

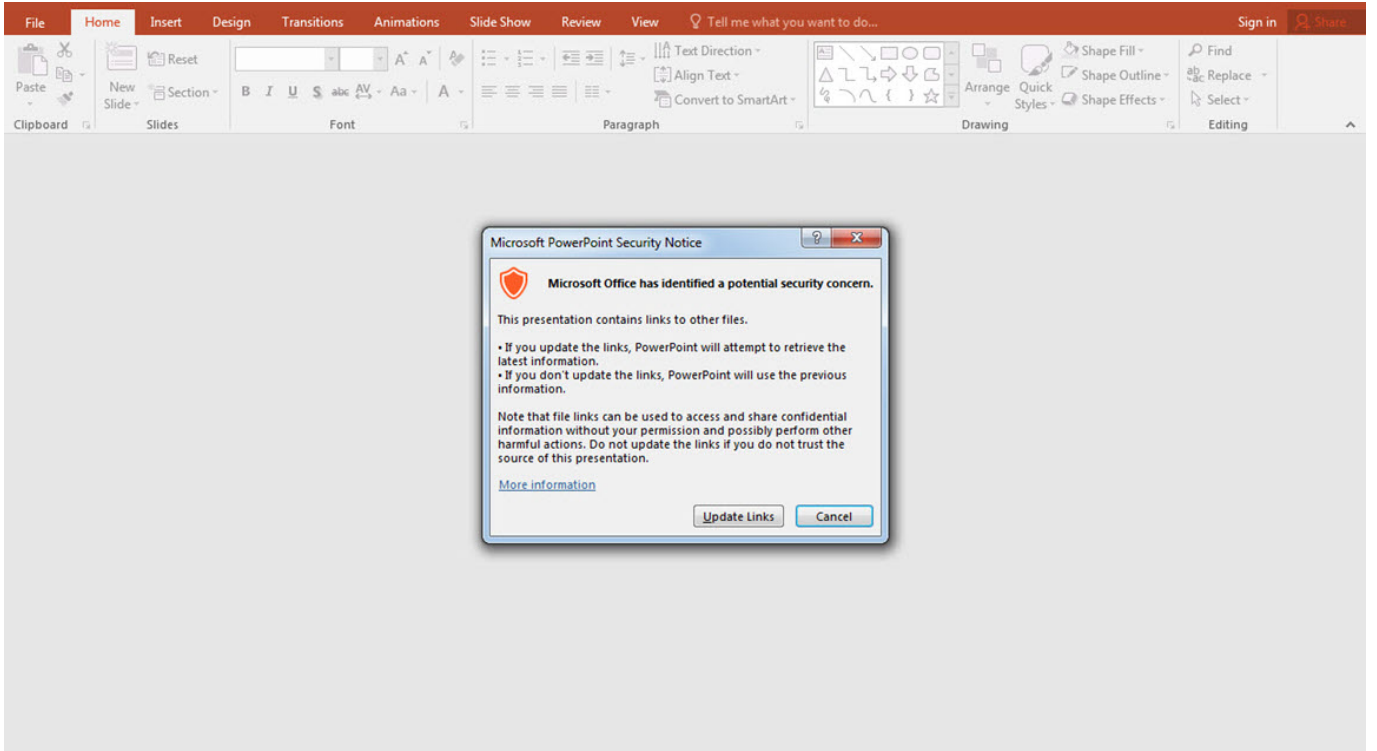
Önüm Arkam Sağım Solum Cobalt Strike

written by Mert SARICA | 1 February 2019

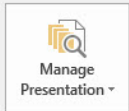
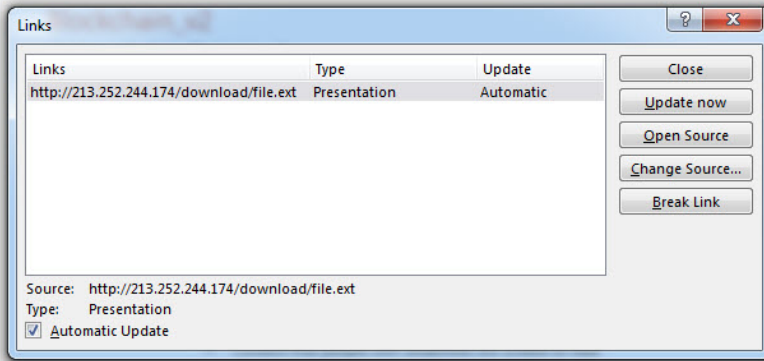
Son yıllarda özellikle finansal kurumlara gerçekleştirilen hedeflenmiş siber saldırılara (APT) bakıldığında, sızma testi uzmanlarının da yakından bildiği Cobalt Strike aracının kullanıldığını görebilirsiniz. Hatta Rusya'nın merkez bankası yetkililerine kulak vererseniz, 2017 yılında bu araçla 240 bankaya 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 üretilip 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/](http://213[.]252.244.174/download/) web adresinden file.ext dosyasının indirilip çalıştırılacağı anlaşılır.



Info



Manage Presentation

Check in, check out, and recover unsaved changes.

There are no unsaved changes.

Properties

Size	4,13MB
Slides	30
Hidden slides	0
Title	PowerPoint Presentation
Tags	Add a tag
Categories	Add a category

Related Dates

Last Modified	03.04.2018 09:26
Created	15.09.2014 10:14
Last Printed	

Related People

Author	
	Add an author
Last Modified By	Windows User

Related Documents

- Open File Location
- Edit Links to Files
- Show All Properties

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.

Haberler

“Festy Unveils Digital Currency Payments Wristband”

Amaç: Festivalde ödemeleri Dash dijital para birimini kullanarak yapmak

Kurumlar: Festy

Combining two of the most hyped trends in fintech, wearables and cryptocurrencies, Irish startup Festy has unveiled a wristband that lets festival-goers make contactless payments in Dash.

User add the Dash currency to their QR code and NFC-integrated wristband and then use it to pay for food and drinks at POS terminals where Visa contactless is accepted as well as on phones with NFC tags.

Festy is linked directly to a consumer's Dash account so transactions occur within seconds, while merchants have the ability to cash out their Dash for the equivalent fiat currency.

