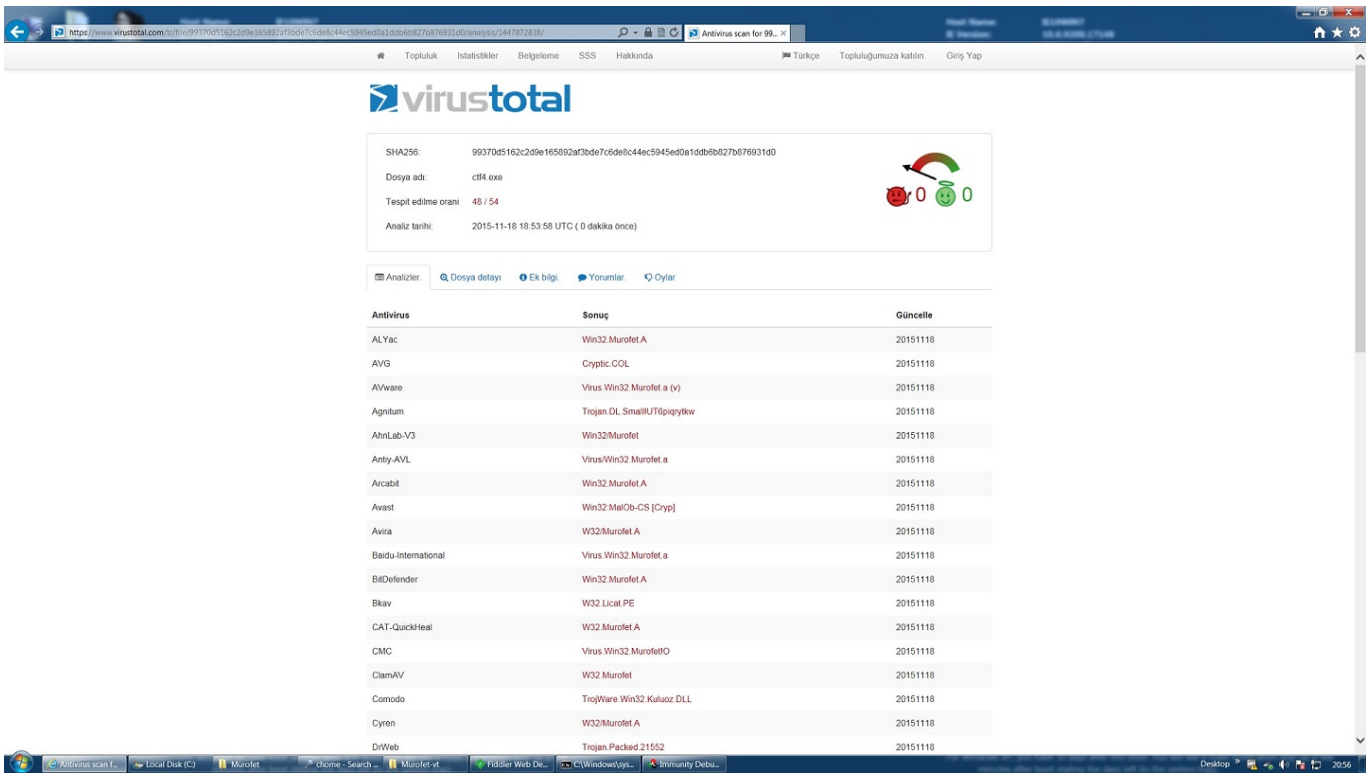
Pi Hediyem Vardı, Verdim, Gitti #4 :)

