Zararlı yazılım bilgileri

Dosya adı	d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2afd66.exe
Dosya boyutu	205.50 KB
Dosya türü	PE32/EXE
MD5	baa9e1a92bab85279dca0aed641f1fa9
SHA1	e26721107dce1355b8ecc71b457543b25ceab823
SHA256	d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2afd66
Botnet	f624ecb4a0335cf66bf78da0cad7ec5c
Paketleyici/Derleyici Bilgisi	Microsoft Visual C/C++(2010)
Derlenme zamanı	2024-04-05 16:00:03

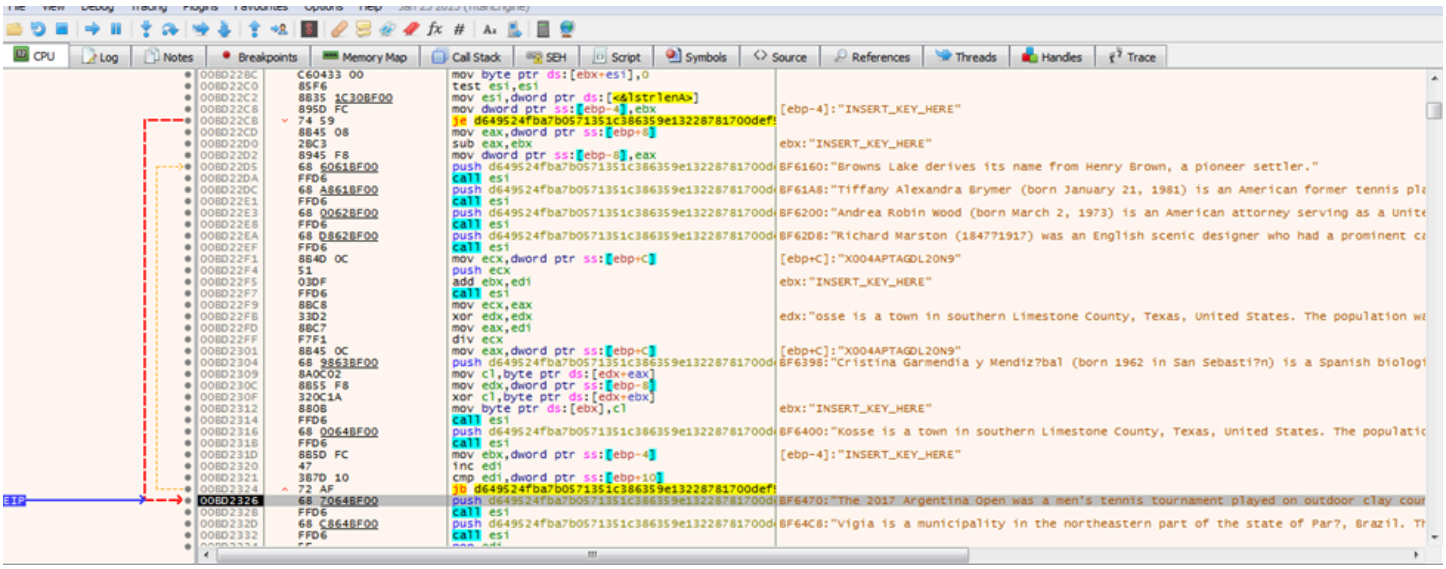
Zararlı yazılım gereklilikleri

Zararlı yazılımın hedef aldığı işletim sistemi:

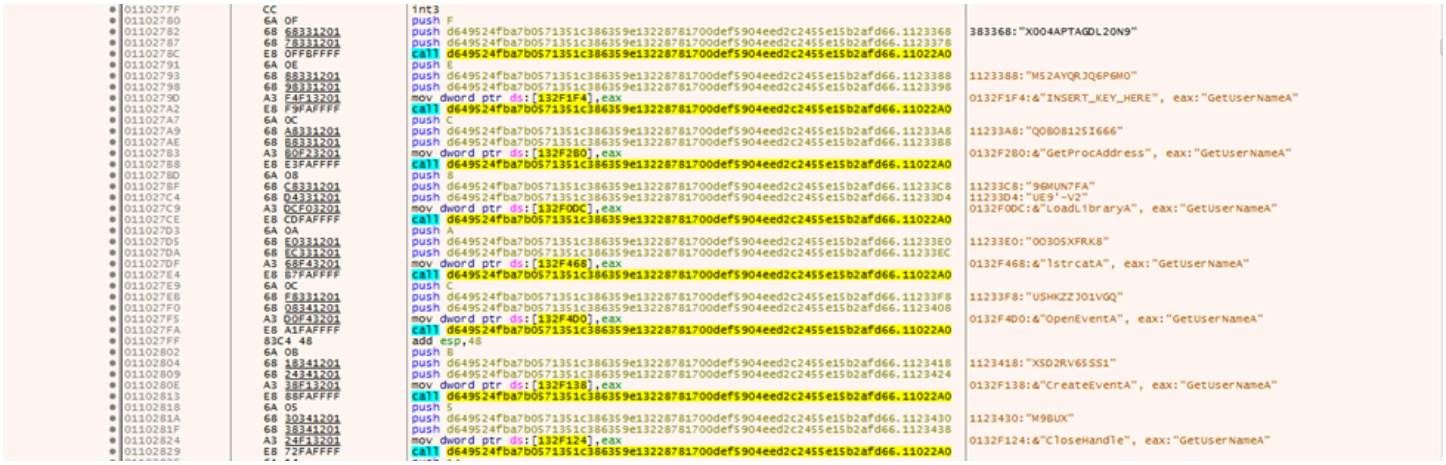
- Windows 10 ve üzeri. Zararlı yazılım Windows 7 makinelerde çalışmamakta.

