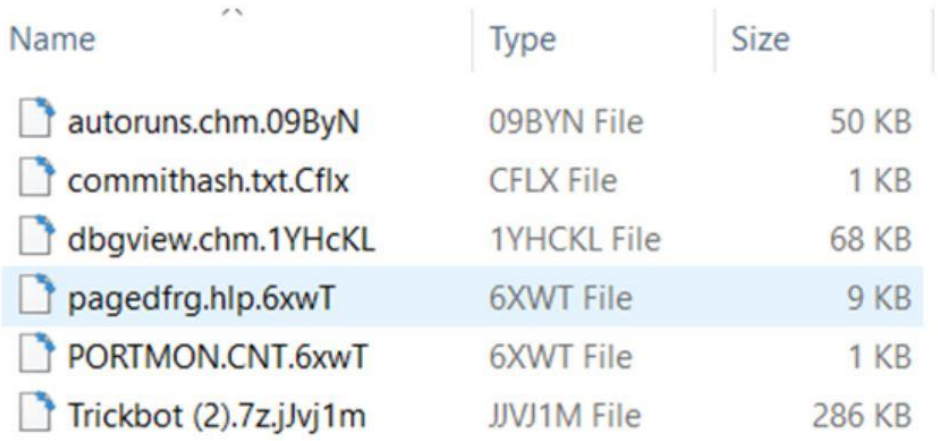
Maze Fidye Yazılımı

Bu yazımızda Comodo güvenlik araştırmacıları tarafından analiz işlemi gerçekleştirilen Maze fidye yazılımından bahsedeceğiz. Yazımıza başlamadan önce fidye yazılımları nedir, neler yapar kısa cevap verelim.

Fidye yazılımları kısaca hedef sistemdeki dosyaları güçlü bir şifreleme algoritması ile şifreler ve şifrelemenin çözülebilmesi için hedeften ücret talep eden zararlı yazılımlardır. Güçlü bir şifreleme kullanılması halinde verilerin şifresi çözülememektedir ve bu da yedekleme yapmayan şirketler için tehlikeli olabilmektedir. Bazı şirketler verilerini kurtarmak için saldırganlara ödeme yapabiliyor fakat verilerini geri alamayabiliyorlar, bazı şirketler ise verilerini kaybederek yollarına devam ediyor. Maze geliştiricileri ise fidye yazılım sektörüne bir yeni özelik ekleyerek hedef ödeme yapmadığı taktirde verilerini kamuya açıklıyor ve web sitelerinde ödeme yapmamış olan şirketlerin listelerini yayınlıyorlar. Hastaneler, finans kurumları vb. gibi kuruluşların verilerinin kamu ile paylaşılması, rakiplerine satılması, itibar kaybı veya doğrudan Kişisel Verilerin Korunması Kanunu kapsamında cezalandırılması gibi kritik durumlar söz konusu olabilmektedir. FBI Maze zararlı yazılımını büyük bir tehdit olarak gördü ve hakkında tüm şirketlere 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 şifrelemesi ile şifreliyor ve ardından verilerin şifresinin çözülebilmesi için ödeme talep etmektedir. Aşağıdaki ekran görüntüsü Maze fidye yazılımının şifreli dosyalara eklediği çeşitli dosya uzantılarını göstermektedir.



Fidye yazılımı sonrasında hedefin masaüstüne bir fidye mesajı oluşturuyor. Comodo güvenlik araştırmacılarına göre fidye yazılımının bağlantı gerçekleştirdiği ilk 5 sunucunun Rusya, Polonya, Türkiye, Hollanda ve Avusturya olduğu belirtildi.

Maze Fidye Yazılımının Anatomisi

Analiz üç bölümden oluşmaktadır:

1-) IP listesi, Web Uzantıları ve Şifrelenmiş Web Adresleri
2-) Dosya Şifreleme İşlemleri
3-) Şifre Çözme Notları ve Şifre Çözme Bağlantıları

