

e-Devlet Hesaplarımızı Nasıl Hackliyorlar?

written by Mert SARICA | 1 December 2023

If you are looking for an English version of this article, please visit [here](#).

İÇİNDEKİLER

1. Başlangıç
2. Hedef Kim?
3. Teknik Araştırma
 1. IP Adresi Tespiti
 2. IP Sahiplik Bilgileri
 3. Bağlantı Noktaları
 4. IPv6'dan IPv4'e Yolculuk
 5. Tehdit Araştırması
 6. Yeni Bağlantı Noktaları
 7. Neden IPv6 adresi kullanıyorlar?
4. e-Devlet Hesabımı Nasıl Koruyabilirim?

Başlangıç

25 Ekim 2023 günü saat 11:46'da e-Devlet uygulamasından ve e-posta adresime gelen uyarılardan e-Devlet Kapısı hesabıma üst üste birden fazla defa yanlış parola ile giriş yapılmaya çalışıldığı için hesabımın bir saatliğine geçici olarak kullanıma kapatıldığını öğrendim.



Üst üste başarısız giriş denemesi yaptığınız için şifreniz geçici olarak kullanıma kapatılmıştır.

25/10/2023 19:46:22 tarihi itibarıyla şifreniz otomatik olarak yeniden kullanıma açılacaktır.

e-Devlet Şifresi

Şifremi Unuttum

Giriş Yap

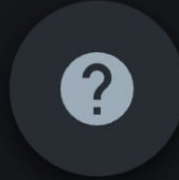
Mobil İmza ile Giriş Yap



Mobil Onay



Karekod Okut



YARDIM

HIZLI ERİŞİM



Hava Durumu



Nöbetçi Eczane
Sorgulama



Acil Toplanma
Alanları



TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ



Art niyetli bir kişinin uzun ve karmaşık olan parolamı tahmin etme ihtimalinin oldukça zayıf olması ve ayrıca e-Devlet Kapısı'nda da iki aşamalı giriş yöntemini kullandığım için bu konu beni çok fazla endişelendirmese de bir güvenlik araştırmacısı olarak hesabımın nasıl kullanıma kapatıldığını öğrenmeye karar verdim.

Meslek hayatıma 2005 yılında Etik Hacker, Sızma Testi Uzmanı olarak başladığım ve yıllarca web uygulamalarına yönelik güvenlik testleri de gerçekleştirdiğim için ilk iş olarak e-Devlet Kapısı giriş sayfasını, hesabımı hacklemeye çalışan art niyetli bir kişi gözüyle incelemeye başladım.

Art niyetli bir kişinin hesabıma giriş yapabilmesi için öncelikle TCKN bilgime sahip olması gerekiyordu. Çiçekçiden kargocuya kadar yıllar içinde herkese vermek zorunda kaldığımız ve e-Devlet Hacklendi mi? yazımdan da anlaşılacağı üzere birçok bilgimizin yeraltı dünyasında elden ele gezdiğini gördüğümüz için TCKN bilgimi nereden, nasıl buldukları üzerine pek kafa yormama pek gerek kalmadı.

Peki TCKN bilgime sahip olan art niyetli bir kişi deneme yanılma / kaba kuvvet saldırısı (brute force) gerçekleştirerek er ya da geç parolamı tespit edip, iki aşamalı giriş aşamasına gelebilir miydi? Bu saldırı tekniğini engellemeye yönelik olarak e-Devlet Kapısı'nda CAPTCHA veya IP adresi engelleme gibi bir dizi güvenlik önlemi yok muydu? sorularına yanıt bulmak için öncelikle hatalı parolalar ile e-Devlet hesabıma giriş yapmaya çalıştım. İki hatalı giriş denemesinden sonra güvenli bir web uygulamasında olması gerektiği gibi karşıma CAPTCHA kontrolü çıktı ve hesabım kullanıma kapatılmadı. O halde saldırgan hesabımı nasıl geçici süreliğine kullanıma kapatmayı başarmıştı?



e-Devlet Kapısı

KİMLİK DOĞRULAMA SİSTEMİ



e-Devlet Kapısı
https://www.turkiye.gov.tr

e-Devlet Şifresi

Mobil İmza

Elektronik İmza

T.C. Kimlik Kartı

İnternet Bankacılığı

T.C. Kimlik Numaranızı ve e-Devlet Şifrenizi kullanarak kimliğiniz doğrulandıktan sonra işleminize kaldığınız yerden devam edebilirsiniz. [e-Devlet Şifresi Nedir, Nasıl Alınır?](#)



Kimlik no veya şifre hatalıdır. e-Devlet Kapısı profilinizde cep telefonunuz veya cep telefonu ile birlikte e-posta adresiniz kayıtlı ise (profilde tanımlı olan güvenlik ayarlarına göre) şifrenizi unuttuğunuzda PTT'ye giderek yeni şifre zarfı almak zorunda değilsiniz. Şifrenizi kendiniz kolay ve hızlı bir şekilde yenileyebilirsiniz. Şifrenizi unuttuğunuzda alta yer alan "Şifremi Unuttum" düğmesine basarak şifre yenileme işlemi yapabilirsiniz. Youtube sayfamızdan (<https://youtu.be/I9I6j0o2peE>) şifre yenileme ile ilgili Kamu spotumuzu izleyebilirsiniz.

* T.C. Kimlik No

* e-Devlet Şifresi

* e-Devlet [şifrenizi unutmanız durumunda](#) doğruladığınız cep telefonunuzdan yenileme işlemi yapabilirsiniz.

* Güvenlik Kodu

Lütfen resimde gördüğünüz karakterleri yanında bulunan kutuya giriniz. Resmi okuyamıyorsanız, üzerine tıklayarak yeni bir tane oluşturabilirsiniz.

