

How Do They Hack Turkish e-Government Accounts?

written by Mert SARICA | 1 December 2023

Table of Contents

1. Introduction
2. Who is the Target?
3. Technical Investigation
 1. Attackers' IP Addresses
 2. IP Addresses Lookup
 3. Ports
 4. Journey from IPv6 to IPv4
 5. Threat Research
 6. New Ports
 7. Why are they using an IPv6 address?
4. How Can I Protect My e-Government Account?

Introduction

On October 25, 2023, at 11:46, I learned that my Turkish e-Government Gateway account had been temporarily disabled for one hour due to multiple unsuccessful login attempts with the wrong password through the e-Government application and warnings sent to my email address.



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

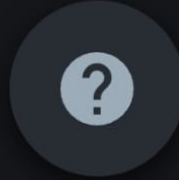
Mobil İmza ile Giriş Yap



Mobil Onay



Karekod Okut



YARDIM

HIZLI ERİŞİM



Hava Durumu



Nöbetçi Eczane
Sorgulama



Acil Toplanma
Alanları



TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ




Although the likelihood of a threat actor guessing my long and complex password was low, and I also use a two-step authentication method on the e-Government Gateway, as a security researcher, I decided to investigate how my account was temporarily disabled.


Having started my professional career in 2005 as an Ethical Hacker and Penetration Tester, conducting security tests for web applications for years, I began examining the e-Government Gateway login page as if I were a threat actor attempting to hack my account.

For a threat actor to access my account, they needed to have my TCKN (Turkish ID) information. Given that, as seen in my article “Was Turkey’s e-Government Hacked?”, many of our details circulate in the underground, obtained from various sources over the years, I didn’t need to dwell on where and how they found my TCKN information.

Could a threat actor with my TCKN information eventually determine my password through brute force attack and reach the two-step authentication stage? Did e-Government Gateway not have a series of security measures to prevent this attack technique, such as CAPTCHA or IP address blocking? To find answers to these questions, I attempted to log into my e-Government account with incorrect passwords. After two unsuccessful attempts, a CAPTCHA control appeared, as expected in a secure web application, and my account was not disabled. So, how did the attacker manage to temporarily disable my account?


← → ↻ 🏠 giris.turkiye.gov.tr/Giris/gir 🔑 📄 ☆

**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 altta 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

* Güvenlik Kodu

[Şifremi Unuttum](#)

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of security measure known as challenge-response authentication. CAPTCHA helps protect you from spam and password decryption by asking you to complete a simple test that proves you are human and not a computer trying to break into a password protected account. (Source: Google)

In an attempt to find an answer to this question, when I started making unsuccessful login attempts to my e-Government account from different IP addresses using a VPN, I observed that my account was temporarily disabled for one hour on the 5th attempt. This once again demonstrated a security control that should exist in a secure web application. It effectively prevents the detection of the password through a brute force attack, which might target the account through possibly hundreds or thousands of bots.

Who is the Target?

In recent months, due to my articles on WhatsApp Scammers and Cryptocurrency Scammers, I've been able to thwart the plans of scammers. In this cyber attack, I set out to determine whether the threat actors had specifically targeted my account or if they had coincidentally come across my account in a password spraying attack targeting broad accounts.

In a password spray attack, the bad guys try the most common passwords across many different accounts and services to gain access to any password protected assets they can find. Usually these span many different organizations and identity providers. For example, an attacker will use a commonly available toolkit like Mailsniper to enumerate all of the users in several organizations and then try "P@\$\$w0rd" and "Password1" against all of those accounts. (Source: Microsoft)

How Password Spraying Works



Image: Arkose Labs

To find an answer to this question, I conducted a Google search to see if there were other individuals like me whose e-Government accounts had been temporarily disabled. Through my search, I discovered that a significant number of people have been subjected to such attacks since 2020.

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

yerem 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


← → × 🏠 technopat.net/sosyal/konu/ip-adresi-uezerinden-adres-bulunur-mu.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](#)

When I investigated the source of the IP addresses in these screenshots, I found that some of them were originating from a network called Tor, which is frequently used by cybercriminals for anonymous communication.

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

Considering that this situation has occurred to many individuals over the years, it is highly likely that it was not a targeted attack against me but rather a part of a password spraying attack. To further investigate the IP addresses that played a role in locking my account, I decided to broaden my research.

Technical Investigation

Attackers' IP Addresses

When I accessed my e-Government account immediately after it was reopened, and began examining the History page, I quickly noticed that the unsuccessful login attempts were made using IPv6 addresses instead of IPv4.

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 Addresses Lookup

When I checked the WHOIS information of the IPv6 addresses through IPinfo, I found that all of them belonged to cloud service providers named Vultr and Linode.