written by Mert SARICA | 30 November 2015

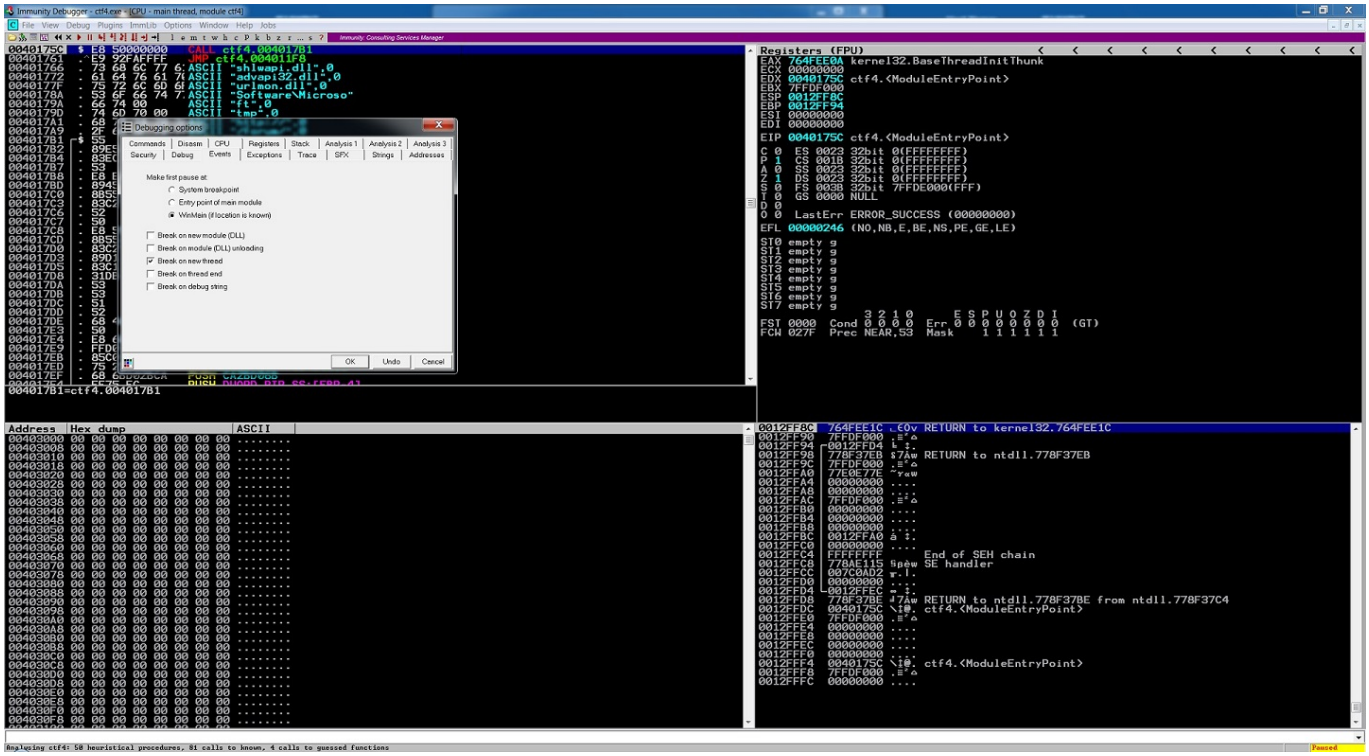
18 Kasım 2015 tarihinde dördüncüsü düzenlenen Pi Hediyem Var oyununun çözüm yolu ve Raspberry Pi kazanan talihli karşınızda!

ÇÖZÜM YOLU:

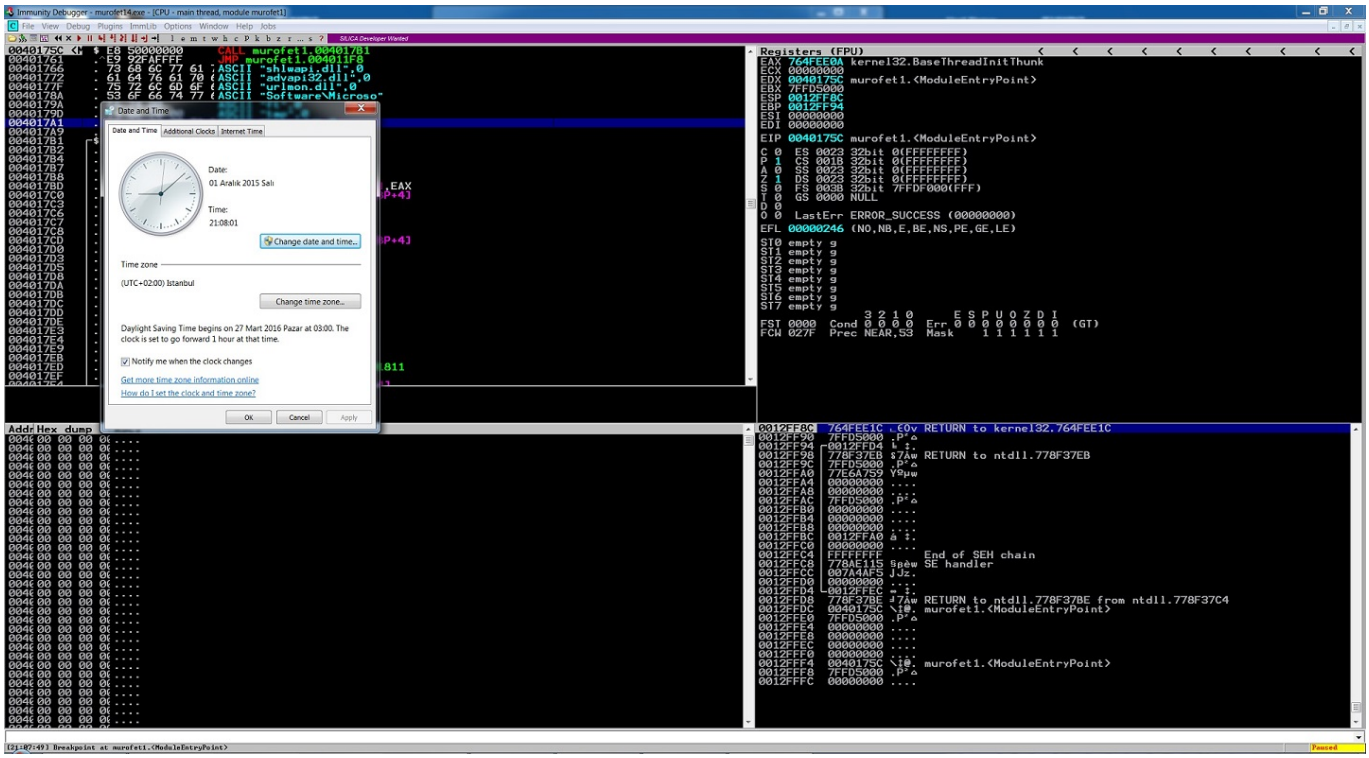
Yapacağınız ilk iş, her zararlı yazılım analizinde olduğu gibi ctf4.exe isimli bu zararlı yazılımı VirusTotal web sitesine yüklemek ve zararlı yazılım ile ilgili olarak olabildiğince bilgi toplamaya çalışmaktı. VirusTotal'a dosyayı yüklediğinizde karşınıza çıkan Antivirüs çıktılarından bunun Murofet isimli bir zararlı yazılım olduğunu anlayabilirdiniz.