[Şifremi Unuttum](#)

İptal

Giriş Yap

CAPTCHA (İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi), sorgulama-yanıt doğrulaması olarak bilinen bir güvenlik önlemidir. CAPTCHA spam ve şifre çözme koruması sağlanmasına yardımcı olur. Bunun için sizden basit bir testi yanıtlamanızı isteyerek şifre korumalı bir hesaba girmeye çalışan bir bilgisayar değil insan olduğunuzu kanıtlamanızı sağlar. (Kaynak: Google)

Bu soruya yanıt bulmak için bu sefer VPN ile farklı IP adreslerinden e-Devlet hesabıma hatalı giriş denemeleri yapmaya başladığımda 5. denemede hesabımın bir saatliğine geçici olarak kullanıma kapatıldığını gördüm. Bu da yine güvenli bir web uygulamasında olması gereken bir güvenlik kontrolü olup, belki yüzlerce belki binlerce bot üzerinden hedef hesaba yönelik gerçekleştirilecek kaba kuvvet saldırısı (brute force) ile parolanın tespit edilmesinin (password guessing) önüne geçiyordu.

Hedef Kim?

Son aylarda WhatsApp Dolandırıcıları ve Kripto Para Dolandırıcıları yazılarım ile dolandırıcıların tekerine çomak soktuğum için bu siber saldırıda art niyetli kişi veya kişiler direkt benim hesabımı mı hedef almışlardı yoksa geniş çaplı kullanıcı kitlesine yönelik olarak gerçekleştirdikleri parola spreyi saldırısında tesadüfen benim hesabıma mı denk gelmişlerdi bu defa da bu soruya yanıt aramak için işe koyuldum.

Parola spreyi saldırılarında kötü amaçlı kişiler, en yaygın kullanılan parolaları birçok farklı hesap ve hizmette deneyerek bulabildikleri tüm parola korumalı varlıklara erişim elde etmeye çalışır. Bu saldırılar çoğu zaman birçok farklı kurumu ve kimlik sağlayıcısını kapsar. (Kaynak: Microsoft)

How Password Spraying Works



Görsel: Arkose Labs

Bu soruya yanıt bulmak için benim gibi e-Devlet hesabı geçici süreliğine kapatılan başka kişiler var mı diye Google arama motorunda arama yaptığımda aslında 2020 yılından beri çok sayıda kişinin bu saldırılara mağruz kaldığını öğrendim.

forum.donanimhaber.com/e-devlet-hesabima-girilmeye-calisilmis--146042390

DH Forum

Üye Giriş | Bağlan | Yeni Kayıt

0 oy

3 Cevap | 0 Favori | 1.989 Tıklama | Daha Fazla İstatistik

kelime veya @üye | Konudaki Resimler | Konuya Özel

Sayfa: 1

Giriş

RoseCity
Yüzbaşı
★★★★

383 Mesaj

Konu Sahibine Özel

Mesaj

16 Ekim 2020 20:08:27 | Konu Sahibi

avantajix'e bak | Mesaj Linkini Kopyala | Şikayet

Merhaba bugün gelen mail ile E-Devlet hesabıma birçok kez başarısız giriş yapılmaya çalışıldığı uyarısı aldım. Giriş denemelerini görselde paylaşıyorum. Sanırım başarılı giriş yapamamışlar(Umarım öyledir).

Sifre Durumunuz	Son Değişiklik Tarihi	Sonraki Değişiklik Tarihi	Son Başarısız Giriş Denemesi

Tarih	Uygulama	Sonuç	IP Adresi	Tür
16/10/2020 17:06:20	-	Başarısız	2.58.12.206	Şifre
16/10/2020 17:04:22	-	Başarısız	192.200.158.166	Şifre
16/10/2020 17:02:56	-	Başarısız	5.183.10.234	Şifre
16/10/2020 17:02:40	-	Başarısız	216.151.183.46	Şifre
16/10/2020 17:02:34	-	Başarısız	209.107.196.82	Şifre
16/10/2020 17:02:10	-	Başarısız	205.185.222.128	Şifre
16/10/2020 17:01:34	-	Başarısız	45.10.233.33	Şifre
16/10/2020 17:01:22	-	Başarısız	173.245.203.135	Şifre

EDIT: Twitter'da yaptığım aramada birçok kişiye benzer ip'lerden VPN ile saldırı olmuş.

< Bu mesaj bu kişi tarafından değiştirildi RoseCity -- 16 Ekim 2020; 20:27:14 >

Reklamlar

GOLSEVEN

Bizde Kalasın

Takip

SosyalDigital

SosyalEvin

Bu sayfanın

Mobil sürümü

Mini Sürümü

BR6

0,194

1.2.165

fresh

Amazon Fresh Grocery Store

Amazon Fresh

teknoseyir

Keşfet | Videolar | Bloglar | İncelemeler

Intel 14. Nesil İşlemcilerle İlk Bakış

Soru-Cevap #52

YouTube'ta telif haklarını ihlal etmeden nasıl yayın yapılır?

Tüketici hakları ve hakem heyeti ile hakkımızı nasıl ararız?

Motor hacimleri kafa karıştırmasin

Tümünü gör

Öne çıkan bloglar

Kablolu interneti kablo suza çevirme, bilgisayar wifi olarak kullanmak

Mahkeme ve Savcılık Telefon Verilerimize Erişebilir Mi? Elektronik Eşyalara El Koyma Nasıl Yapılır? Honor ve Huawei Şifrelemesi Güvenli mi?

Türk Telekom Sil Süpür Çıkıyor Çözümü

Ahmet Apa ve Aidin Salih'in Gerçek

Kimliklerimiz her yerde. İyi olmuş.

2 yıl önce Yanıtla Beğen 1

Yorum yap

Engin. @nginx

2 yıl önce

birileri sürekli edevletime girmeye çalışıyor, neden ki ? yurt dışı ip'den giriş kapalı ama denenebiliyor yine de sanırım, birkaç ipye baktım yurtdışı kaynaklı. #edevlet

29/11/2021 14:45:18	-	Başarısız	103.241.54.239:41029	Şifre
29/11/2021 14:44:37	-	Başarısız	73.252.70.67:51427	Şifre
29/11/2021 14:44:10	-	Başarısız	167.71.222.133:48236	Şifre
29/11/2021 14:42:00	-	Başarısız	172.85.105.241:34181	Şifre
29/11/2021 14:41:43	-	Başarısız	174.57.233.32:34539	Şifre
29/11/2021 14:41:23	-	Başarısız	104.248.148.28:58856	Şifre
29/11/2021 14:41:03	-	Başarısız	68.83.240.119:33986	Şifre
29/11/2021 14:39:36	-	Başarısız	45.77.33.190:42768	Şifre
29/11/2021 01:03:25	-	Başarısız	52.142.12.10:1570	Şifre