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

Ports

When I scanned the IPv6 addresses for their most well-known open ports using the nmap tool, I found that only the 22nd port, associated with the SSH service, was open.

```
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)
```

Journey from IPv6 to IPv4

When I used the nmap tool again (`nmap -iL hosts.txt -6 -sV --script ssh-hostkey.nse --script-args ssh_hostkey=all`) to search for the fingerprints of SSH services and queried Shodan, I easily found the IPv4 addresses of these servers to gather more information about them.

```
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
```

```
2001:19f0:8001:e5d:8404:4a87:e3cf:58cb
```

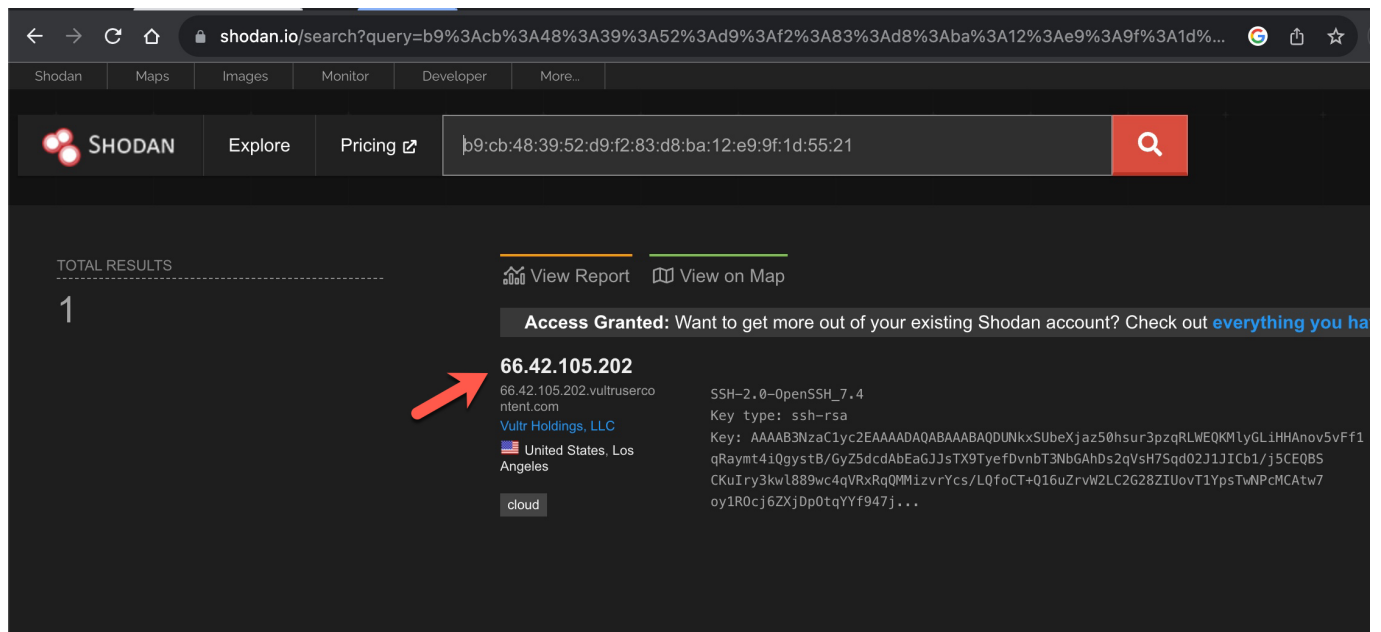

ssh-hostkey: 20:c1:8b:f9:06:9a:bc:e0:89:73:02:07:b3:71:b0:0b

2600:3c03:e000:b44:ec11:517f:1d99:7cbc

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

2001:19f0:8001:13a:f42d:4d56:deb9:c465

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



66.42.105.202 – b9:cb:48:39:52:d9:f2:83:d8:ba:12:e9:9f:1d:55:21

45.32.148.233 – 41:4f:6f:b8:3e:96:c0:6e:28:d8:7e:f0:81:e9:10:99

137.220.33.75 – 20:c1:8b:f9:06:9a:bc:e0:89:73:02:07:b3:71:b0:0b

143.42.185.244 – 1b:c3:d3:43:b5:b1:9a:09:24:18:d3:d8:14:3f:34:fb

104.207.158.196 – 5d:2b:6d:11:c9:f5:e2:8f:99:bc:2a:30:19:63:90:3c

Threat Research

The information gathered from the obtained IPv4 and IPv6 addresses, when searched on various platforms such as VirusTotal, SOCRadar XTI, AlienVault OTX, resulted in findings only on SOCRadar XTI.