Kullanıcı adının “JohnDoe” kullanıcı adından farklı olması gerekmekte:

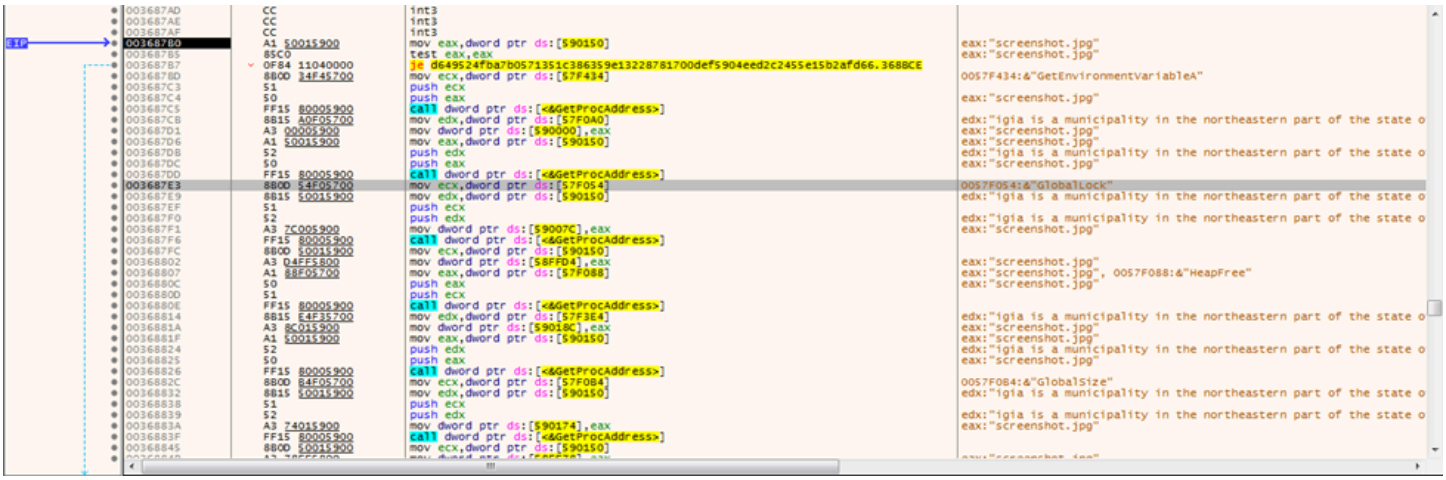
Ek Bilgiler/ Analist Notları



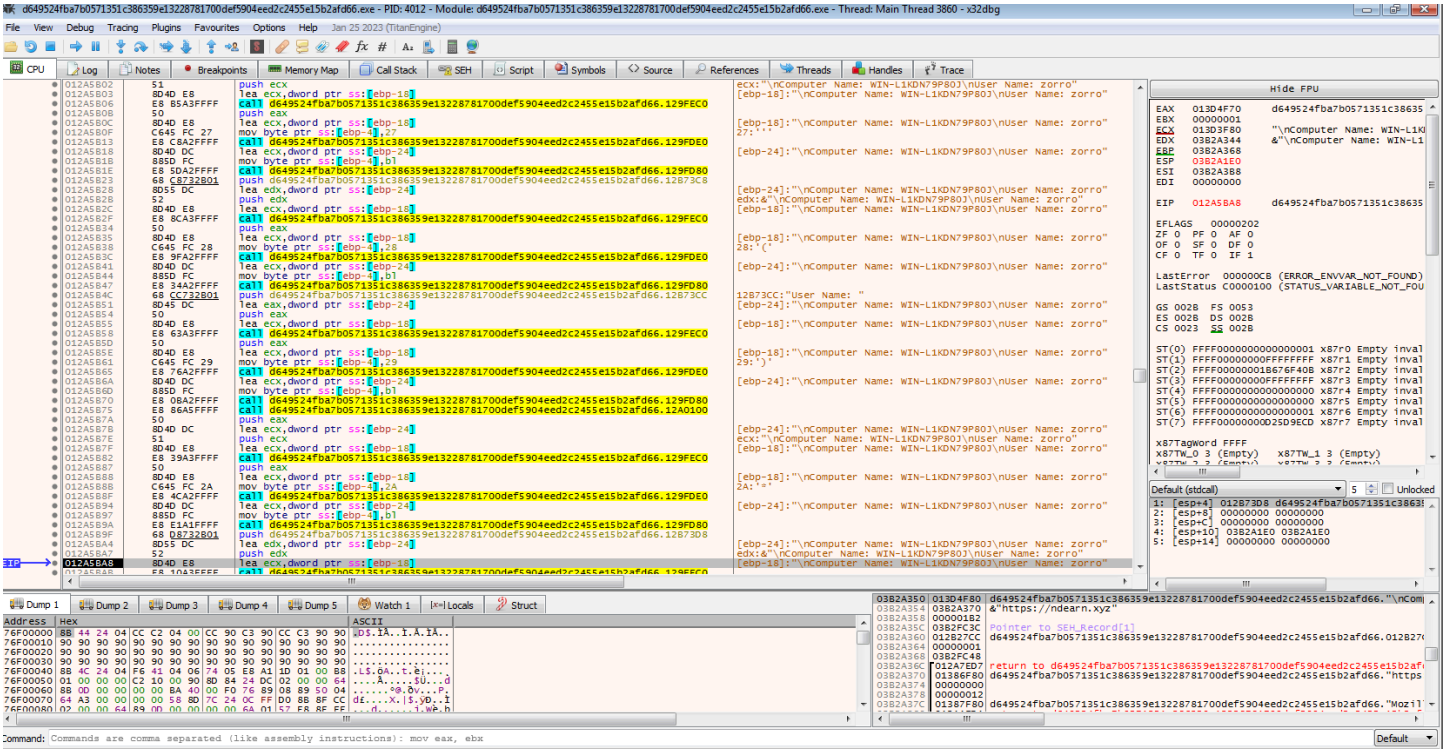
Stringler üzerinde gördüğümüz şifreli textlerin dinamikte çözüldüğünü görüyoruz. Stringlerin Windows API'ları çözdüğü gözlemlenmiştir.



Farklı bir algortima ile dynamic resolving işlemi yapılmaktadır.

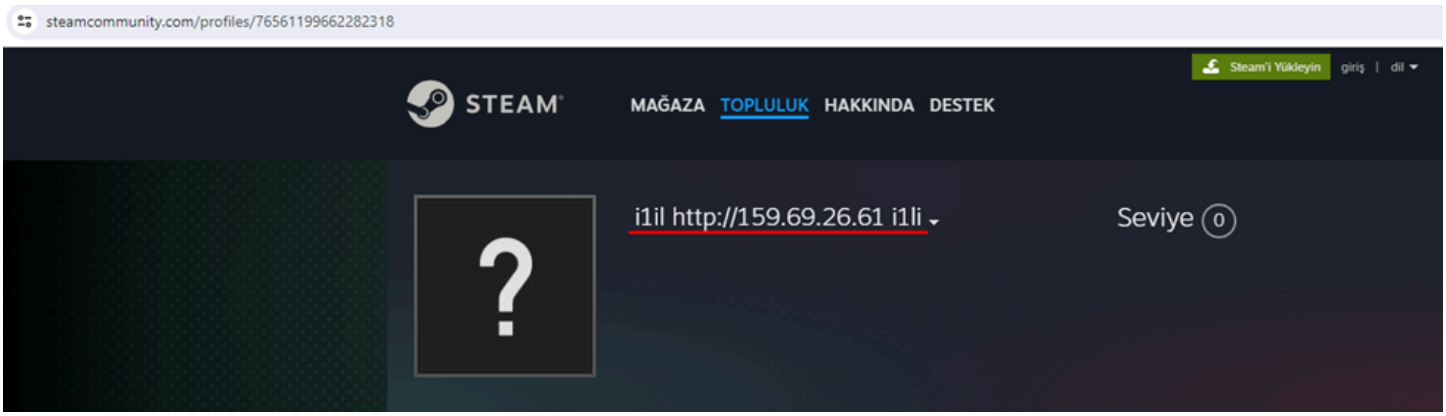


GetProcAddress ile Dynamic resolving işlemi yapılmaktadır. API'ler çözümleniyor.