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

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

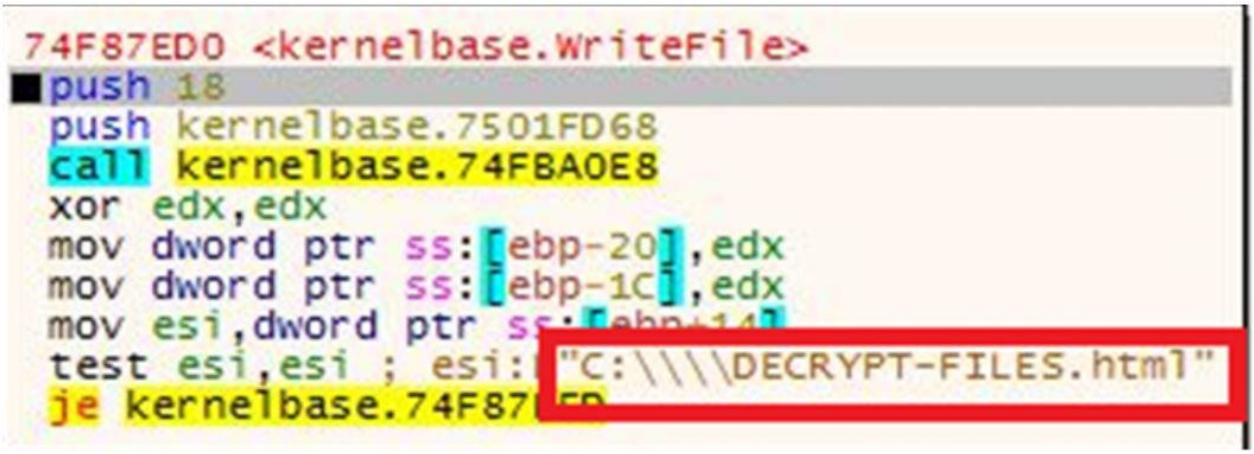
- 92.63.8.47
- 92.63.32.2
- 92.63.37.100
- 92.63.194.20
- 92.63.17.245
- 92.63.32.55
- 92.63.11.151
- 92.63.194.3
- 92.63.15.8
- 92.63.29.137
- 92.63.32.57
- 92.63.15.56
- 92.63.32.52
- 92.63.15.6

Ayrıca altı sabit web uzantısının kullanıldığı tespit edilmiştir.

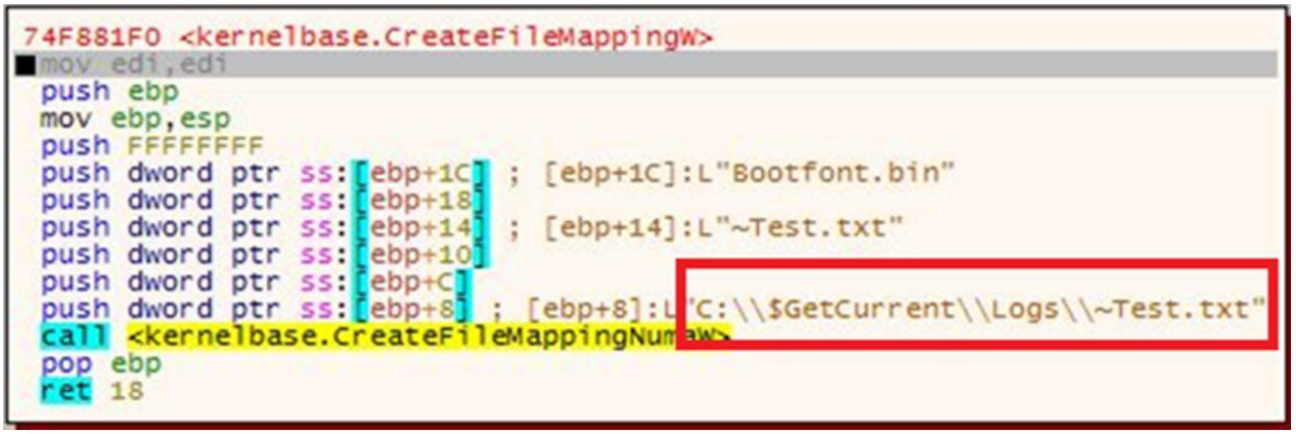
Maze aşağıdaki URL oluşumlarını kullanır (Post/Edit ve Siginin/Transfer)