According to the results, an end user system associated with the server having the IP address 45.32.148.233, used by the attacker, was compromised in May 2023. A malware named Racoon, used for stealing information, operated on this system. In 2022, another end user system associated with the same IP address was infected with another information-stealing malware called RedLine. All the stolen information was later put up for sale on the Russian underground market.

platform.socradar.com/app/threat-hunting?q=45.32.148.233

SOCRadar Threat Hunting

You are currently using **Freemium License** for your company. If you want to use more features you can see the subscription plans and request an upgrade.

5/10 Remaining Decks

Remaining Credit

All Results Stealer Logs Reputation Data

Source (46/46) Country (250/250) Sector (41/41) Date Range

Results are searched from 2022-10-19 to 2023-10-25

Infected Device - Accounts for "45.32.148.233" were observed for sale on the Russian Market, On May 28, 2023

Russian Market Bot - 2023 May 28 10:13 UTC

france net android twitter server

45.32.148.233

"passport.twitch.tv",
 "account.pearlabyss.com",
 "pizzahut.fr",
 "digital-world1.com",
 "discordapp.com",
 "pizzahut.fr",
 "unknowncheats.me",
 "blackdesertonline.com",
 "facebook.com",
 "scsmo..."

Data Insights

Source: Russian Market Bot

Discover Date: 28 May 2023 10:13

Content Link: <http://rumakstror5mvgzzodqzofkj3fna71...>

Country: FR

Date: 24 May 2023 00:00

Files: archive.zip

Price: 10.00

Size: 0.32Mb

Stealer: Racoon

Vendor: Mo####yf [Diamond]

Province: Île-de-France

ISP: Societe Francaise Du Radiotelephone - SFR SA

Links: account.ubisoft.com | france-elite.com | namecheap.com | innovation-gaming.fr | warpixel.olympic.in | ...

Tags: france net

Full Content

Domains: 752

IPV4s: 10

Search

Examining the content of the files obtained by the SOCRadar Dark Web team, it became apparent that there was once a phpMyAdmin, a database management tool, on the server. In light of this information, threat actors might have had unauthorized access to this server for a long time and could have been using it in their attacks.

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	



```
*****
*                                     *
*  REOULINE                         *
*                                     *
*  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
=====
```

New Ports

When examining the IPv4 addresses on the search engine named Censys and scanning the ports using the nmap tool, I discovered that, unlike IPv6 scans, each server had nearly 2000 new ports, excluding port 22.



Hosts104.207.158.196

104.207.158.196

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

SummaryHistoryWHOISExplore

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





Hosts



143.42.185.244

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



Hosts



137.220.33.75

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//

```

Having nearly 2000 open ports on a server is not a typical configuration, so I decided to inspect these ports.

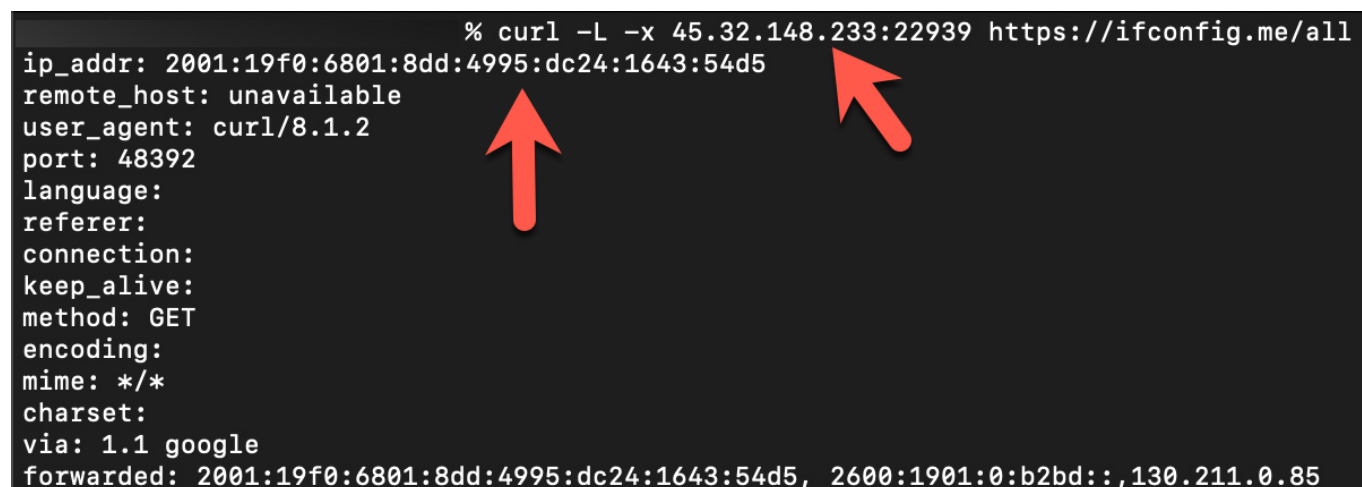
Usually, encountering such a large number of open ports on a system is reminiscent of an open proxy server. Therefore, my initial suspicion was towards a proxy server. As I continued to examine the information about the IPv4 addresses used by the attacker on Censys, a line in the records related to the IPv4 address 45.32.148.233 (Proxy-Connection: close) immediately caught my attention, raising a new question in my mind. Could these be similar to the open proxy servers that were frequently encountered on the Internet in the early 2000s?

Anonymous proxy: This server reveals its identity as a proxy server but does not disclose the originating IP address of the client. Although this type of server can be discovered easily, it can be beneficial for some users as it hides the originating IP address. (Source: Wikipedia)

To find an answer to this question, I used the cURL tool to make a request to the <https://ifconfig.me/all> webpage, specifying the IPv4 address 45.32.148.233 and a random port (22939) listed as a proxy server on Censys. Upon making the request, I observed that the request from the proxy server to this webpage was sent using the IPv6 address

2001:19f0:6801:8dd:4995:dc24:1643:54d5. In short, the answer to the question was “Yes.” These were indeed open proxy servers, allowing me to make web requests to target web pages while hiding my own IPv4 address.