Sistem bilgilerini çeken birçok fonksiyon mevcuttur. Sadece bilgisayar ve kullanıcı adını gösteren ekran görüntüsü iletilmiştir.

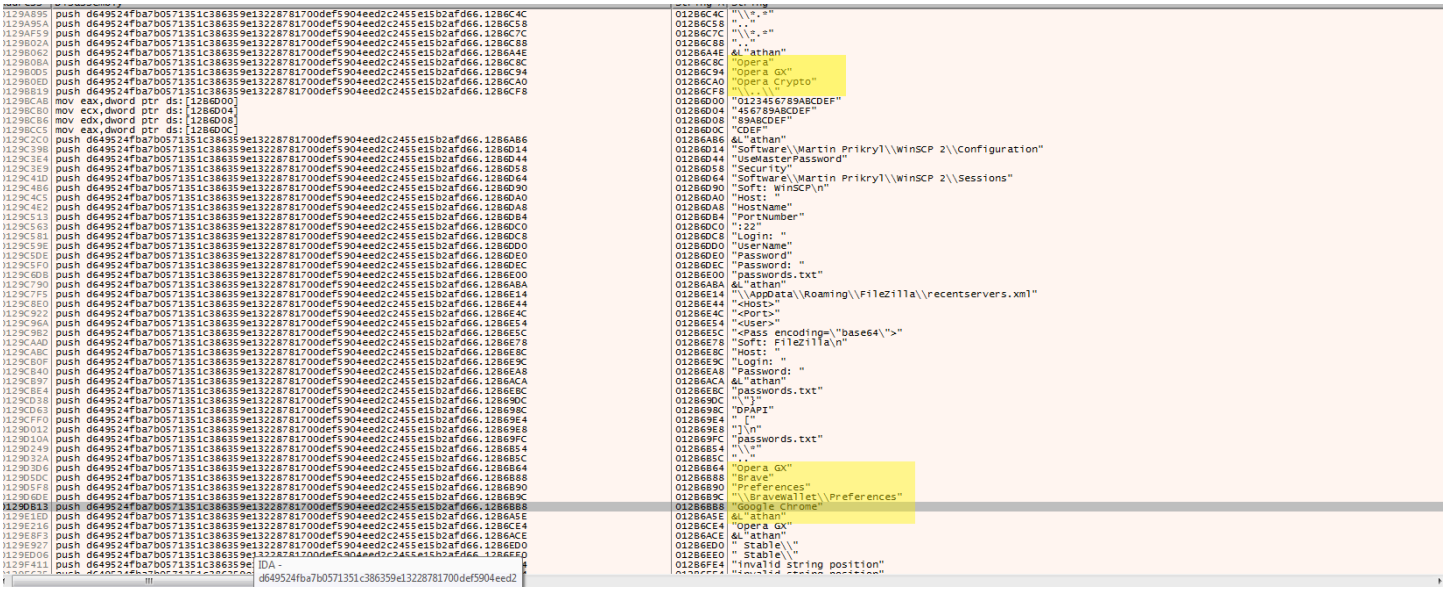
Ndearn.xyz'ye istek atacak fakat Internet açık olmadığından KiUserExceptionDispatcher yakalıyor ve hata veriyor. O sebeple isteğin gideceği alanı nope'luyorum.