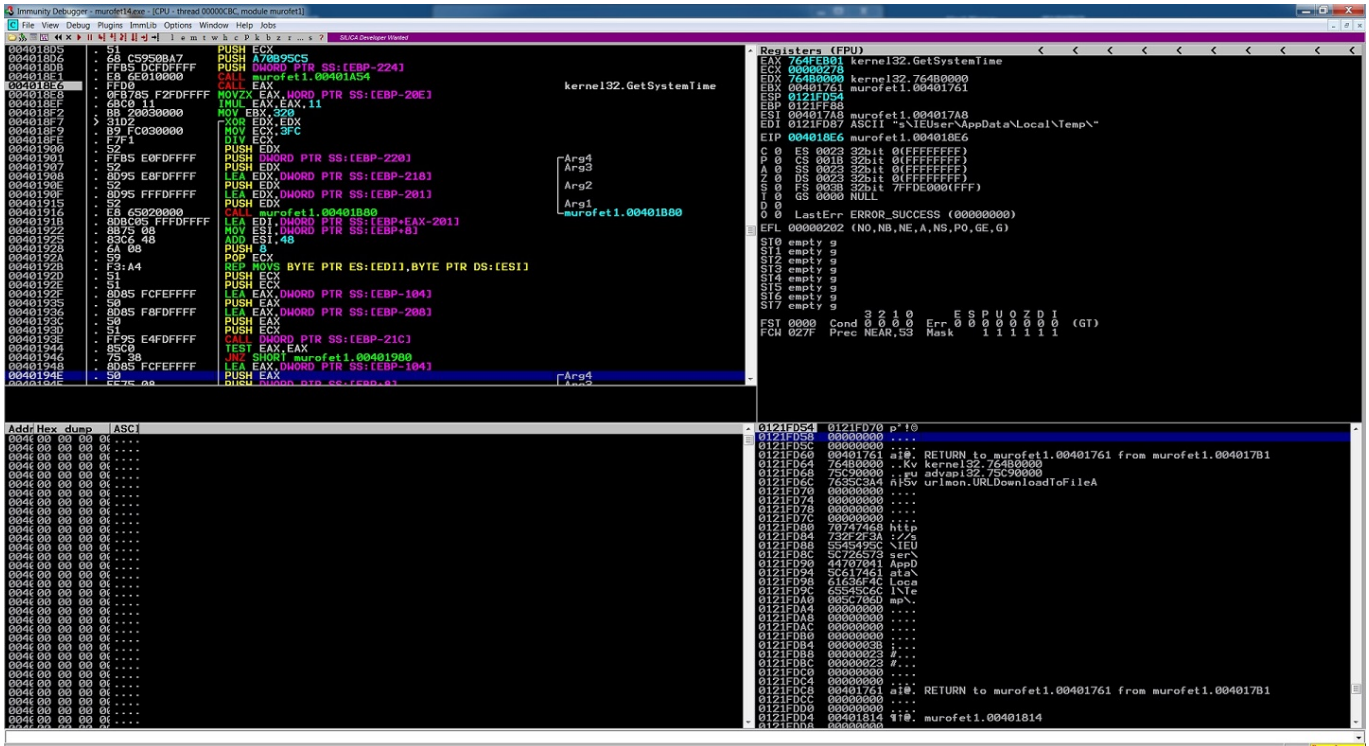
Ardından ctf4.exe zararlı yazılımını Windows XP işletim sistemi üzerinde çalıştırsaydınız, zararlı yazılımın göçtüğünü ancak yazılımı kapatmadığınız taktirde arka planda çalışmaya devam ettiğini görebilirdiniz. Zararlı yazılımı Immunity Debugger aracı ile analiz ettiğinizde, programın akışının çalıştıktan 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.