Beğen | Favori | Paylaş | Yorum yap

serhanhepsen @serhanhepsen

https://teknoseyir.com/durum/1487034

2 yıl önce Yanıtla Beğen 1

Engin. @nginx

yerçek sepetinde doğru düzgün bir aboneliğim yok aslında tcmi de verdiğimi hatırlıyorum

#Stream

#KonuDışı

#Shaft

#Pentagram

Öne çıkan incelemeler

Pentel Graph Gear 1000 Mekanik Kalem

Sinbo SCM-2928 Elektrikli Çeşme (Türk Kahvesi Makinesi)

TURKCELL SÜPERBOX KULLANICI DENEYİMLERİM

A101'DE SATILAN GoSmart GS-BT-02 BLUETOOTH KULAKLIK İNCELEMESİ

Renault Megane III 1.5 dci - Expression (2011)

Tümünü gör

Son bir saat içinde 123 ziyaretçi, 167 kayıtlı kullanıcı giriş yaptı.

© 2023 TeknoSeyir | Hakkımızda | İletişim

← → × 1866387/

Anasayfa Sosyal Blog Sorular Videolar Tavsiyeler TurkNet Son etkinlik İndir

IP adresi üzerinden adres bulunur mu?

aynadakiadam · 21 Şubat 2022 · 10 · 18

1 2 Sonraki ▸



aynadakiadam
Decapat
Katılım: 12 Eylül 2021
Mesajlar: 251
[Daha fazla ▾](#)

21 Şubat 2022 #1

Merhaba, az önce "e-Devlet Kapısı hesabınıza üst üste birden fazla defa yanlış şifre ile giriş yapılmaya çalışılmıştır." diye mail geldi. Geçmişten girmeye çalışan kişilerin IP adresleri çok garip.

2a0c:8dc6:eb1:29a6:9560:33fc:238d:XXXX:XXXX	Şifre		
21/02/2022 16:05:49	-	Başarısız	2a0c:8dc6:eb1:7bf7:f223:66a4:6dab:21
21/02/2022 16:04:55	-	Başarısız	2a0c:8dc6:eb1:b37e:996a:c196:e63b:7
21/02/2022 16:04:20	-	Başarısız	2a0c:8dc6:eb1:e706:8823:b282:5ce9:2
21/02/2022 16:03:24	-	Başarısız	2a0c:8dc6:eb1:529a:5c20:b1a5:9ad:1c

Bu IP adresinden onları bulabilir miyim?

[Cevapla](#) [Etiketle](#)

Bu ekran görüntülerindeki IP adreslerinin kaynağını araştırdığımda bunlardan bazılarının, kullanıcılarına anonim iletişim imkanı sağladığı için siber suçluların da sıklıkla kullandığı Tor isimli bir ağdan gerçekleştirildiğini öğrendim.

171.25.193.78 – Tor Exit Node
185.220.100.252 – Tor Exit Node
185.220.101.46 – Tor Exit Node
77.68.20.217 – Tor Exit Node
104.244.73.193 – Tor Exit Node

Bu durumun yıllar içinde çok sayıda kişinin başına gelmesinden dolayı kuvvetle muhtemel bunun bana yönelik, hedeflenmiş bir saldırı olmayıp parola spreyi saldırısının bir parçası olduğuna kanaat getirerek, hesabımın kilitlenmesinde rol oynayan IP adresleri özelinde araştırmamı genişletmeye karar verdim.

Teknik Araştırma

IP Adresi Tespiti

e-Devlet hesabım kullanıma geri açıldıktan hemen sonra hesabıma giriş yapıp Kullanım Geçmişi sayfasını incelemeye başladığımda, başarısız giriş denemelerinin IPv4 yerine IPv6 adresleri üzerinden yapıldığı hemen dikkatimi çekti.

Şifre Durumunuz

Son Değişiklik Tarihi



Sonraki Değişiklik Tarihi



Son Başarısız Giriş Denemesi

Şifre 25/10/2023 18:46:22 (IP:2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067)

Sisteme Giriş Geçmişiniz

Tarih	Uygulama	Sonuç	IP Adresi	Tür
25/10/2023 20:18:01	-	Başarılı		Şifre
25/10/2023 18:46:22	-	Başarısız	2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067	Şifre
25/10/2023 18:46:18	-	Başarısız	2001:19f0:6801:8dd:daab:291b:a4d6:dfc7:41456	Şifre
25/10/2023 18:46:16	-	Başarısız	2001:19f0:8001:e5d:8404:4a87:e3cf:58cb:59377	Şifre
25/10/2023 18:46:10	-	Başarısız	2600:3c03:e000:b44:ec11:517f:1d99:7cbc:37865	Şifre
25/10/2023 18:44:18	-	Başarısız	2001:19f0:8001:13a:f42d:4d56:deb9:c465:44215	Şifre
12/10/2023 19:48:33	-	Başarısız	2600:3c06:e001:7ab:c6a6:9c89:949f:96f9:48360	Şifre

IP Sahiplik Bilgileri

IPinfo üzerinden IPv6 adreslerinin WHOIS bilgilerine baktığımda tamamının Vultr ve Linode isimli bulut servis sağlayıcılarına ait olduğunu gördüm.

2001:19f0:6001:20f:9a7f:d317:c645:37eb – Vultr
2001:19f0:6801:8dd:daab:291b:a4d6:dfc7 – Vultr
2001:19f0:8001:e5d:8404:4a87:e3cf:58cb – Vultr
2600:3c03:e000:b44:ec11:517f:1d99:7cbc – Linode
2001:19f0:8001:13a:f42d:4d56:deb9:c465 – Vultr
2600:3c06:e001:7ab:c6a6:9c89:949f:96f9 – Linode

Bağlantı Noktaları

Bu IPv6 adreslerinin en bilinen açık bağlantı noktalarını (port) nmap aracı ile taradığımda sadece SSH servisine ait 22. bağlantı noktalarının açık olduğunu öğrendim.

```
root@~# nmap -iL hosts.txt -6 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-25 14:12 EDT
Nmap scan report for 2001:19f0:6001:20f:9a7f:d317:c645:37eb
Host is up (0.067s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
```

```
Nmap scan report for 2001:19f0:6801:8dd:daab:291b:a4d6:dfc7
Host is up (0.081s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
```

```
Nmap scan report for 2001:19f0:8001:e5d:8404:4a87:e3cf:58cb
Host is up (0.060s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
```

```
Nmap scan report for 2600:3c03:e000:b44:ec11:517f:1d99:7cbc
Host is up (0.00019s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
```

```
Nmap scan report for 2001:19f0:8001:13a:f42d:4d56:deb9:c465
Host is up (0.060s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
```