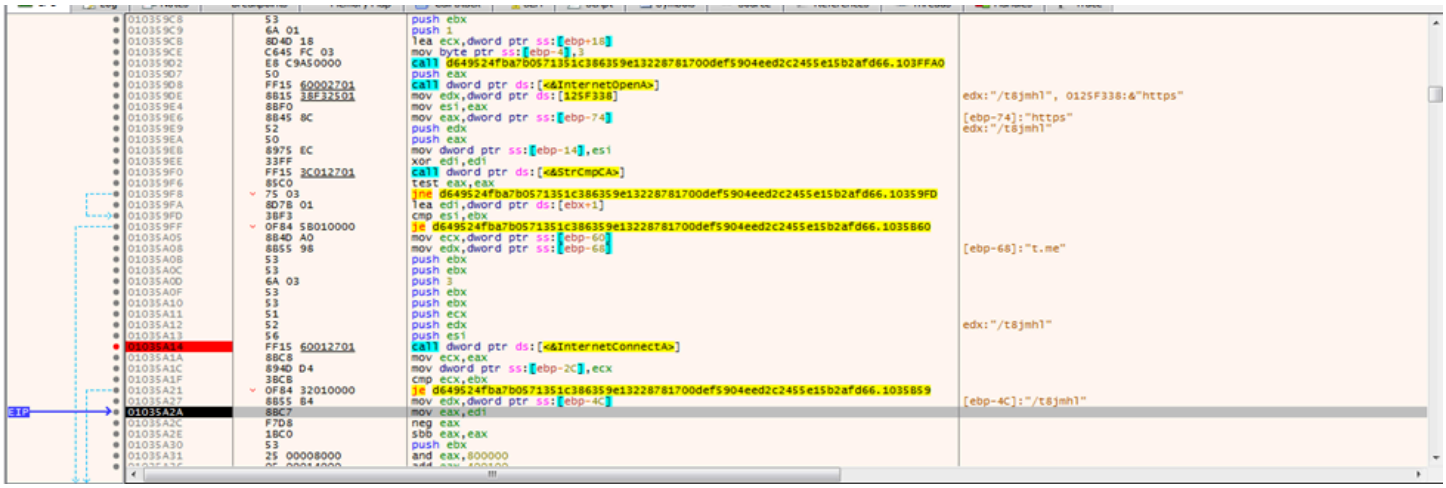
https://steamcommunity.com/profiles/76561199662282318 profilinde isim alanı i1il http://159.69.26.61 i1li şeklinde eklenmiştir. Dinamik analizde i1li alanları ayrıştırdığı gözlemlenmiştir. (Kırmızı ile vurgulanmıştır.)

```
.rdata:0114E91D 00 00 00                    align 10h
.rdata:0114E920 68 74 74 70 73 3A 2F 2F 73 74+aHttpsSteamcomm db 'https://steamcommunity.com/profiles/76561199662282318',0
.rdata:0114E920 65 61 6D 63 6F 6D 6D 75 6E 69+                              ; DATA XREF: sub_112A790+8↑o
.rdata:0114E956 00 00                       align 4
.rdata:0114E958 69 31 69 6C 00              aI1il db 'i1il',0               ; DATA XREF: sub_112A7C0+8↑o
.rdata:0114E95D 00 00 00                    align 10h
.rdata:0114E960 4D 6F 7A 69 6C 6C 61 2F 35 2E+aMozilla50Macin db 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1'
.rdata:0114E960 30 20 28 4D 61 63 69 6E 74 6F+                              ; DATA XREF: sub_112A7F0+8↑o
.rdata:0114E960 73 68 3B 20 49 6E 74 65 6C 20+db '22.0.0.0 Safari/537.36 OPR/108.0.0.0',0
.rdata:0114E9E4 68 74 74 70 73 3A 2F 2F 74 2E+aHttpsTMeT8jmhl db 'https://t.me/t8jmhl',0
.rdata:0114E9E4 6D 65 2F 74 38 6A 6D 68 6C 00                               ; DATA XREF: sub_112A820+8↑o
.rdata:0114E9F8 69 31 69 6C 00              aI1il_0 db 'i1il',0             ; DATA XREF: sub_112A850+8↑o
.rdata:0114E9FD 00 00 00                    align 10h
.rdata:0114EA00 4D 6F 7A 69 6C 6C 61 2F 35 2E+aMozilla50Macin_0 db 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1'
.rdata:0114EA00 30 20 28 4D 61 63 69 6E 74 6F+                              ; DATA XREF: sub_112A880+8↑o
.rdata:0114EA00 73 68 3B 20 49 6E 74 65 6C 20+db '22.0.0.0 Safari/537.36 OPR/108.0.0.0',0
.rdata:0114EA84 68 74 74 70 73 3A 2F 2F 73 74+aHttpsSteamcomm_0 db 'https://steamcommunity.com/profiles/76561199662282318',0
```

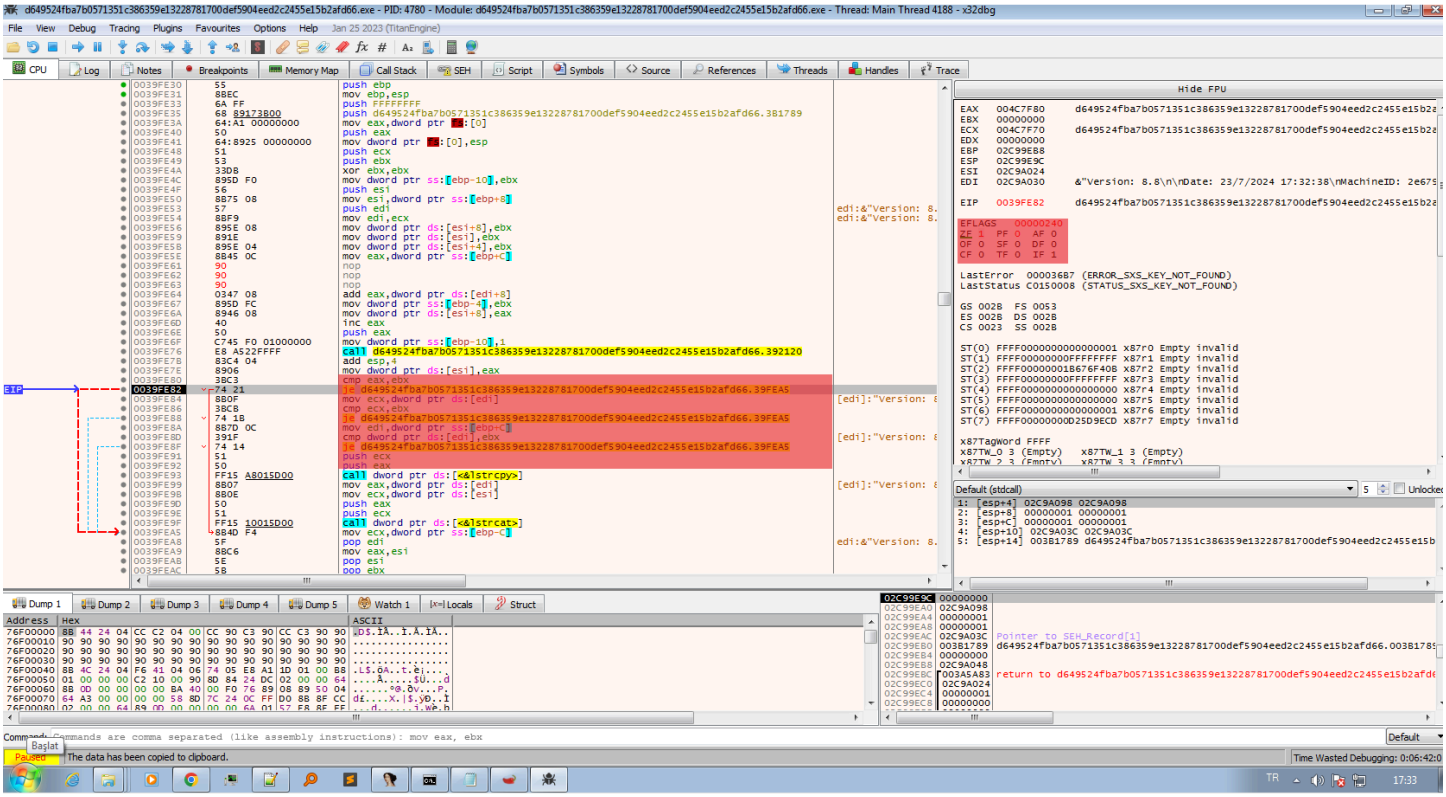
User Agent bilgileri de uygulamada depolanmaktadır.