2-) Dosya Şifreleme İşlemi

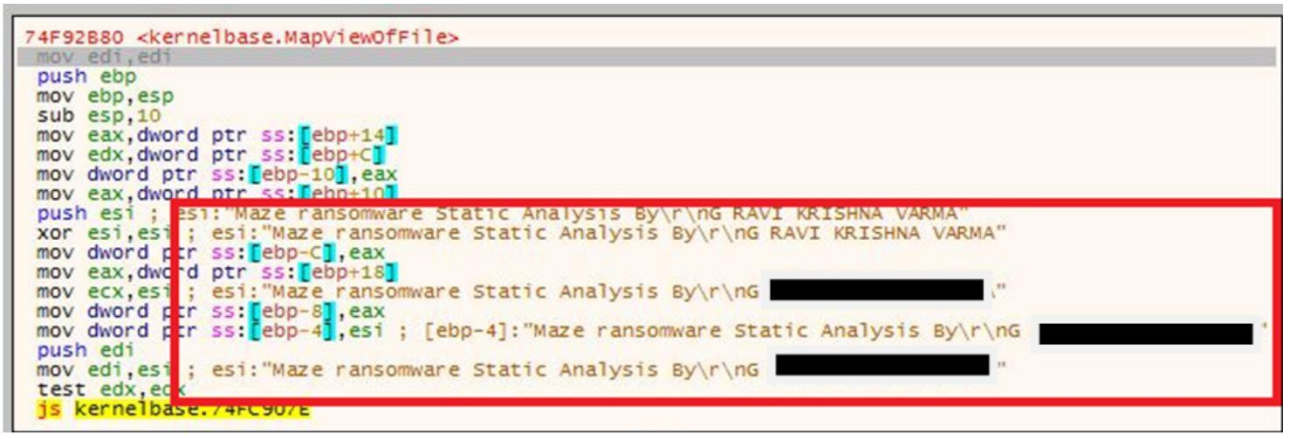
Maze, hedef makinenin sürücüsündeki tüm dosyaların/klasörlerin bir envanterini oluşturur ve bunları "**DECRYPT-FILES.html**" adlı bir dosyada listeler.



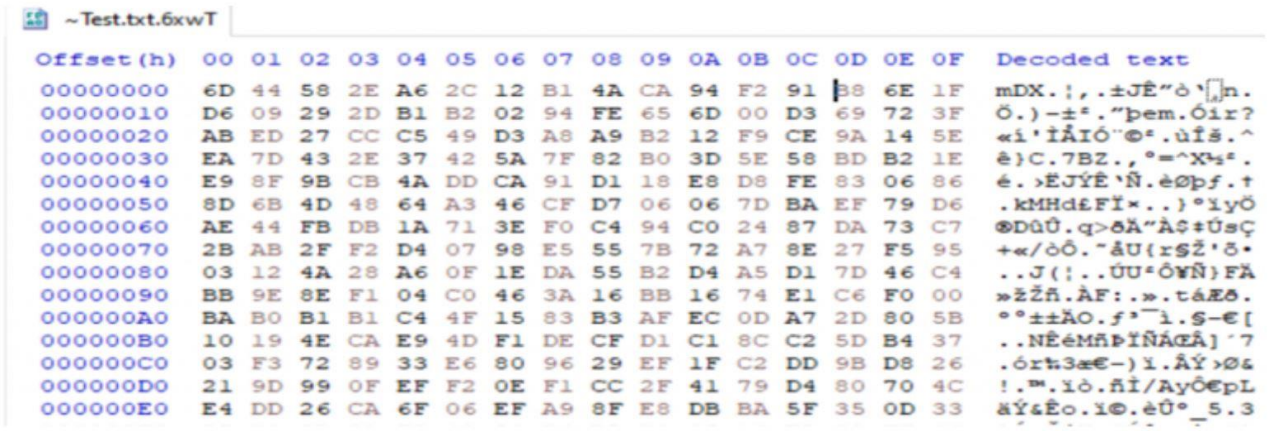
Comodo ekibi şifreleme işlemini anlayabilmek için test.txt dosyası oluşturarak test işlemi gerçekleştirdi. Fidye yazılımı Test.txt dosyasını şifrelerken CreateFileW, ReadFile, CreateFileMappingW ve MapViewOfFile API'lerini çağırdığı tespit edildi.