Dash claims to be the world's leading digital currency for payments and is currently the sixth most valued cryptocurrency at over \$1.3 billion. Festy argues that the currency is ideal for festivals, where party-goers often have long waits in line to use ATMs that can charge several euros per withdrawal.

Graham de Barra, CEO, Festy: "Unlike existing traditional bank payments that take a 2-5% fee, there is no cost on receiving Dash for merchants. Merchants accepting payments will never have a chargeback, and there are potentially enormous savings to be made compared to the crippling fees from existing payment solutions."



Haberler

“Festy Unveils Digital Currency Payments Wristband”

Amaç: Festivalde ödemeleri Dash dijital para birimini kullanarak yapmak

Kurumlar: Festy

Combining two of the most hyped trends in fintech, wearables and cryptocurrencies, Irish startup Festy has unveiled a wristband that lets festival-goers make contactless payments in Dash.

User add the Dash currency to their QR code and NFC-integrated wristband and then use it to pay for food and drinks at POS terminals where Visa contactless is accepted as well as on phones with NFC tags.

Festy is linked directly to a consumer's Dash account so transactions occur within seconds, while merchants have the ability to cash out their Dash for the equivalent fiat currency.

Dash claims to be the world's leading digital currency for payments and is currently the sixth most valued cryptocurrency at over \$1.3 billion. Festy argues that the currency is ideal for festivals, where party-goers often have long waits in line to use ATMs that can charge several euros per withdrawal.

Graham de Barra, CEO, Festy: "Unlike existing traditional bank payments that take a 2-5% fee, there is no cost on receiving Dash for merchants. Merchants accepting payments will never have a chargeback, and there are potentially enormous savings to be made compared to the crippling fees from existing payment solutions."