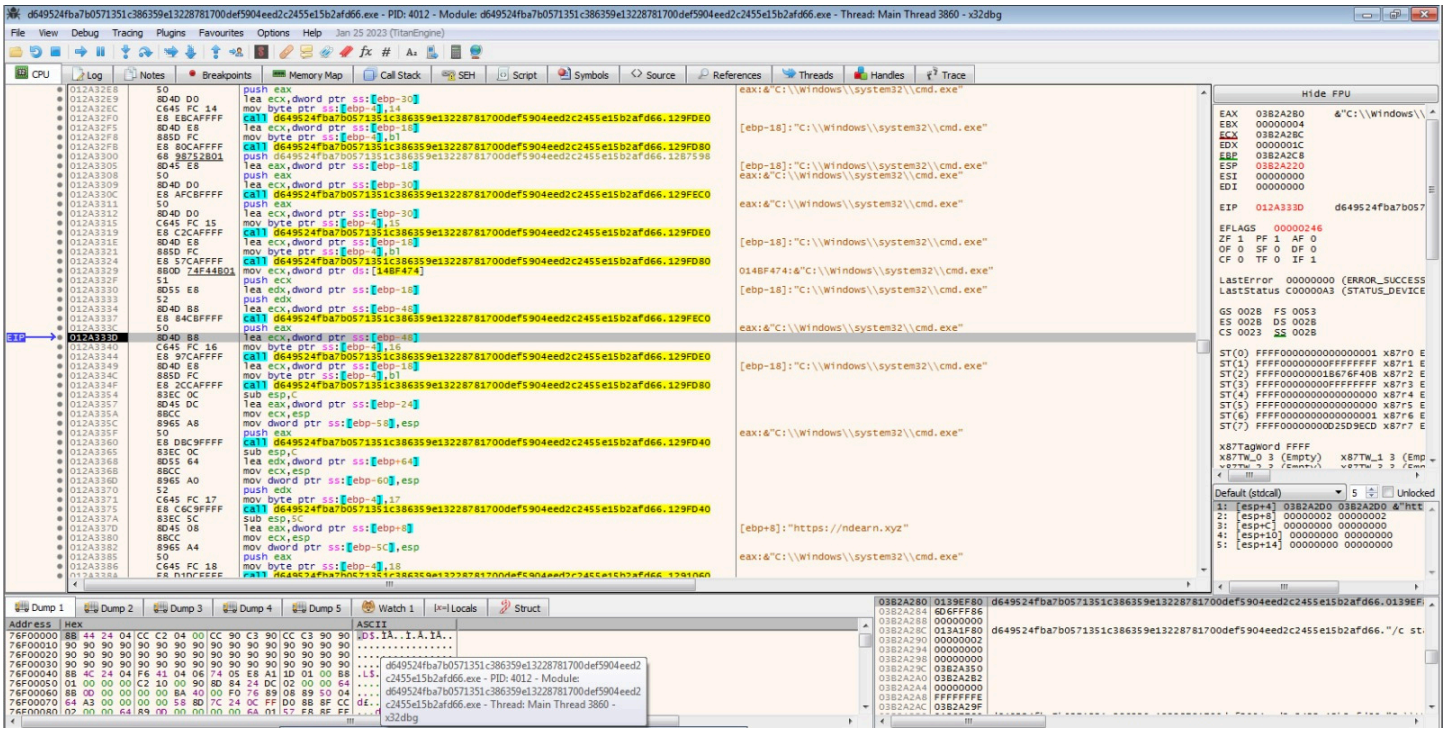
Farklı tarayıcıların vallet bilgileri de uygulama tarafından alınmaktadır.



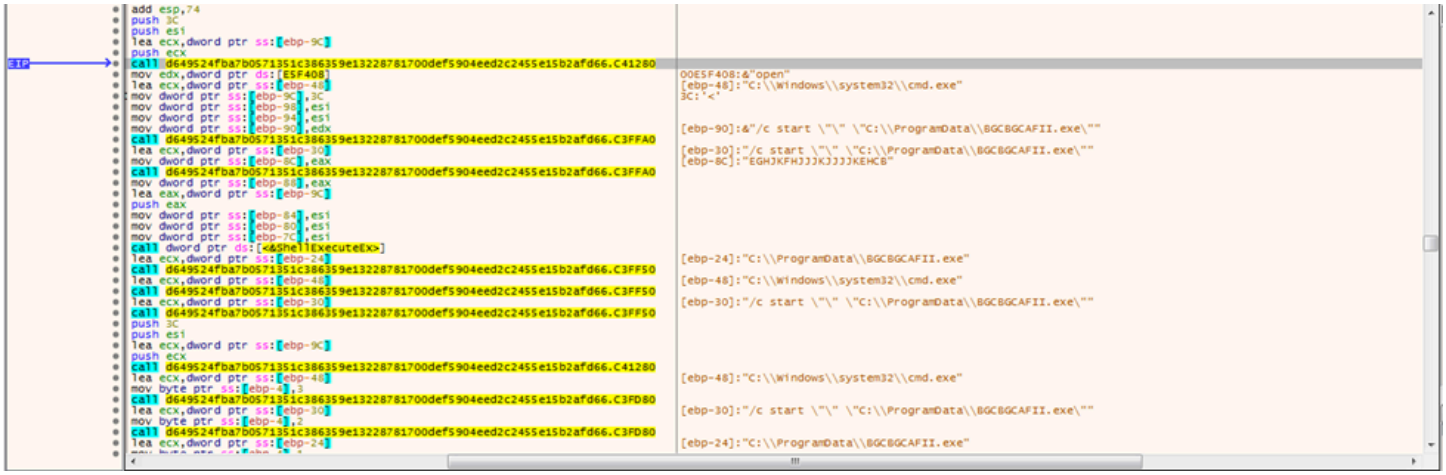
Ek olarak “https://t.me/t8jmh1” adresine istek gitmektedir.



vurgulanan kısımda tarih kontrolü yapıyor. Zero flagi 1 yaparak kontrolden kurtulduk.