IPv6'dan IPv4'e Yolculuk

IPv6 adreslerine ait sunucularla ilgili daha fazla bilgi toplamak için yine nmap aracı ile (nmap -iL hosts.txt -6 -sV --script ssh-hostkey.nse --script-args ssh_hostkey=all) SSH servislerinin parmak izlerini (ssh fingerprint) Shodan arama motorunda arattığımda, bu sunucuların IPv4 adreslerini kolaylıkla bulabildim.

```
2001:19f0:6001:20f:9a7f:d317:c645:37eb
ssh-hostkey: b9:cb:48:39:52:d9:f2:83:d8:ba:12:e9:9f:1d:55:21
```

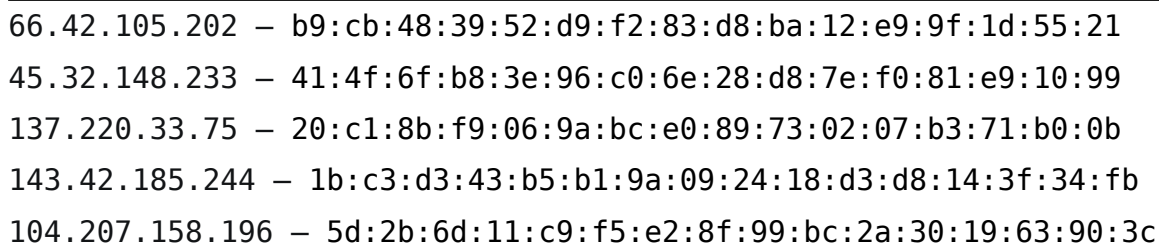
```
2001:19f0:6801:8dd:daab:291b:a4d6:dfc7
ssh-hostkey: 41:4f:6f:b8:3e:96:c0:6e:28:d8:7e:f0:81:e9:10:99
```



```
ssh-hostkey: 20:c1:8b:f9:06:9a:bc:e0:89:73:02:07:b3:71:b0:0b
```

```
ssh-hostkey: 1b:c3:d3:43:b5:b1:9a:09:24:18:d3:d8:14:3f:34:fb
```

```
ssh-hostkey: 5d:2b:6d:11:c9:f5:e2:8f:99:bc:2a:30:19:63:90:3c
```



Elde ettiğim bu IPv4 ve IPv6 adreslerini tehdit araştırmalarında sıklıkla kullanılan başta VirusTotal, SOCRadar XTI, AlienVault OTX olmak üzere çeşitli platformlarda arattığımda bunlardan sadece SOCRadar XTI üzerinde bir sonuca ulaşabildim.

Buradaki sonuca göre, saldırgan tarafından kullanılan 45.32.148.233 IP adresine sahip sunucuya ait erişim bilgilerinin yer aldığı bir son kullanıcı sistemi, 2023 yılının Mayıs ayında hacklenmiş ve üzerinde Racoon isimli bilgi çalmakta kullanılan bir zararlı yazılım çalışmıştı. 2022 yılında ise yine bu IP adresinin yer aldığı başka bir son kullanıcı sistemi benzer şekilde RedLine isimli bilgi çalan başka bir zararlı yazılım tarafından enfekte olmuştu. Tüm çalınan bu bilgiler de daha sonrasında Rus yeraltı marketinde

(Russian Market) satışa çıkmıştı.

The screenshot shows the SOCRadar Threat Hunting interface. The main search area displays results for the IP address 45.32.148.233. The results show that the IP was observed for sale on the Russian Market on May 28, 2023. The search results are filtered by Source (46/46), Country (250/250), Sector (41/41), and Date Range. The search results are displayed in a table with columns for Source, Discover Date, Content Link, Country, Date, Files, Price, Size, Stealer, Vendor, Province, ISP, Links, and Tags. The search results are filtered by Source (46/46), Country (250/250), Sector (41/41), and Date Range. The search results are displayed in a table with columns for Source, Discover Date, Content Link, Country, Date, Files, Price, Size, Stealer, Vendor, Province, ISP, Links, and Tags. The search results are filtered by Source (46/46), Country (250/250), Sector (41/41), and Date Range. The search results are displayed in a table with columns for Source, Discover Date, Content Link, Country, Date, Files, Price, Size, Stealer, Vendor, Province, ISP, Links, and Tags.

SOCRadar Dark Web ekibi tarafından temin edilen dosyaların içeriğine baktığımda, sunucu üzerinde bir zamanlar phpMyAdmin isimli veritabanı yönetim aracı bulunduğu anlaşıyordu. Bu bilgiler ışığında art niyetli kişiler uzun zamandan beri bu sunucuya yetkisiz olarak erişim sağlıyor ve saldırılarında kullanıyor olabilirlerdi.

LOGID-4704366					
Name	Date Modified	Size	Kind		
> Autofills	August 23, 2022, 03:14		--	Folder	
> Cookies	August 23, 2022, 03:14		--	Folder	
DomainDetects.txt	August 23, 2022, 03:14	133 bytes		Plain Text	
ImportantAutofills.txt	August 23, 2022, 03:14	1 KB		Plain Text	
InstalledBrowsers.txt	August 23, 2022, 03:14	962 bytes		Plain Text	
InstalledSoftware.txt	August 23, 2022, 03:14	3 KB		Plain Text	
Passwords.txt	August 23, 2022, 03:14	2 KB		Plain Text	
Screenshot.jpg	August 23, 2022, 03:14	291 KB		JPEG image	
> Steam	August 23, 2022, 03:14		--	Folder	
UserInformation.txt	August 23, 2022, 03:14	1 KB		Plain Text	


```
*****
*                                     *
* REOOLINE                          *
*                                     *
* Telegram: https://t.me/          *
*                                     *
*****

URL: https://hebergtonserv.fr/password/reset/change
Username: 
Password: 
Application: Opera Software_Unknown
=====

URL: http://45.32.148.233/phpmyadmin/index.php
Username: 
Password: 
Application: Microsoft_[Edge]_Default
=====
```

Yeni Bağlantı Noktaları

Censys isimli arama motorunda IPv4 adreslerini inceleyip, her birinin bağlantı noktalarını yine nmap aracı ile taradığımda bu defa IPv6 taramalarından farklı olarak her bir sunucuda 22. bağlantı noktası hariç 2000'e yakın yeni bağlantı noktası olduğunu keşfettim.