```
% 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
```



However, the proxy server with the IPv6 address 2001:19f0:6801:8dd:4995:dc24:1643:54d5, as shown in the screenshot above, was not one of those involved in the temporary closure of my e-Government account (2001:19f0:6801:8dd:daab:291b:a4d6:dfc7). To determine the relationship between this proxy server and the mentioned IPv6, I prepared a simple script that connects to the open 2000 ports of the IPv4 address 45.32.148.233 and sends a request to the <https://ifconfig.me/ip> webpage.

```
#!/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
```

In each response from the webpage, a different IPv6 address was present. According to this result, malicious individuals could perform a brute-force attack on a webpage using 2000 different IPv6 addresses. After the script ran for a while, I was able to identify the IPv6 address that was responsible for the attack on my e-Government account among these addresses.

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:9394:25b6:6f8a
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:836: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

```

Why are they using an IPv6 address?

While conducting all these investigations, I began to ponder why the attacker chose to use IPv6 addresses. After some time, I realized that the devil is in the details.

When you rent a server from service providers like DigitalOcean, Linode, Vultr, they allocate one IPv4 address to you, and you use this IP address for all your internet-related activities on that server.

Cybercriminals often rent servers from such service providers to carry out or camouflage their cyber attacks. Over time, the IPv4 addresses of servers used in their cyber attacks get detected, blocked, and added to global blacklists by security technologies. As the attempted attacks get thwarted, and their IPv4 addresses become unusable, and with accounts and servers rapidly getting shut down due to complaint notifications, they find themselves in the quest for new servers.

For instance, if we assume that they perform these cyber attacks from 100 servers, paying \$6 per server, they would incur a total cost of \$600. The longer they can carry out these attacks without being detected, the more cost-effective it becomes for them. Otherwise, as they get blacklisted, they repeatedly have to bear this cost as their accounts and servers are shut down.

Now, how does using IPv6 instead of IPv4 change the game? These service

providers typically grant their customers using rented servers only one IPv4 address. However, when it comes to IPv6, they can produce and use thousands of them. This allows malicious actors to conduct their attacks using over a thousand IPv6 addresses by paying just \$6. As they get blacklisted, they can generate and use new IPv6 addresses on the servers they employ, effectively avoiding significant consequences until complaints reach the service provider.

So, did the e-Government application, with its security controls and measures, truly make it difficult for attackers to use IPv4 instead of IPv6? Or did attackers prefer IPv6 to secure their operations? To investigate this, after my e-Government account was temporarily closed due to five incorrect login attempts, I tried to log in with the correct password to my wife's account immediately afterward and successfully gained access.

According to this result, if, in the application or at the network level, an IPv4 account is not blacklisted or blocked when a brute-force attack is attempted on more than two accounts, attackers could carry out these attacks with a single IPv4 address on multiple accounts for an extended period. Otherwise, using IPv6 addresses becomes their only option.

Since I didn't have the chance to test and confirm this on more than two e-Government accounts, and considering that attackers conducted these attacks through IPv6 systems, it is highly likely that e-Government security measures were effective against the IPv4 addresses used by attackers.

How Can I Protect My e-Government Account?

In conclusion, we can see that cyber attackers, over the years, have resorted to various methods to hack Turkish e-Government accounts, utilizing compromised systems forming bot networks, occasionally using their systems, employing proxy server software to hide their tracks and avoid detection, and purchasing servers from service providers with IPv6 support. In short, they have explored every avenue.

So how can you protect yourself from the attacks discussed in this article? The most crucial step you need to take is to use one of the two-factor authentication methods when logging into your e-Government account.

On this occasion, I wish you a happy new year and hope that 2024 brings

health, happiness, and success to you and all your loved ones.

Hope to see you in the following articles.