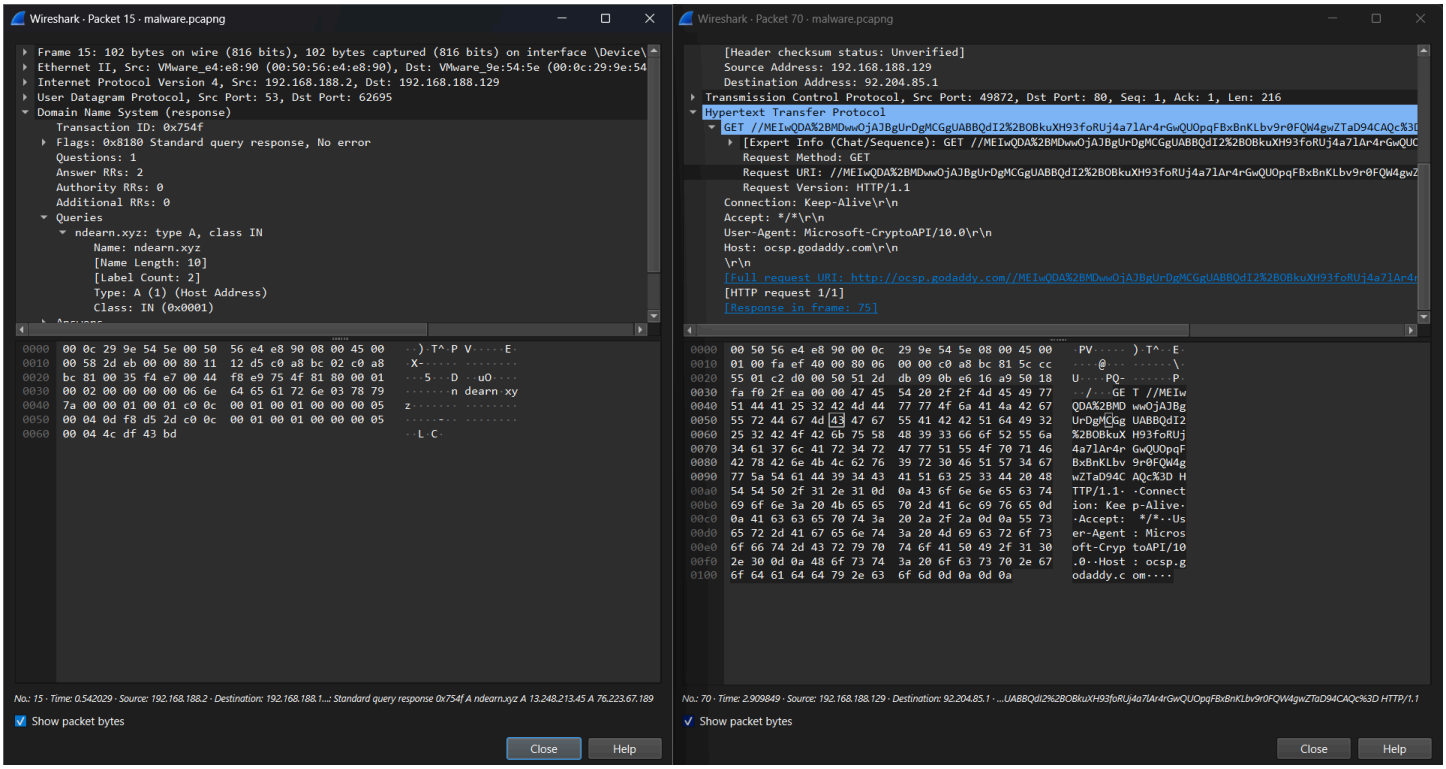
Uygulamanın komut istemini de açtığı görülmüştür ancak kullandığına dair bir bulgu bulunamamıştır.



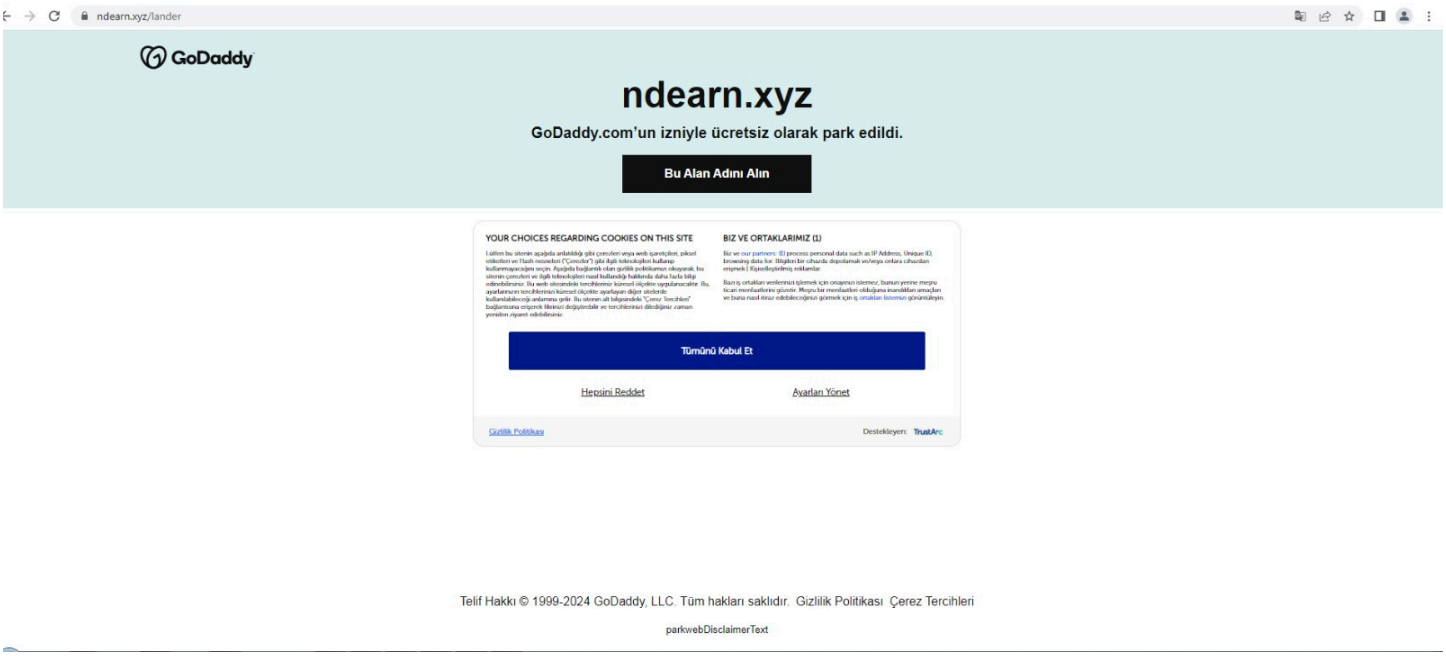
Zararlı her çalıştığında farklı isimlerde .exe oluşturmaktadır.