 Hosts 104.207.158.196

104.207.158.196

As of: Nov 12, 2023 1:33am UTC | Latest

Summary History WHOIS Explore

Basic Information

Reverse DNS	104.207.158.196.vultrusercontent.com
Routing	104.207.156.0/22 via AS-CHOOPA, US (AS20473)
OS	linux
Services (75)	22/SSH, 30005/HTTP, 30024/HTTP, 30025/HTTP, 30046/HTTP, 30120/HTTP, 30139/HTTP, 30153/HTTP, 30159/HTTP, 30216/HTTP, 30227/HTTP, 30235/HTTP, 30266/HTTP, 30322/HTTP, 30333/HTTP, 30362/HTTP, 30384/HTTP, 30386/HTTP, 30430/HTTP, 30481/HTTP, 30487/HTTP, 30574/HTTP, 30591/HTTP, 30594/HTTP, 30596/HTTP, 30614/HTTP, 30650/HTTP, 30673/HTTP, 30720/HTTP, 30752/HTTP, ...
Labels	TRUNCATED

143.42.185.244

As of: Nov 11, 2023 10:57pm UTC | Latest

Summary

History

WHOIS

Explore

Basic Information

Reverse DNS	143-42-185-244.ip.linodeusercontent.com
Forward DNS	143-42-185-244.ip.linodeusercontent.com, 143-42-185-244.ipv4.staticdns1.io
Routing	143.42.176.0/20 via AKAMAI-LINODE-AP Akamai Connected Cloud, SG (AS63949)
OS	linux
Services (125)	22/SSH, 10000/HTTP, 10001/HTTP, 10006/HTTP, 10049/HTTP, 10055/HTTP, 10060/HTTP, 10068/HTTP, 10081/HTTP, 10144/HTTP, 10148/HTTP, 10193/HTTP, 10197/HTTP, 10220/HTTP, 10229/HTTP, 10238/HTTP, 10251/HTTP, 10252/HTTP, 10254/HTTP, 10258/HTTP, 10275/HTTP, 10285/HTTP, 10319/HTTP, 10328/HTTP, 10368/HTTP, 10382/HTTP, 10405/HTTP, 10408/HTTP, 10442/HTTP, 10443/HTTP, ...
Labels	TRUNCATED

137.220.33.75

As of: Nov 11, 2023 5:32pm UTC | Latest

Summary

History

WHOIS

Explore

Basic Information

Reverse DNS	137.220.33.75.vultrusercontent.com
Routing	137.220.32.0/20 via AS-CHOOPA, US (AS20473)
OS	linux
Services (154)	22/SSH, 42005/HTTP, 42011/HTTP, 42022/HTTP, 42034/HTTP, 42036/HTTP, 42040/HTTP, 42042/HTTP, 42070/HTTP, 42116/HTTP, 42135/HTTP, 42136/HTTP, 42143/HTTP, 42167/HTTP, 42172/HTTP, 42184/HTTP, 42192/HTTP, 42218/HTTP, 42231/HTTP, 42256/HTTP, 42269/HTTP, 42299/HTTP, 42304/HTTP, 42307/HTTP, 42308/HTTP, 42309/HTTP, 42311/HTTP, 42315/HTTP, 42381/HTTP, 42383/HTTP, ...
Labels	TRUNCATED

45.32.148.233

As of: Nov 11, 2023 9:47pm UTC | Latest

📄 Summary

🕒 History

📄 WHOIS

👤 Explore

Basic Information

Reverse DNS	45.32.148.233.vultrusercontent.com
Routing	45.32.144.0/21 via AS-CHOOPA, US (AS20473)
OS	linux
Services (154)	22/SSH, 22014/HTTP, 22016/HTTP, 22019/HTTP, 22029/HTTP, 22035/HTTP, 22038/HTTP, 22055/HTTP, 22082/HTTP, 22107/HTTP, 22117/HTTP, 22122/HTTP, 22123/HTTP, 22154/HTTP, 22160/HTTP, 22164/HTTP, 22166/HTTP, 22168/HTTP, 22172/HTTP, 22186/HTTP, 22187/HTTP, 22192/HTTP, 22210/HTTP, 22222/HTTP, 22224/HTTP, 22225/HTTP, 22274/HTTP, 22277/HTTP, 22284/HTTP, 22288/HTTP, ...
Labels	TRUNCATED