[Loading...Please wait](#)

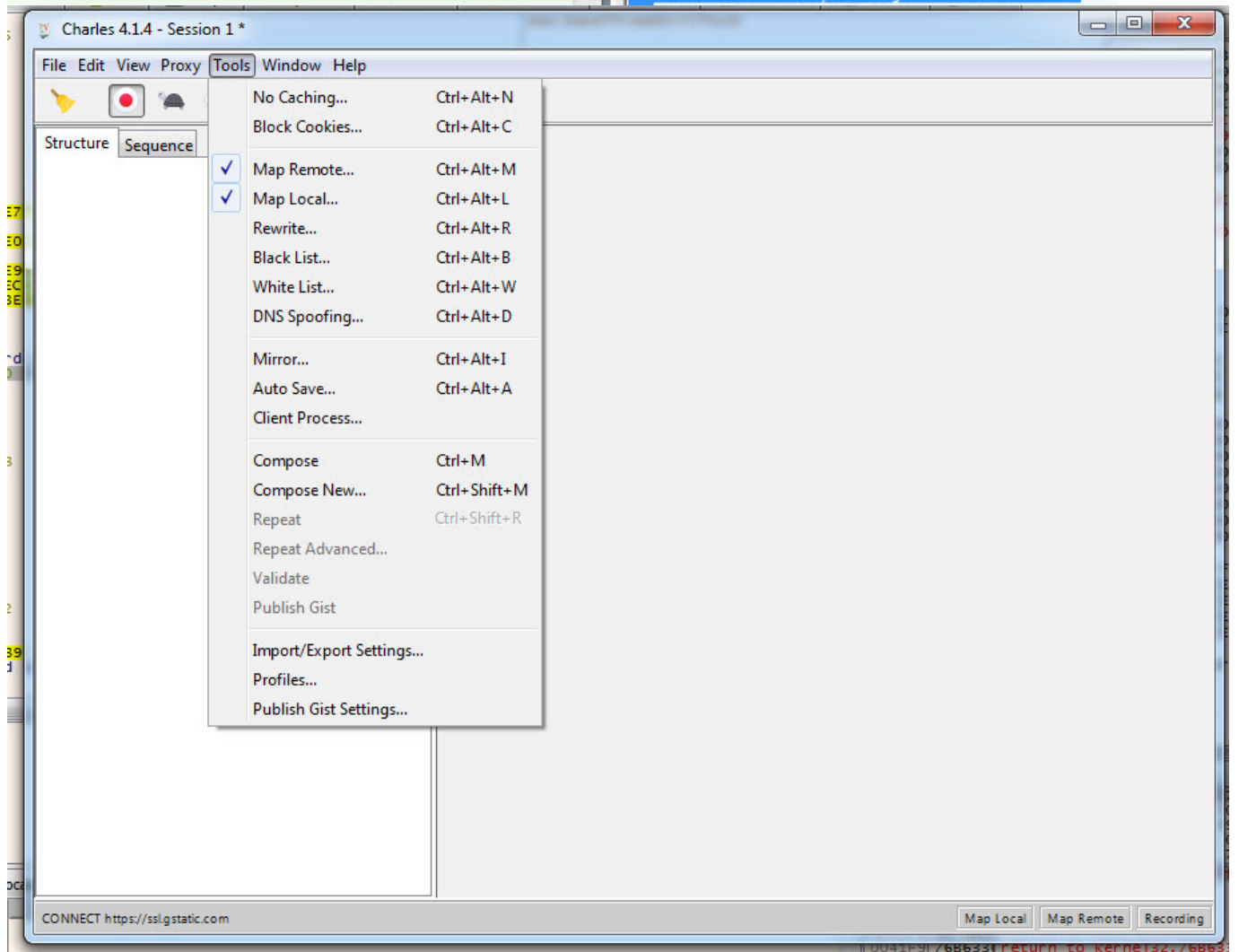
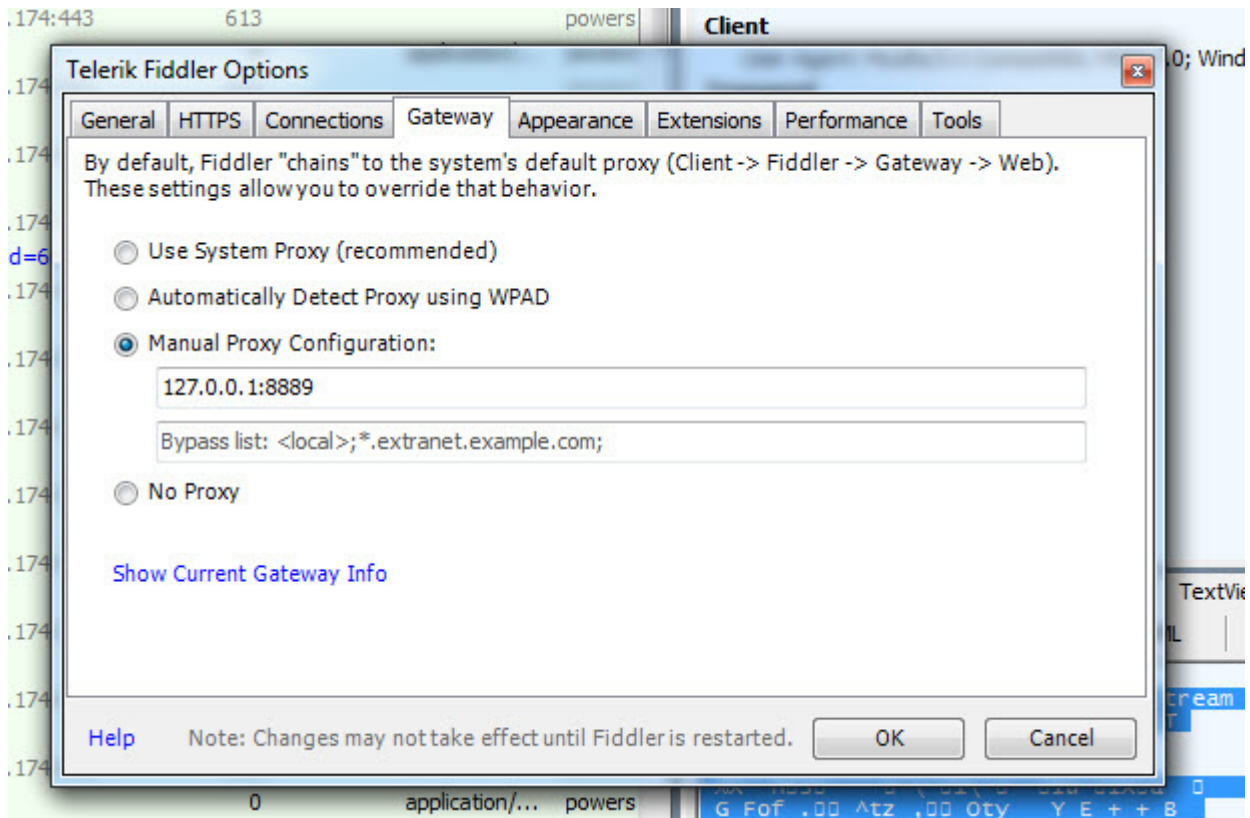
file.ext dosyasının içeriğine bakıldığında, VBS (Visual Basic Script) betiği içerisinde çağrılan, base64 ile gizlenmiş (encode) bir powershell betiği olduğu görülür. Bu betik çözüldükten (decode) sonra ise bu defa bellekte bir alana enjekte edildikten sonra CreateThread API'si ile çalıştırılan, base64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