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



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.¦,.±JÊ"ò'¸n.
00000010	D6	09	29	2D	B1	B2	02	94	FE	65	6D	00	D3	69	72	3F	Ö.)-±².”þem.Óir?
00000020	AB	ED	27	CC	C5	49	D3	A8	A9	B2	12	F9	CE	9A	14	5E	«í'ÌÅIÓ¨©².ùÎš.^
00000030	EA	7D	43	2E	37	42	5A	7F	82	B0	3D	5E	58	BD	B2	1E	ê}C.7BZ.‚°=^X½²..
00000040	E9	8F	9B	CB	4A	DD	CA	91	D1	18	E8	D8	FE	83	06	86	é.›ËJÝÊ'Ñ.èØþƒ.†
00000050	8D	6B	4D	48	64	A3	46	CF	D7	06	06	7D	BA	EF	79	D6	.kMHd£FÏ×..}ºïyÖ
00000060	AE	44	FB	DB	1A	71	3E	F0	C4	94	C0	24	87	DA	73	C7	®DûÛ.q>ðÄ”À$‡ÚsÇ
00000070	2B	AB	2F	F2	D4	07	98	E5	55	7B	72	A7	8E	27	F5	95	+«/òÔ.˜åU{r§Ž'õ•
00000080	03	12	4A	28	A6	0F	1E	DA	55	B2	D4	A5	D1	7D	46	C4	..J(¦..ÚU²Ô¥Ñ}FÄ
00000090	BB	9E	8E	F1	04	C0	46	3A	16	BB	16	74	E1	C6	F0	00	»žŽñ.ÀF:.».táÆð.
000000A0	BA	B0	B1	B1	C4	4F	15	83	B3	AF	EC	0D	A7	2D	80	5B	º°±±ÄO.ƒ³¯ì.§-€[
000000B0	10	19	4E	CA	E9	4D	F1	DE	CF	D1	C1	8C	C2	5D	B4	37	..NÊéMñÞÏÑÁŒÂ]´7
000000C0	03	F3	72	89	33	E6	80	96	29	EF	1F	C2	DD	9B	D8	26	.ór‰3æ€–)ï.ÂÝ›Ø&
000000D0	21	9D	99	0F	EF	F2	0E	F1	CC	2F	41	79	D4	80	70	4C	!.™.ïò.ñÌ/AyÔ€pL
000000E0	E4	DD	26	CA	6F	06	EF	A9	8F	E8	DB	BA	5F	35	0D	33	äÝ&Êo.ï©.èÛº_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.

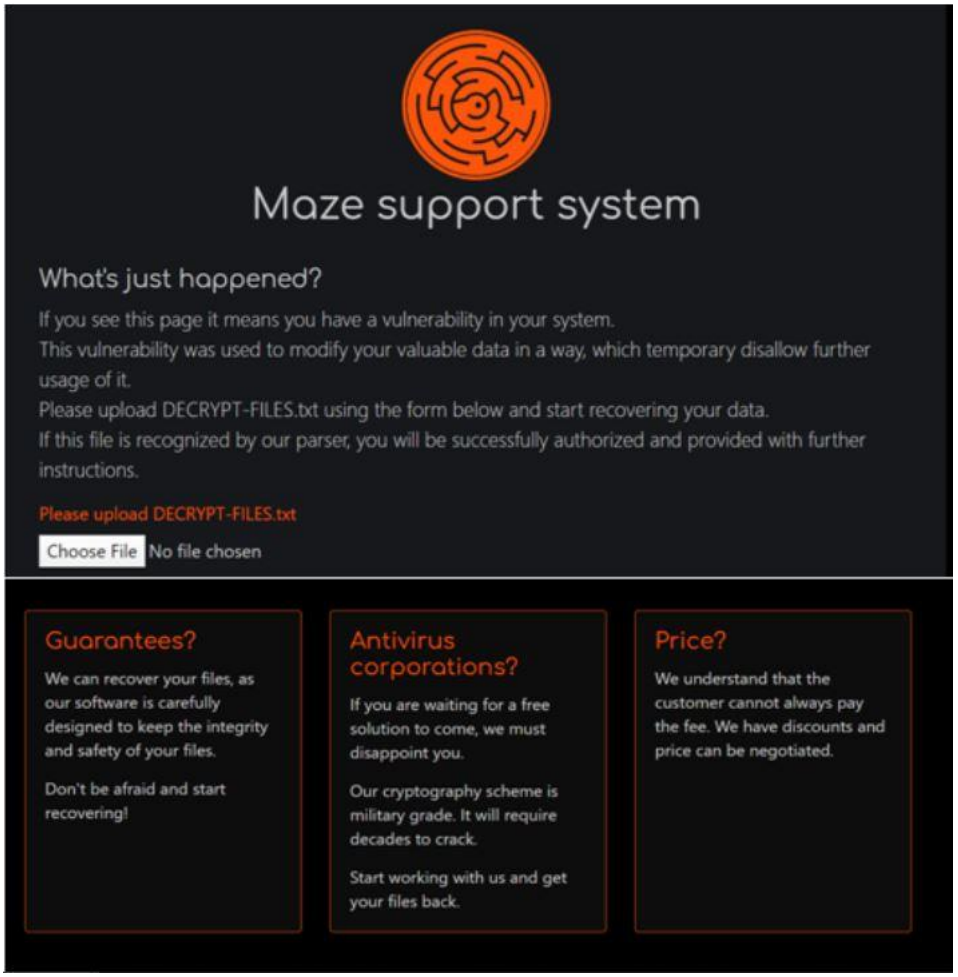
Ekteki not ise durumun ciddiyetini yinelemekte ve ödeme yapmak için saldırganlar ile nasıl iletişime geçileceği konusunda ayrıntılı talimatlar içermektedir.