66.42.105.202

As of: Nov 11, 2023 6:12pm UTC | Latest

📄 Summary

🕒 History

📄 WHOIS

👤 Explore

Basic Information

Reverse DNS	66.42.105.202.vultrusercontent.com
Routing	66.42.96.0/20 via AS-CHOOPA, US (AS20473)
OS	linux
Services (105)	22/SSH, 14020/HTTP, 14022/HTTP, 14067/HTTP, 14071/HTTP, 14079/HTTP, 14127/HTTP, 14184/HTTP, 14185/HTTP, 14218/HTTP, 14284/HTTP, 14291/HTTP, 14302/HTTP, 14314/HTTP, 14318/HTTP, 14325/HTTP, 14341/HTTP, 14351/HTTP, 14369/HTTP, 14385/HTTP, 14392/HTTP, 14397/HTTP, 14398/HTTP, 14401/HTTP, 14402/HTTP, 14407/HTTP, 14417/HTTP, 14426/HTTP, 14475/HTTP, 14484/HTTP, ...
Labels	TRUNCATED

```
root@ :~# cat nmap.txt
# Nmap 7.80 scan initiated Wed Oct 25 20:23:15 2023 as: nmap -sS -p 1-65535 -oG nmap.txt 45.32.148.233
Host: 45.32.148.233 (45.32.148.233.vultrusercontent.com) Status: Up
Host: 45.32.148.233 (45.32.148.233.vultrusercontent.com) Ports: 22/open/tcp//ssh///, 22000/open/tcp//
/snappenetio///, 22001/open/tcp//optocontrol///, 22002/open/tcp//optohost002///, 22003/open/tcp//optohost003
///, 22004/open/tcp//optohost004///, 22005/open/tcp//optohost004///, 22006/open/tcp///// , 22007/open/tcp///
//, 22008/open/tcp///// , 22009/open/tcp///// , 22010/open/tcp///// , 22011/open/tcp///// , 22012/open/tcp/////
, 22013/open/tcp///// , 22014/open/tcp///// , 22015/open/tcp///// , 22016/open/tcp///// , 22017/open/tcp///// ,
22018/open/tcp///// , 22019/open/tcp///// , 22020/open/tcp///// , 22021/open/tcp///// , 22022/open/tcp//unknown
///, 22023/open/tcp///// , 22024/open/tcp///// , 22025/open/tcp///// , 22026/open/tcp///// , 22027/open/tcp/////
/ , 22028/open/tcp///// , 22029/open/tcp///// , 22030/open/tcp///// , 22031/open/tcp///// , 22032/open/tcp///// ,
22033/open/tcp///// , 22034/open/tcp///// , 22035/open/tcp///// , 22036/open/tcp///// , 22037/open/tcp///// , 2
2038/open/tcp///// , 22039/open/tcp///// , 22040/open/tcp///// , 22041/open/tcp///// , 22042/open/tcp///// , 220
43/open/tcp///// , 22044/open/tcp///// , 22045/open/tcp///// , 22046/open/tcp///// , 22047/open/tcp///// , 22048
/open/tcp///// , 22049/open/tcp///// , 22050/open/tcp///// , 22051/open/tcp///// , 22052/open/tcp///// , 22053/o
pen/tcp///// , 22054/open/tcp///// , 22055/open/tcp///// , 22056/open/tcp///// , 22057/open/tcp///// , 22058/ope
n/tcp///// , 22059/open/tcp///// , 22060/open/tcp///// , 22061/open/tcp///// , 22062/open/tcp///// , 22063/open/
tcp//unknown///, 22064/open/tcp///// , 22065/open/tcp///// , 22066/open/tcp///// , 22067/open/tcp///// , 22068/
open/tcp///// , 22069/open/tcp///// , 22070/open/tcp///// , 22071/open/tcp///// , 22072/open/tcp///// , 22073/op
en/tcp///// , 22074/open/tcp///// , 22075/open/tcp///// , 22076/open/tcp///// , 22077/open/tcp///// , 22078/open
/tcp///// , 22079/open/tcp///// , 22080/open/tcp///// , 22081/open/tcp///// , 22082/open/tcp///// , 22083/open/t
cp///// , 22084/open/tcp///// , 22085/open/tcp///// , 22086/open/tcp///// , 22087/open/tcp///// , 22088/open/tcp
///// , 22089/open/tcp///// , 22090/open/tcp///// , 22091/open/tcp///// , 22092/open/tcp///// , 22093/open/tcp/
///, 22094/open/tcp///// , 22095/open/tcp///// , 22096/open/tcp///// , 22097/open/tcp///// , 22098/open/tcp/////
/ , 22099/open/tcp///// , 22100/open/tcp//unknown///, 22101/open/tcp///// , 22102/open/tcp///// , 22103/open/tc
p///// , 22104/open/tcp///// , 22105/open/tcp///// , 22106/open/tcp///// , 22107/open/tcp///// , 22108/open/tcp/
///// , 22109/open/tcp///// , 22110/open/tcp///// , 22111/open/tcp///// , 22112/open/tcp///// , 22113/open/tcp/
///, 22114/open/tcp///// , 22115/open/tcp///// , 22116/open/tcp///// , 22117/open/tcp///// , 22118/open/tcp/////
, 22119/open/tcp///// , 22120/open/tcp///// , 22121/open/tcp///// , 22122/open/tcp///// , 22123/open/tcp///// ,
22124/open/tcp///// , 22125/open/tcp//dcap///, 22126/open/tcp///// , 22127/open/tcp///// , 22128/open/tcp//gsi
dcap///, 22129/open/tcp///// , 22130/open/tcp///// , 22131/open/tcp///// , 22132/open/tcp///// , 22133/open/tcp
///// , 22134/open/tcp///// , 22135/open/tcp///// , 22136/open/tcp///// , 22137/open/tcp///// , 22138/open/tcp/
```

Bir sunucu üzerinde 2000'e yakın açık bağlantı noktasının bulunması alışlagelmiş bir yapılandırma biçimi olmadığı için bu bağlantı noktalarını kontrol etmeye karar verdim.

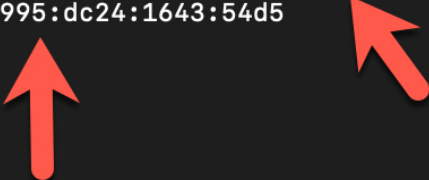
Bir sistem üzerinde bu kadar çok açık bağlantı noktasına genelde vekil sunucuda (proxy) rastlandığı için ilk olarak bundan şüphelenmeye başladım. Saldırgan tarafından kullanılan IPv4 adreslerinin bilgilerini Censys üzerinde incelemeye devam ettiğimde, 45.32.148.233 IPv4 adresi ile ilgili kayıtlarda bir satır (Proxy-Connection: close) hemen dikkatimi çekti ve aklımda yeni bir soru daha belirdi. Bunlar 2000'li yılların başında internette sıklıkla rastladığımız açık vekil sunucular gibi olabilirler miydi ?