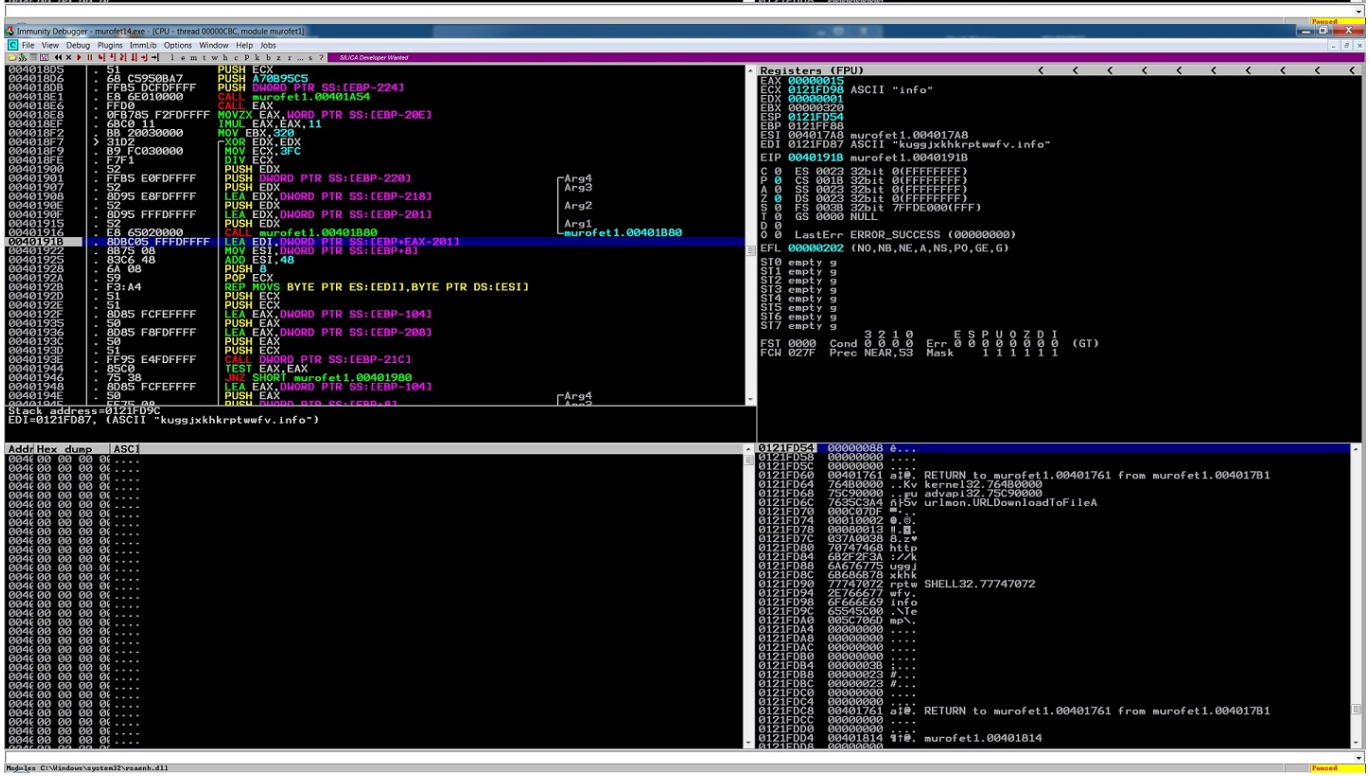


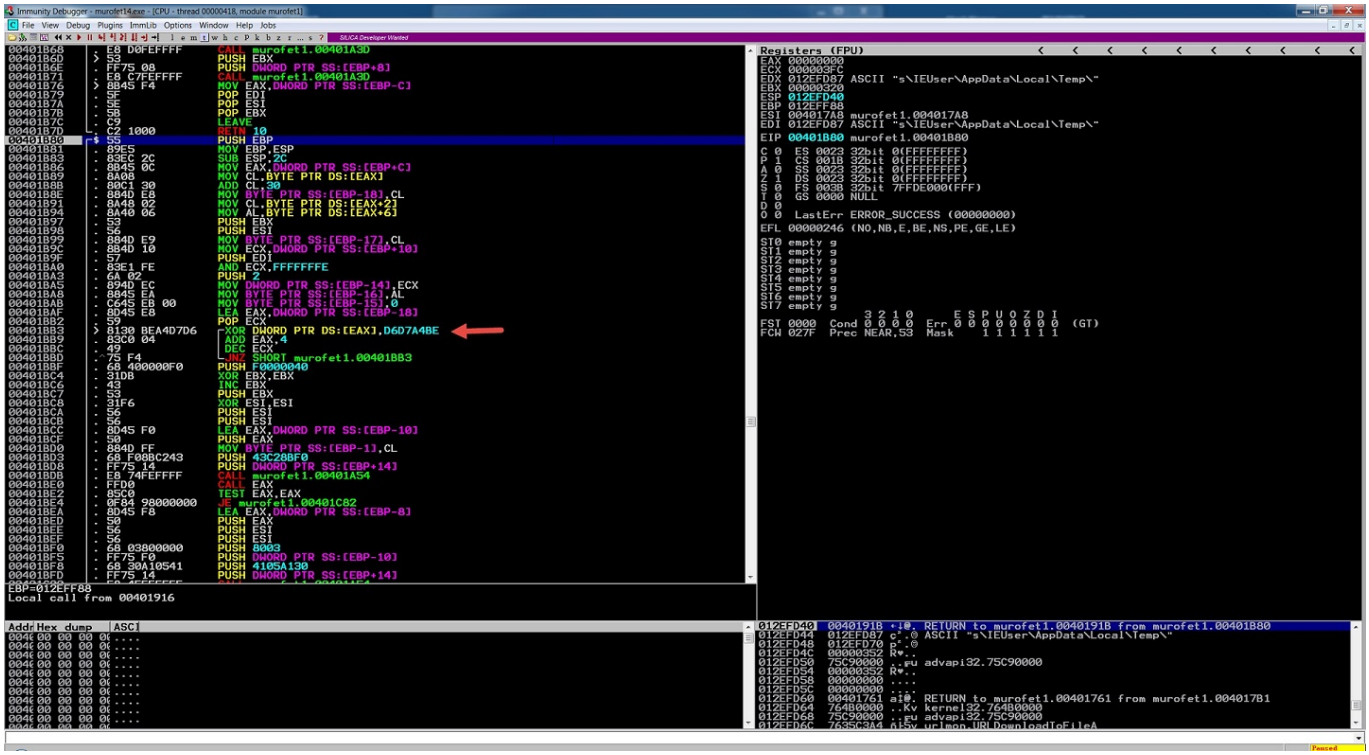
Size 1 Aralık 2015 tarihinde zararlı yazılım tarafından oluşturulacak 10 tane alan adının neler olduğunu sorduğum için de, sistem tarihini 1 Aralık 2015 yapmanız gerekiyordu.