DECRYPT-FILES.txt - Notepad

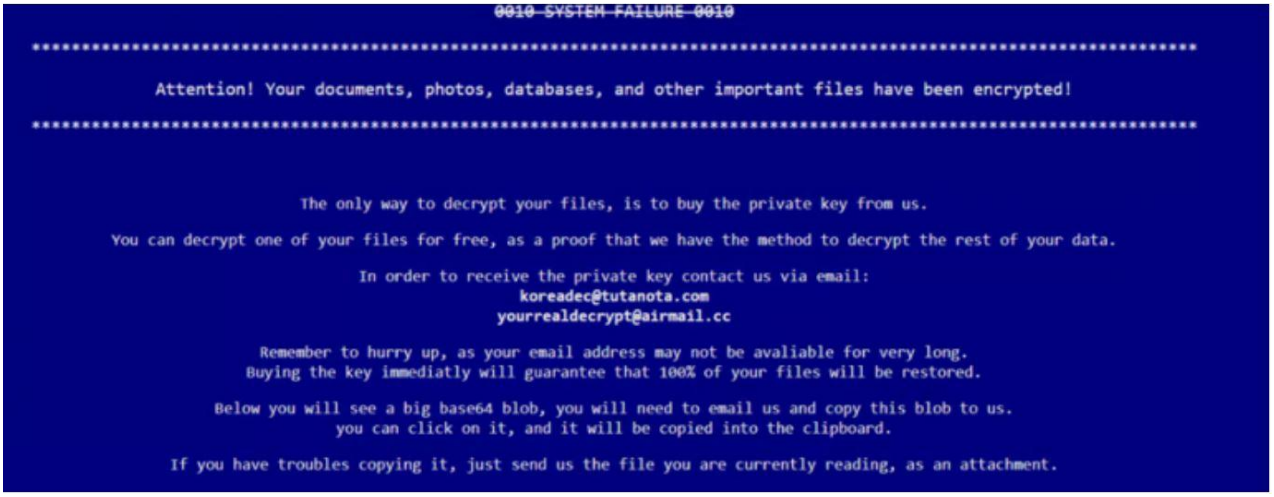
File Edit Format View Help

```
Attention!

------------------------------
| 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.

  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR Browser.
  c) Open the TOR Browser.
  d) Open our website in the TOR browser: http://aoacugmutagkwctu.onion/1b010b7e5a3ebe7d
  e) Follow the instructions on this page.

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

  a) Open our website: https://mazedecrypt.top/1b010b7e5a3ebe7d
  b) 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---
grMgC/YT9ozlrnIG7dsLiboGmXY017niDCDdk78qcN+Ooap+cad6X4WTCg6rEFE6Nshu6+IPutsN30KBPZK8MoNyxjV0+UzeFvdUsJfcH+GNyEWM0iZfO2mb102tQ83K9zukpCj/uAa5wNQv+jMgN3b6GAHupdi/u9MM7AxOyeQsMxGEIH3wTxLc191i
PZ+YINIO28QP78jk+hL6L5OSeyPHXSgfZq1YnX0H6wr2/IPK3mOcRcIOtdJjrilf0fmRt6HeddSCobeanrw1z28z14woyK+p2jZrGM/I1fz7oLUx9PW5zejlIhHxsoQJu0Sulo9HEcTLUz1apJkqEg/NgdIl7p7RaE7yWfky/Ll9rvqTmjERQIXhylBy3
8ZsJhPC0dOhAGYAOvtf1f3umyUpP//fNvzC7jX8dnFqetGsgRAAjGGnIQ1JDd7QWCkB3rbNxP7IOhyHDVNmLMw/vRyYb6Ta8kTe1/DymXgYrACQd2TcIm6DEivGuiOBWRVNQ4s9sKajqMtX3TWGSBvs5jxvDK6LSh92ZWPnMiBKoccv0glJkcB7qWIMvA
---END MAZE KEY---
```

Nottaki ikinci seçenek ise kullanıcıyı hxxp://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.



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 verilmeyedebilir. 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/