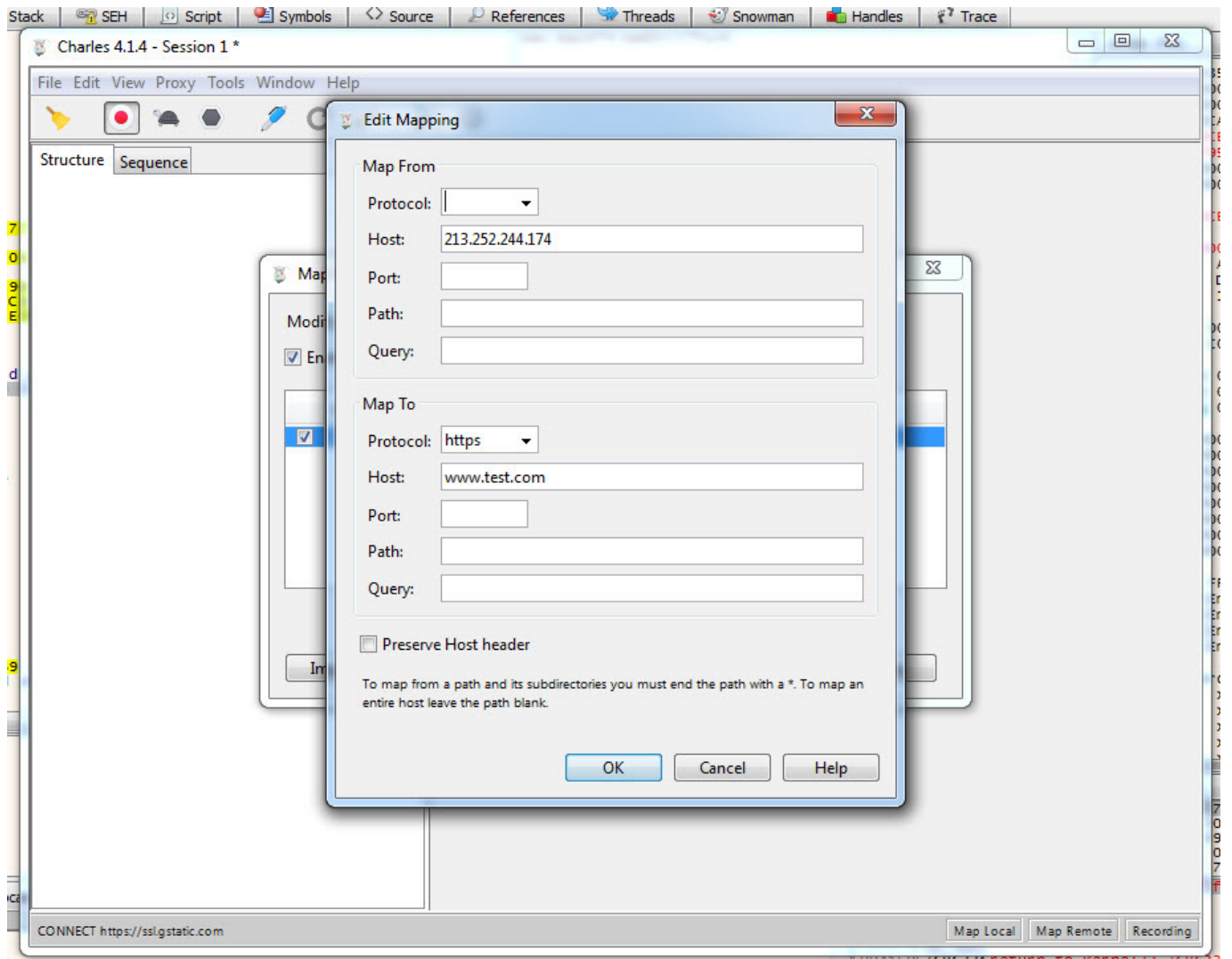
[illegible][illegible]