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


Immunity Debugger - murofet14.exe - [CPU - thread 00000CBC, module murofet1]
File View Debug Plugins ImmLib Options Window Help Jobs
SILICA Developer Wanted
004018D5 . 51 PUSH ECX
004018D6 . 68 C59950BA7 PUSH A70B95C5
004018DB . FFB5 DCFDFFFF PUSH DWORD PTR SS:[EBP-224]
004018E1 . E8 6E010000 CALL murofet1.00401A54
004018E6 . FFD0 CALL EAX kernel32.GetSystemTime
004018E8 . 0FB785 F2FDFFFF MOVZX EAX,WORD PTR SS:[EBP-20E]
004018EF . 6BC0 11 IMUL EAX,EAX,11
004018F2 . B8 20030000 MOV EBX,320
004018F7 > 31D2 XOR EDX,EDX
004018F9 . B9 FC030000 MOV ECX,3FC
004018FE . F7F1 DIV ECX
00401900 . 52 PUSH EDX
00401901 . FFB5 E0FDFFFF PUSH DWORD PTR SS:[EBP-220] Arg4
00401907 . 52 PUSH EDX Arg3
00401908 . 8D95 E8FDFFFF LEA EDX,DWORD PTR SS:[EBP-218] Arg2
0040190E . 52 PUSH EDX
0040190F . 8D95 FFFDFFFF LEA EDX,DWORD PTR SS:[EBP-201]
00401915 . 52 PUSH EDX Arg1
00401916 . E8 65020000 CALL murofet1.00401B80 murofet1.00401B80
0040191B . 8DBC05 FFFDFFFF LEA EDI,DWORD PTR SS:[EBP+EAX-201]
00401922 . 8B75 08 MOV ESI,DWORD PTR SS:[EBP+8]
00401925 . 83C6 48 ADD ESI,48
00401928 . 6A 08 PUSH 8
0040192A . 59 POP ECX
0040192B . F3:A4 REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
0040192D . 51 PUSH ECX
0040192E . 51 PUSH ECX
0040192F . 8D85 FCFEFFFF LEA EAX,DWORD PTR SS:[EBP-104]
00401935 . 50 PUSH EAX
00401936 . 8D85 F8FDFFFF LEA EAX,DWORD PTR SS:[EBP-208]
0040193C . 50 PUSH EAX
0040193D . 51 PUSH ECX
0040193E . FF95 E4FDFFFF CALL DWORD PTR SS:[EBP-21C]
00401944 . 85C0 TEST EAX,EAX
00401946 . 75 38 JNZ SHORT murofet1.00401980
00401948 . 8D85 FCFEFFFF LEA EAX,DWORD PTR SS:[EBP-104]
0040194E . 50 PUSH EAX Arg4
Registers (FPU)
EAX 764FEB01 kernel32.GetSystemTime
ECX 00000278
EDX 76480000 kernel32.764B0000
EBX 00401761 murofet1.00401761
ESP 0121FD54
EBP 0121FF88
ESI 004017A8 murofet1.004017A8
EDI 0121FD87 ASCII "s\IEUser\AppData\Local\Temp\"
EIP 004018E6 murofet1.004018E6
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDE000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Addr Hex dump ASCI
0121FD54 0121FD70 p'!@
0121FD58 00000000 ....
0121FD5C 00000000 ....
0121FD60 00401761 ai@. RETURN to murofet1.00401761 from murofet1.004017B1
0121FD64 76480000 ..Kv kernel32.76480000
0121FD68 75C90000 ..ɣu advapi32.75C90000
0121FD6C 7635C3A4 ñ5Sv urlmon.URLDownloadToFileA
0121FD70 00000000 ....
0121FD74 00000000 ....
0121FD78 00000000 ....
0121FD7C 00000000 ....
0121FD80 70747468 http
0121FD84 732F2F3A :// s
0121FD88 5545495C \IEU
0121FD8C 5C726573 ser\
0121FD90 44707041 AppD
0121FD94 5C617461 ata\
0121FD98 61636F4C Loca
0121FD9C 6554456C l\Te
0121FDA0 005C706D mp\.
0121FDA4 00000000 ....
0121FDA8 00000000 ....
0121FDAC 00000000 ....
0121FDB0 00000000 ....
0121FDB4 0000003B ;...
0121FDB8 00000023 #...
0121FDBC 00000023 #...
0121FDC0 00000000 ....
0121FDC4 00000000 ....
0121FDC8 00401761 ai@. RETURN to murofet1.00401761 from murofet1.004017B1
0121FDCC 00000000 ....
0121FDD0 00000000 ....
0121FDD4 00401814 ¶¶@. murofet1.00401814
0121FDD8 00000000 ....