BGCBGCAFII.exe	23.07.2024 14:59	Uygulama	0 KB
CAFBGDHCBA.exe	23.07.2024 15:04	Uygulama	0 KB
CBKJEGCBKK.exe	23.07.2024 15:05	Uygulama	0 KB
DGDBAKKJKK.exe	23.07.2024 15:05	Uygulama	0 KB
DGIJEGHDAE.exe	23.07.2024 14:43	Uygulama	0 KB
EGIDBFBFHJ.exe	23.07.2024 14:46	Uygulama	0 KB
KJJJKFIIIJ.exe	23.07.2024 14:41	Uygulama	0 KB
KJKJJEGIDB.exe	23.07.2024 14:54	Uygulama	0 KB

Oluşturduğu exe'nin içerisinde bir veri yazamamaktadır. Bağlantı sağlayarak indirmesi gerekiyor fakat şu an sunucu aktif olmadığında zararlının ek dosyası oluşmamaktadır. Triage üzerinde PCAP dosyası da C2 sunucu kapalı olduğu zamana ait olduğundan oradan da yeterli bilgi elde edilememiştir. Ek olarak sandboxlar kontrol edilmiş olup, ilgili ek dosya bulunamamıştır.



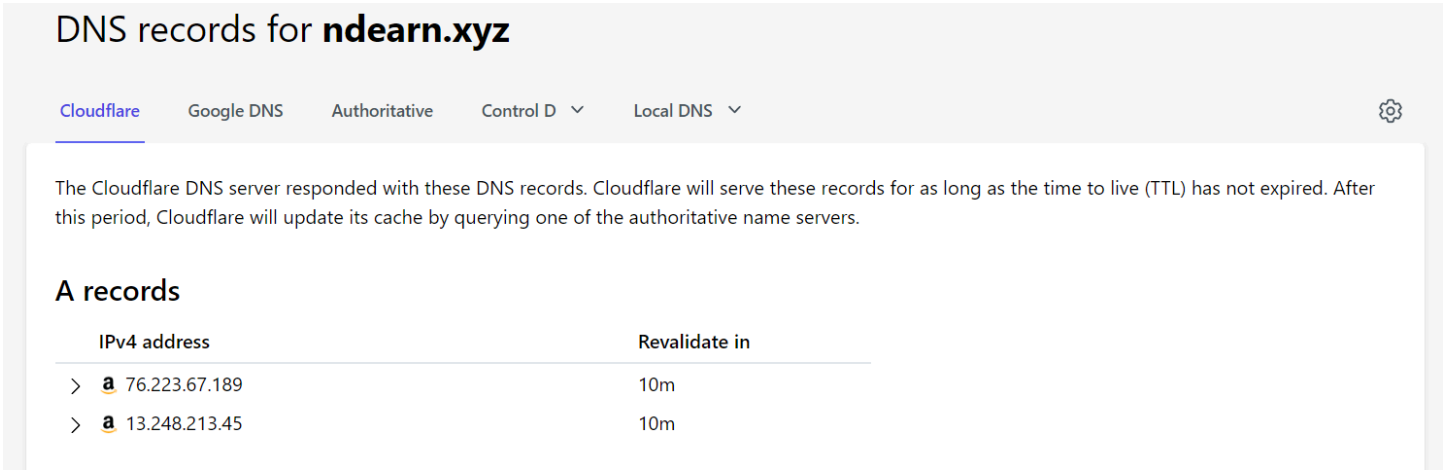
Zararlı yazılım çalıştırıldığında ndearn.xyz'ye erişiyor. Ayrıca görselde yer alan 70. pakette GET metoduyla beraber ocsp.godaddy.com'da //MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABBQdI2%2BOBkuXH93foRUj4a7lAr4rGwQUOpqFBxBnKLbv9r0FQW4gwZTaD94CAQc%3D adlı URI'a istek gönderiliyor. Ne yazık ki domain analizimiz sırasında satılığa çıkmıştı. Bu nedenle belirtilen durum söz konusu.