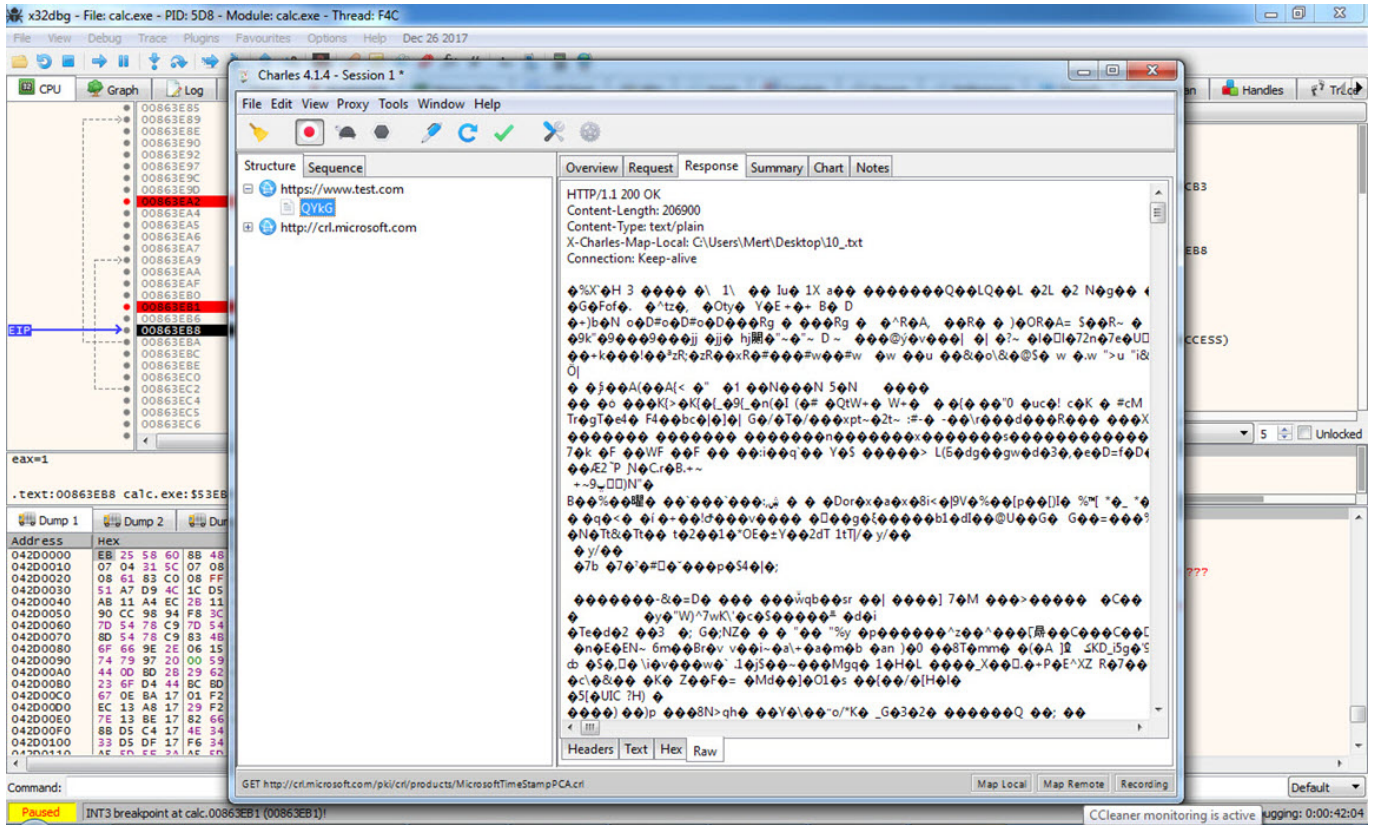
The screenshot displays the Telerik Fiddler Web Debugger interface. The main window is divided into two panes. The left pane shows a list of captured requests with columns for Pro..., Host, URL, Body, Caching, Content-Type, and Process. The right pane shows the details of the selected request, including Request Headers, Cache, Client, Transport, and a hex dump of the body.