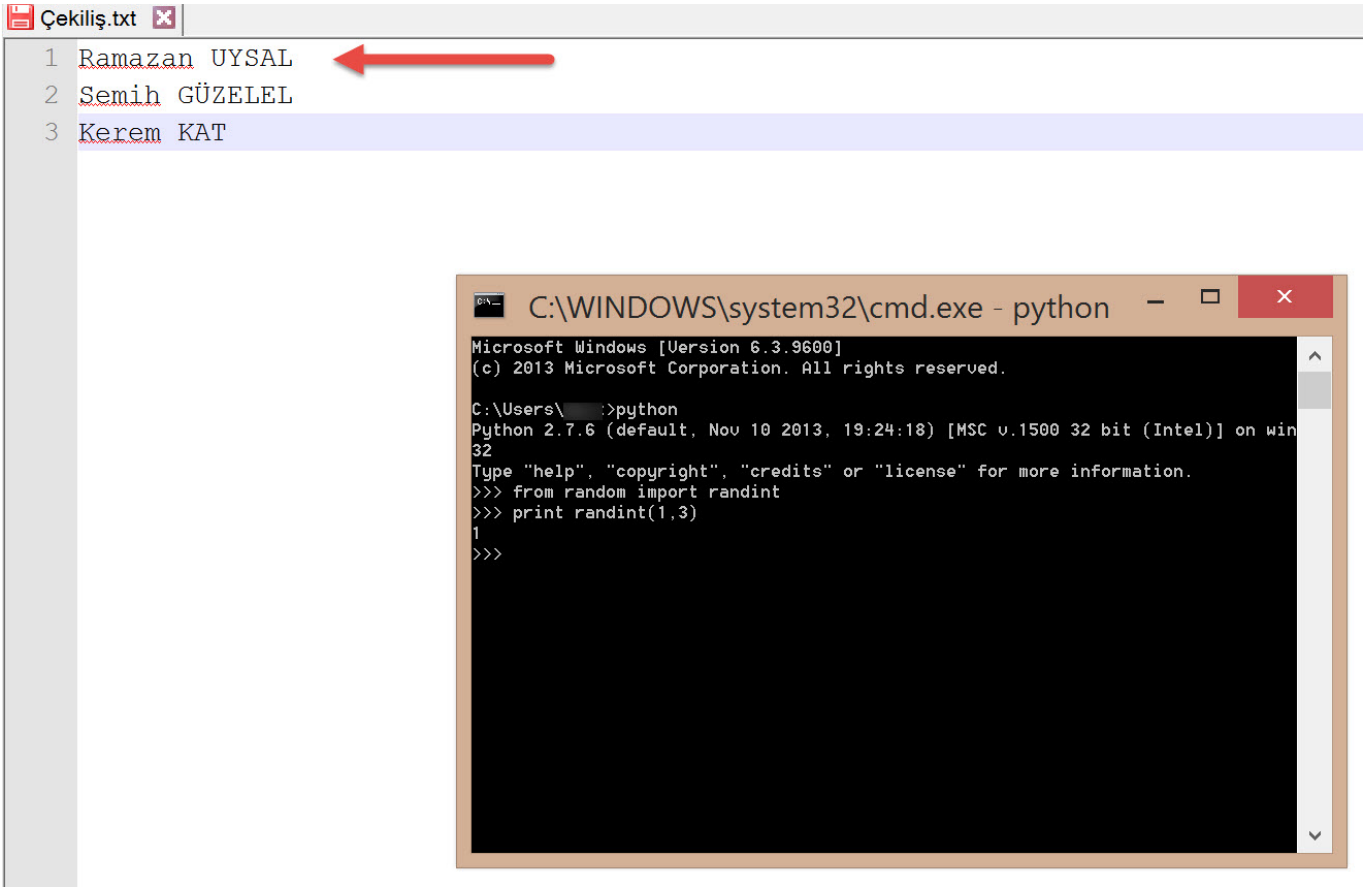

Immunity Debugger - murofet14.exe - [CPU - thread 00000CBC, module murofet1]
File View Debug Plugins ImmLib Options Window Help Jobs
SILICA Developer Wanted
004018D5 . 51 PUSH ECX
004018D6 . 68 C59950BA7 PUSH A70B95C5
004018DB . FFB5 DCFDFFFF PUSH DWORD PTR SS:[EBP-224]
004018E1 . E8 6E010000 CALL murofet1.00401A54
004018E6 . FFD0 CALL EAX
004018E8 . 0FB785 F2FDFFFF MOVZX EAX,WORD PTR SS:[EBP-20E]
004018EF . 6BC0 11 IMUL EAX,EAX,11
004018F2 . B8 20030000 MOV EBX,320
004018F7 > 31D2 XOR EDX,EDX
004018F9 . B9 FC030000 MOV ECX,3FC
004018FE . F7F1 DIV ECX
00401900 . 52 PUSH EDX
00401901 . FFB5 E0FDFFFF PUSH DWORD PTR SS:[EBP-220] Arg4
00401907 . 52 PUSH EDX Arg3
00401908 . 8D95 E8FDFFFF LEA EDX,DWORD PTR SS:[EBP-218] Arg2
0040190E . 8D95 FFFDFFFF LEA EDX,DWORD PTR SS:[EBP-201]
00401915 . 52 PUSH EDX Arg1
00401916 . E8 65020000 CALL murofet1.00401B80 murofet1.00401B80
0040191B . 8DBC05 FFFDFFFF LEA EDI,DWORD PTR SS:[EBP+EAX-201]
00401922 . 8B75 08 MOV ESI,DWORD PTR SS:[EBP+8]
00401925 . 83C6 48 ADD ESI,48
00401928 . 6A 08 PUSH 8
0040192A . 59 POP ECX
0040192B . F3:A4 REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
0040192D . 51 PUSH ECX
0040192E . 51 PUSH ECX
0040192F . 8D85 FCFEFFFF LEA EAX,DWORD PTR SS:[EBP-104]
00401935 . 50 PUSH EAX
00401936 . 8D85 F8FDFFFF LEA EAX,DWORD PTR SS:[EBP-208]
0040193C . 50 PUSH EAX
0040193D . 51 PUSH ECX
0040193E . FF95 E4FDFFFF CALL DWORD PTR SS:[EBP-21C]
00401944 . 85C0 TEST EAX,EAX
00401946 . 75 38 JNZ SHORT murofet1.00401980
00401948 . 8D85 FCFEFFFF LEA EAX,DWORD PTR SS:[EBP-104]
0040194E . 50 PUSH EAX Arg4
Stack address=0121FD9C
EDI=0121FD87, (ASCII "kuggjxkhkrptwwfv.info")
Registers (FPU)
EAX 00000015
ECX 0121FD98 ASCII "info"