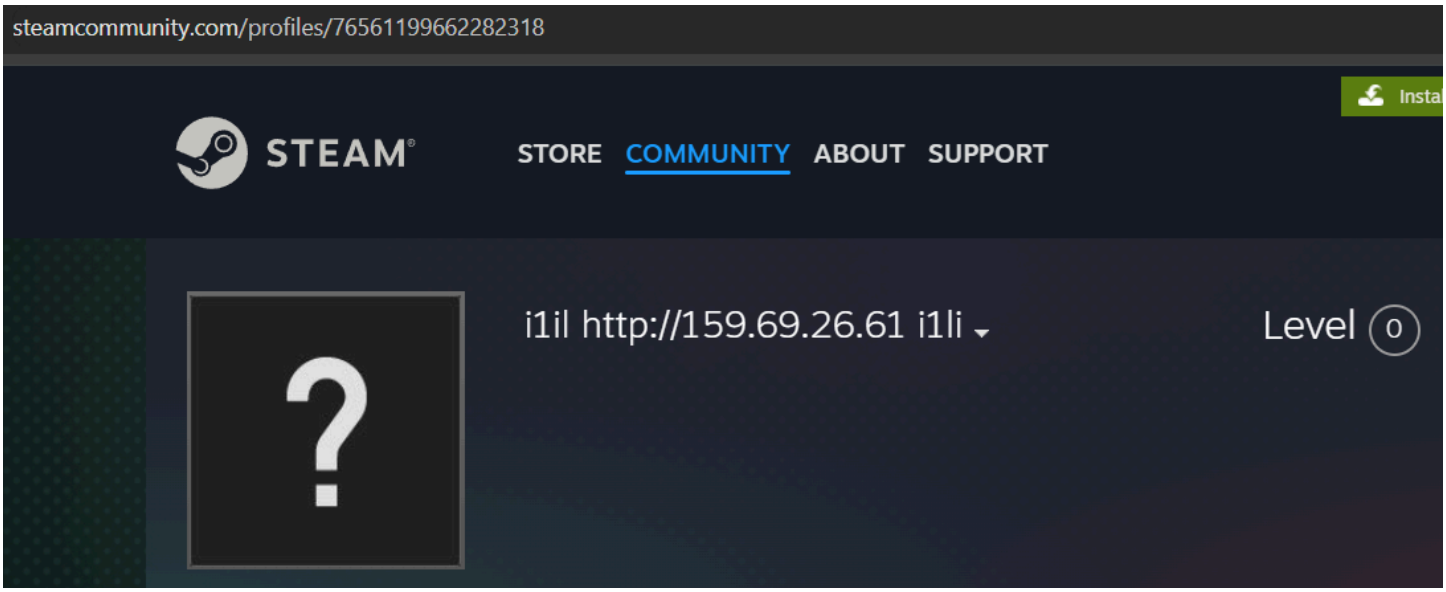


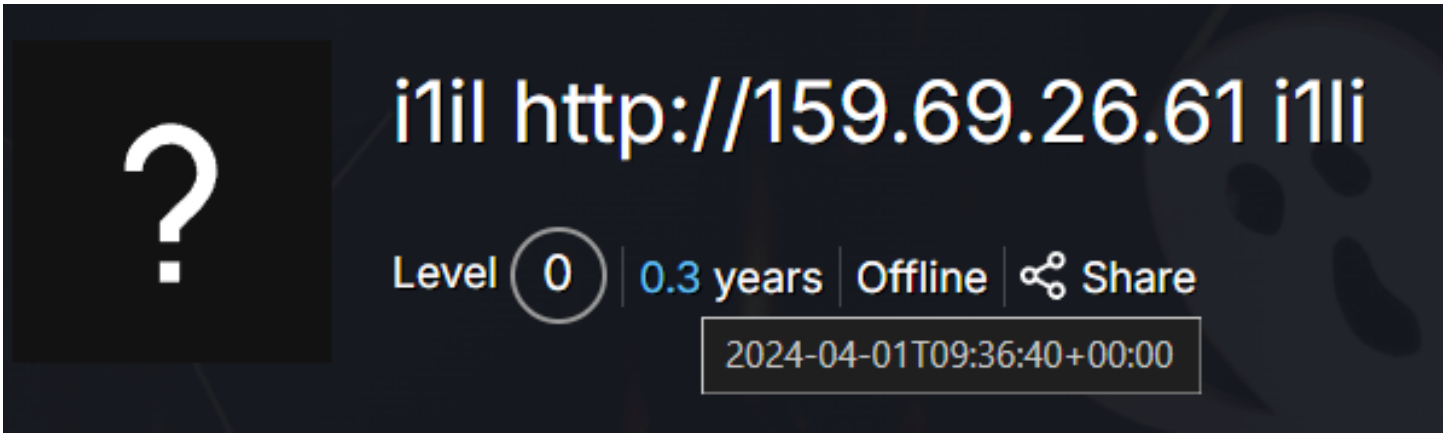
Satılığa çıkarıldığına dair ekran görüntüsü.

IOC'ler

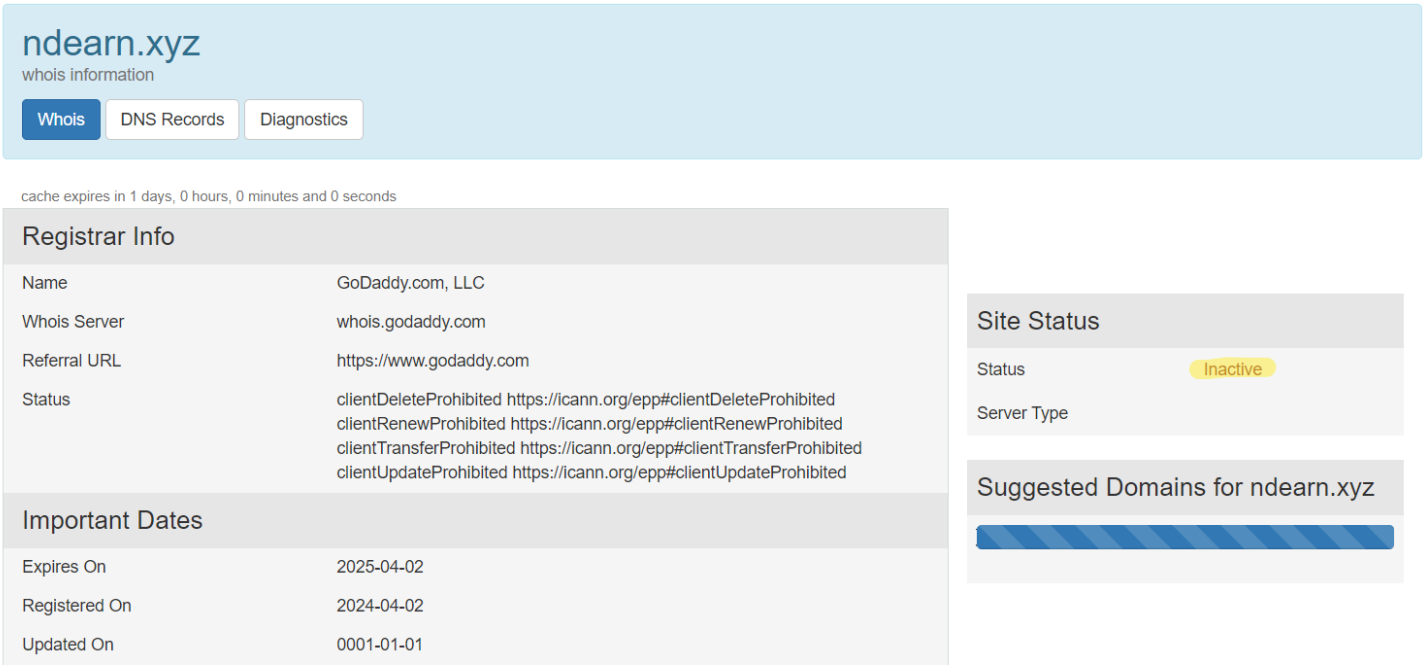
- https://ndearn.xyz
- https:/steamcommunity.com/profiles/76561199662282318
- https:/t.me/t8jmhl







Görüldüğü üzere Steam hesabı 1 Nisan 2024 tarihinde oluşturulmuş.



Ayrıca site durumu inaktif görünmekte. Ek olarak Wayback Machine vb. geçmişe dönük herhangi bir site içeriği tespit edilemediğinden zararlının analizini bitirmek durumunda kalındı.

Yara Kuralı

```
import "pe"
import "hash"
rule vidar_stealer
{
  meta:
  author = "takım8"
  description = "vidar stealer için yara kuralı"
  file_name =
"d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2afd66.exe"

  strings:
  $mz = "MZ"

  $str1 = "X004APTAGDL20N9"
  $str2 = "SLWLVJLOZZGXL9FT3J17"
  $str3 = "passwords.txt"
  $str4 = "65 79 41 69 64 48 6C 77 49 6A 6F 67 49 6B 70 58 56 43 49 73 49 43 4A
68 62 47 63 69 4F 69 41 69 52 57 52 45 55 30 45 69 49 48 30"

  $sql1 = "SELECT target_path, tab_url from downloads"
  $sql2 = "SELECT service, encrypted_token FROM token_service"

  condition:
    filesize<=1MB and hash.md5(0,filesize)=="baa9e1a92bab85279dca0aed641f1fa9"
and all of them and $mz at 0
}
```