Anonim bir açık proxy, sunucu istekleri proxy sunucusundan geliyor gibi görüldüğü için kullanıcıların IP adreslerini web sunucularından gizlemelerine yardımcı olabileceğinden, çevrimiçi anonimlik ve gizlilik isteyenler için yararlıdır. Kimliklerini ortaya çıkarmayı zorlaştırır ve böylece web'e göz atarken veya diğer internet hizmetlerini kullanırken algılanan güvenliklerinin korunmasına yardımcı olur. (Kaynak: Wikipedia)

Bu soruya yanıt bulmak için cURL aracına 45.32.148.233 IPv4 adresini, vekil sunucu olarak Censys'de yer alan rastgele bir bağlantı noktası (22939) ile

birlikte belirtip <https://ifconfig.me/all> web sayfasına istekte bulunduğumda, bu vekil sunucudan bu web sayfasına isteğin 2001:19f0:6801:8dd:4995:dc24:1643:54d5 IPv6 adresinden gönderildiğini gördüm. Kısaca sorunun yanıtı “Evet” idi. Bunlar açık vekil sunuculardı ve bunlar üzerinden hedef web sayfalarına kendi IPv4 adresimi gizleyerek web isteğinde bulunabiliyordum.

```
% curl -L -x 45.32.148.233:22939 https://ifconfig.me/all
ip_addr: 2001:19f0:6801:8dd:4995:dc24:1643:54d5
remote_host: unavailable
user_agent: curl/8.1.2
port: 48392
language:
referrer:
connection:
keep_alive:
method: GET
encoding:
mime: */*
charset:
via: 1.1 google
forwarded: 2001:19f0:6801:8dd:4995:dc24:1643:54d5, 2600:1901:0:b2bd::,130.211.0.85
```



Ancak yukardaki ekran görüntüsünde yer alan 2001:19f0:6801:8dd:4995:dc24:1643:54d5 IPv6 adresine sahip vekil sunucu, benim e-Devlet hesabımın geçici süreliğine kapatılmasında rol oynayanlardan biri (2001:19f0:6801:8dd:daab:291b:a4d6:dfc7) değildi. Bu vekil sunucu ile o IPv6 arasındaki ilişkiyi tespit etmek için bu defa 45.32.148.233 IPv4 adresinin açık 2000 bağlantı noktasına (port) bağlanıp <https://ifconfig.me/ip> web sayfasına istek gönderen basit bir betik (script) hazırladım.

```
#!/bin/sh
for ((i=22000; i<=24000; i++)) do curl -x 45.32.148.233:$i -L -s -k
https://ifconfig.me/ip >> ip_check_45.32.148.233.txt
echo ' ' >> ip_check_45.32.148.233.txt
sleep 1
done
```

Web sayfasından gelen her bir yanıtta farklı bir IPv6 adresi yer alıyordu. Bu sonuca göre art niyetli kişiler, 2000 tane IPv6 üzerinden istedikleri web sayfasına kaba kuvvet saldırısı gerçekleştirebiliyorlardı. Betik bir süre çalıştıktan sonra e-Devlet hesabıma saldırıyı gerçekleştiren IPv6 adresini de bu adresler arasında görebildim.

Şifre Durumunuz				
Son Değişiklik Tarihi				
Sonraki Değişiklik Tarihi				
Son Başarısız Giriş Denemesi Şifre 25/10/2023 18:46:22 (IP:2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067)				
Sisteme Giriş Geçmişiniz				
Tarih	Uygulama	Sonuç	IP Adresi	Tür
25/10/2023 20:18:01	-	Başarılı		Şifre
25/10/2023 18:46:22	-	Başarısız	2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067	Şifre
25/10/2023 18:46:18	-	Başarısız	2001:19f0:6801:8dd:daab:291b:a4d6:dfc7:41456	Şifre
25/10/2023 18:46:16	-	Başarısız	2001:19f0:8001:e5d:8404:4a87:e3cf:58cb:59377	Şifre
25/10/2023 18:46:10	-	Başarısız	2600:3c03:e000:b44:ec11:517f:1d99:7cbc:37865	Şifre
25/10/2023 18:44:18	-	Başarısız	2001:19f0:8001:13a:f42d:4d56:deb9:c465:44215	Şifre
12/10/2023 19:48:33	-	Başarısız	2600:3c06:e001:7ab:c6a6:9c89:949f:96f9:48360	Şifre

```
ip_check_45.32.148.233.txt
1264 2001:19f0:6801:8dd:fee8:e0c0:830:b2bf
1265 2001:19f0:6801:8dd:5712:7427:8663:73f1
1266 2001:19f0:6801:8dd:56d3:2d51:a7b9:b123
1267 2001:19f0:6801:8dd:325e:ac39:e66f:4be2
1268 2001:19f0:6801:8dd:ac34:f4bf:3876:1c68
1269 2001:19f0:6801:8dd:a1db:2544:24d5:5ca6
1270 2001:19f0:6801:8dd:5fb2:bc26:9504:d296
1271 2001:19f0:6801:8dd:bfc4:6195:1183:f35c
1272 2001:19f0:6801:8dd:9e83:1289:e5a4:5f1a
1273 2001:19f0:6801:8dd:933a:939a:25b6:6f8a
1274 2001:19f0:6801:8dd:9f6b:908e:1468:8531
1275 2001:19f0:6801:8dd:7659:7f7b:f29e:f2cc
1276 2001:19f0:6801:8dd:6c8c:22ec:174:37e5
1277 2001:19f0:6801:8dd:836c:ecfb:68b9:4240
1278 2001:19f0:6801:8dd:a7e0:33e7:41c5:5024
1279 2001:19f0:6801:8dd:e605:883a:e6dd:91a3
1280 2001:19f0:6801:8dd:abff:fffb:73b3:1541
1281 2001:19f0:6801:8dd:84a7:246c:312f:3bef
1282 2001:19f0:6801:8dd:c977:9370:1776:55ae
1283 2001:19f0:6801:8dd:8b7f:e341:4f71:18e4
1284 2001:19f0:6801:8dd:d375:7138:74da:dbc6
1285 2001:19f0:6801:8dd:daab:291b:a4d6:dfc7
1286 2001:19f0:6801:8dd:d666:ab22:6786:8ce6
1287 2001:19f0:6801:8dd:5c7f:39ac:55ab:4518
1288 2001:19f0:6801:8dd:3999:3201:c1e4:d4ec
1289 2001:19f0:6801:8dd:94da:74ef:5c85:40a6
1290 2001:19f0:6801:8dd:daba:fdff:c4ca:c0a8
1291 2001:19f0:6801:8dd:c573:fa72:372a:1c75
1292 2001:19f0:6801:8dd:16e:6996:c8b8:b718
1293 2001:19f0:6801:8dd:6b49:1cd3:cfed:3d22
1294 2001:19f0:6801:8dd:d556:cf33:8301:1108
1295 2001:19f0:6801:8dd:f529:3e1f:68c2:8161
1296 2001:19f0:6801:8dd:2702:6559:f02f:af74
1297 2001:19f0:6801:8dd:fd00:3bab:3da2:9bd5
1298 2001:19f0:6801:8dd:980f:b51f:87e1:3e40
1299 2001:19f0:6801:8dd:889d:a6fc:4bfc:57f3
1300 2001:19f0:6801:8dd:829b:2b56:97f3:d011
1301 2001:19f0:6801:8dd:7b0b:2644:f20a:36c9
1302 2001:19f0:6801:8dd:b424:7e93:da5f:f634
1303 2001:19f0:6801:8dd:d9e:64fe:d339:7394
1304 2001:19f0:6801:8dd:41e:a5a:5db1:6f6b
1305 2001:19f0:6801:8dd:f4ba:2874:3485:1b07
1306 2001:19f0:6801:8dd:9522:c4cd:8a1b:d04a
```