EDX 00000001
EBX 00000320
ESP 0121FD54
EBP 0121FF88
ESI 004017A8 murofet1.004017A8
EDI 0121FD87 ASCII "kuggjxkhkrptwwfv.info"
EIP 0040191B murofet1.0040191B
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDE000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Addr Hex dump ASCI
0121FD54 00000088 ê...
0121FD58 00000000 ....
0121FD5C 00000000 ....
0121FD60 00401761 ai@. RETURN to murofet1.00401761 from murofet1.004017B1
0121FD64 76480000 ..Kv kernel32.76480000
0121FD68 75C90000 ..ɣu advapi32.75C90000
0121FD6C 7635C3A4 ñ5Sv urlmon.URLDownloadToFileA
0121FD70 000C07DF ■•..
0121FD74 00010002 ☺.☺.
0121FD78 00000013 !!■.
0121FD7C 037A003B 8.z♥
0121FD80 70747468 http
0121FD84 6B2F2F3A :// k
0121FD88 6A676775 uggj
0121FD8C 6B686B78 xhk k
0121FD90 77747072 rptw SHELL32.77747072
0121FD94 2E766677 wfv.
0121FD98 6F666E69 info
0121FD9C 6554456C l\Te
0121FDA0 005C706D mp\.
0121FDA4 00000000 ....
0121FDA8 00000000 ....
0121FDAC 00000000 ....
0121FDB0 00000000 ....
0121FDB4 0000003B ;...
0121FDB8 00000023 #...
0121FDBC 00000023 #...
0121FDC0 00000000 ....
0121FDC4 00000000 ....
0121FDC8 00401761 ai@. RETURN to murofet1.00401761 from murofet1.004017B1
0121FDCC 00000000 ....
0121FDD0 00000000 ....
0121FDD4 00401814 ¶¶@. murofet1.00401814
0121FDD8 00000000 ....
Modules C:\Windows\system32\rsaenh.dll



Bu fonksiyonun tamamını kopyalamanız ve ardından Fiddler, Charles Proxy, Burp Suite gibi bir proxy aracı ile oluşturulan web trafiğinden tespit ettiğiniz 10 tane alan adı ile birlikte bana göndermeniz, oyunu başarıyla tamamlamanız için yeterli olacaktı.

OYUNU BAŞARIYLA TAMAMLAYANLAR: Ramazan UYSAL, Semih GÜZELEL, Kerem KAT

ÇEKİLİŞ ve KAZANAN TALİHLİ: Ramazan UYSAL



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.