Request List (Left Pane):

Pro...	Host	URL	Body	Caching	Content-Type	Process
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/QYkG	206.900		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/en_US/all.js	48		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/submit.php?id=69555	0		text/html	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/QYkG	206.900		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	p







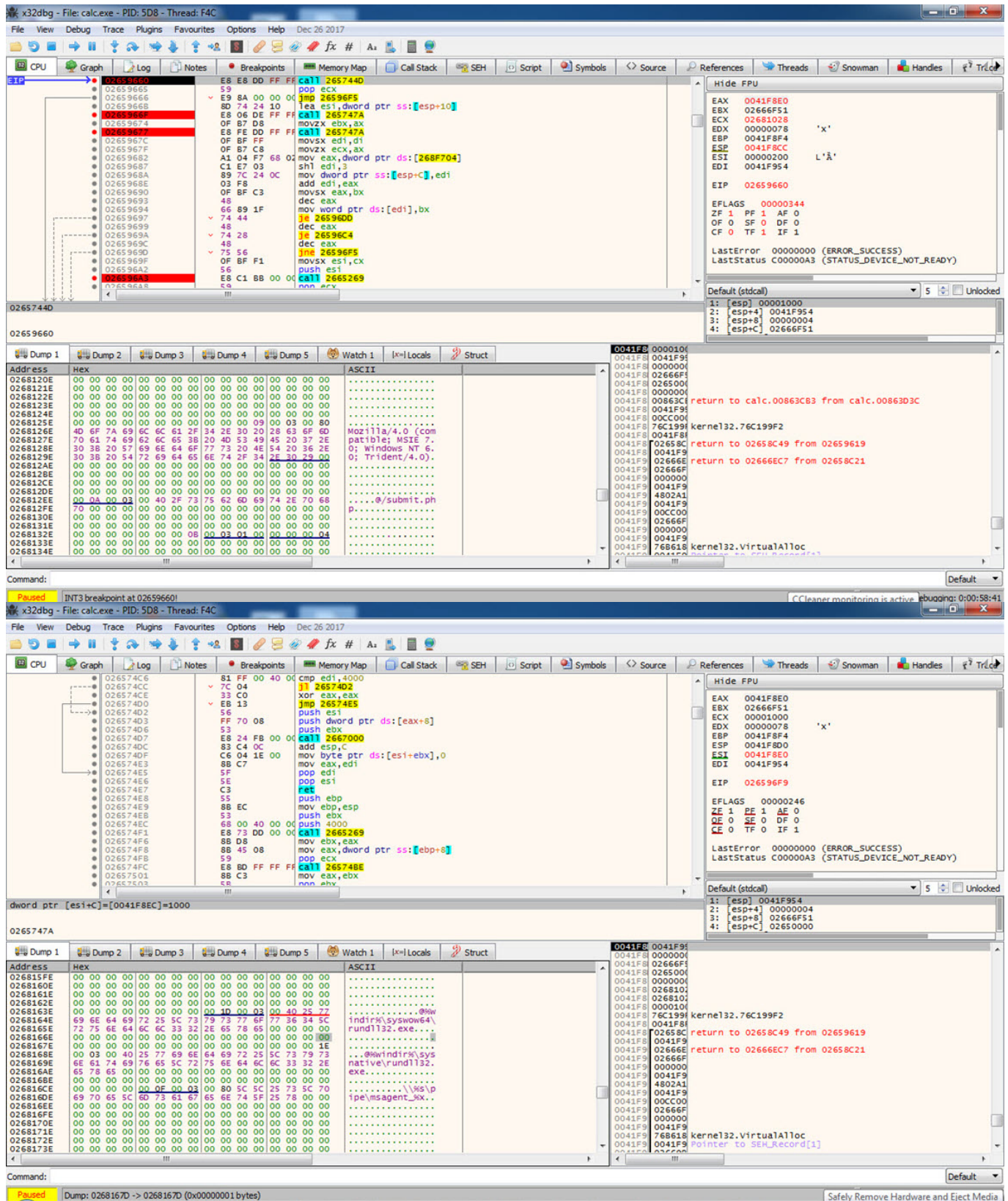
Dinamik sistem analizi esnasında Fiddler ile kayıt edilen HTTPS trafiğinde yer alan gizlenmiş Cookie bilgisine göre bu kabukkodunun Cobalt Strike aracına ait olduğu ihtimali güçlenir.

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.

The image displays two screenshots of the Hex Workshop application, showing the analysis of a DLL file (calc_02650000.bin) for strings.

Top Screenshot: The main window shows the hex editor with the file open. The 'Data Inspector' pane on the right displays the data at offset 0x0002D2A5, showing a series of integers (int8, uint8, int16, uint16, int32, uint32, int64) and their corresponding values. The 'Expression Calc' pane shows the value '1'.

Bottom Screenshot: The 'Structures' pane is open, displaying a list of 421 instances of strings found in the file. The list includes the address, length, and the string content. The strings are categorized into several groups, including 'could not adjust permissions in process: %d', 'could not create remote thread in %d: %d', 'could not open process %d: %d', '%d is an x64 process (can't inject x86 content)', '%d is an x86 pROcess (cAn't inject x64 content)', 'syswow64', 'system32', 'Could not set PPID to %d: %d', and 'Could not set PPID to %d'.



olmalarını öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

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