Neden IPv6 adresi kullanıyorlar?

Tüm bu araştırmaları yaparken bir yandan saldırganın neden IPv6 adresleri kullandığı kafamı kurcalamaya başladı ve bir zaman sonra şeytanın ayrıntıda gizli olduğunu anladım.

DigitalOcean, Linode, Vultr ve benzeri servis sağlayıcılarından bir sunucu kiraladığınızda size bir adet IPv4 tahsis ediyorlar ve bu sunucu üzerinden internet ile ilişkili yaptığınız tüm işlemlerde bu IP adresini kullanıyorsunuz.

Siber suçlular da çoğu zaman siber saldırılarını gerçekleştirmek veya kamufle etmek için bu tür servis sağlayıcılarından sunucu kiralyorlar. Zamanla gerçekleştirdikleri siber saldırılara ait sunucuların IPv4 adresleri güvenlik teknolojileri tarafından tespit edilip, engellenmeye, küresel kara listelere eklenmeye başlıyor. Saldırı girişimleri engellenmeye başlandıkça da bu IPv4 adreslerini kullanamaz noktaya geliyorlar ve şikayet bildirimleri nedeniyle hesapları, sunucuları da hızla kapandığı için yeni bir sunucu arayışına giriyorlar.

Örneğin basit bir hespla bu siber saldırıları 100 tane sunucudan gerçekleştirdiklerini düşündüğümüzde, sunucu başına 6\$ ödedikleri için toplam 600\$ maliyete katlanmaları gerekiyor ve bunu ne kadar uzun süre engellenmeden gerçekleştirebilirlerse yanlarına kar kalıyor aksi halde kara listelere eklendikçe tekrar ve tekrar bu maliyete katlanmaları gerekiyor.

Peki IPv4 yerine IPv6 kullandıklarında işin rengi nasıl değişiyor? Bu servis sağlayıcıları, sunucu kiralayan müşterilerine sadece 1 adet IPv4 kullanma hakkı tanırken, mevzu bahis IPv6 olduğunda binlercesini üretmelerine ve kullanmalarına imkan tanıyorlar. Böyle olunca da art niyetli kişiler sadece 6\$ ödeyerek binden fazla IPv6 adresi üzerinden saldırılarını gerçekleştirebiliyorlar. Kara listelere eklendikçe kullandıkları sunucular üzerinde yeni IPv6 adresleri üretip, kullanabildikleri için de ta ki servis sağlayıcısına şikayetler ulaşana kadar kara listelerden pek fazla etkilenmeden saldırılarını uzun süre aynı sunucu üzerinde gerçekleştirebiliyorlar.

Peki e-Devlet uygulaması, uyguladığı güvenlik kontrolleri, önlemleri nedeniyle saldırganları IPv4 yerine IPv6 kullanmalarına gerçekten zorluyor muydu yoksa saldırganlar işlerini garantiye almak için mi IPv6 kullanmayı tercih ediyorlardı? Bunun için e-Devlet hesabımı 5 defa hatalı giriş denemesi ile geçici olarak kullanıma kapattıktan hemen sonra eşimin hesabına bu defa doğru parola ile giriş yapmaya çalıştığımda başarıyla giriş yapabildiğimi gördüm.

Bu sonuca göre uygulama genelinde ve/veya ağ seviyesinde bir IPv4 hesabı ile ikiden fazla hesaba bu şekilde kaba kuvvet saldırısı yapıldığında bu IPv4 adresi kara listeye eklenmiyorsa, engellenmiyorsa bu durumda saldırganlar bir IPv4 adresi ile uzun süre, birden fazla hesaba bu saldırıları gerçekleştirebilirlerdi. Aksi durumda ise IPv6 adresleri kullanmaktan başka çareleri kalmıyordu.

İkiden fazla e-Devlet hesabı üzerinde bunu test ve teyit etme şansım olmadığı ve saldırganların da IPv6 sistemler üzerinden bu saldırıları gerçekleştirdiğini göz önünde bulundurduğumda, kuvvetle muhtemel saldırganların kullandığı IPv4 adreslerine e-Devlet güvenlik önlemleri geçit vermiyordu.

e-Devlet Hesabımı Nasıl Koruyabilirim?

Sonuç itibariyle siber saldırganların uzun yıllardır e-Devlet hesaplarımızı hacklemek için yeri geldiğinde hacklenmiş, enfekte sistemlerden oluşan bot ağlarını yeri geldiğinde kendi sistemlerini kullandıklarını, izlerini gizlemek, yakalanmamak için vekil sunucu yazılımlarından faydalandıklarını, IPv6 desteği olan servis sağlayıcılardan sunucular satın aldıklarını, kısacası her yolu denediklerini görebiliyoruz.

Peki bu durumda sade bir vatandař olarak kendinizi bu yazıya konu olan saldırılardan nasıl koruyabilirsiniz? Bunun için yapmanız gereken en önemli adım, e-Devlet hesabınıza giriřte mutlaka ama mutlaka iki aşamalı giriř yöntemlerinden birini kullanmanız olacaktır. Nasıl kullanabileceğinizi bu adresi ziyaret ederek öğrenebilirsiniz.

Bu vesileyle yeni yılınızı kutlar, 2024 yılının hem sizlere hem de tüm sevdiklerinize önce saęlık sonra mutluluk ve başarı getirmesini dilerim.

Bir sonraki yazıda görüşmek dileęiyle.