GO-TO CVE

CVE-2023-31893

(DOS) via DNS Recursion

Week 8

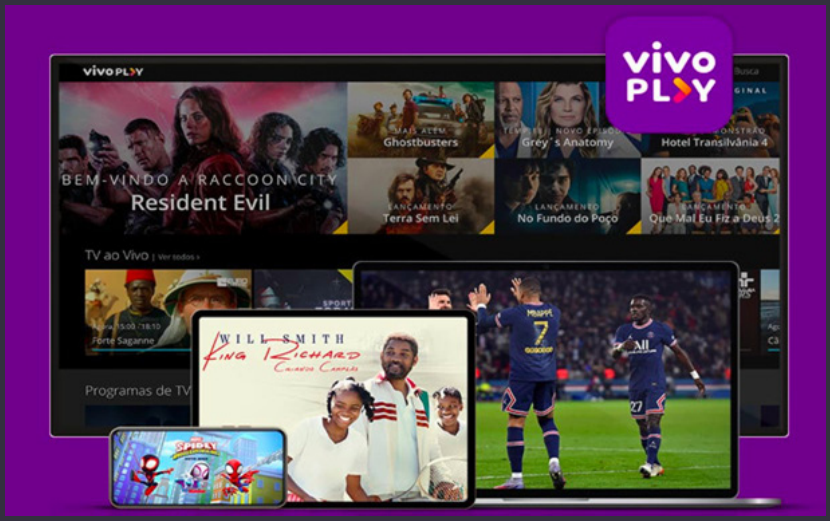
Author : Ali Soltani

مقدمه

سلام به همه عزیزان خوش آمدید به هفته هشتم و تولد دوماهگی از GO-TO CVE. در برنامه این هفته به بررسی CVE-2023-31893 می‌پردازیم که با استفاده از این آسیب‌پذیری روی دستگاه (IPTV Elefnica Brasil Vivo Play) با نسخه Firmware: 2023.04.04.01.06.15 به دلیل قابلیت بازگشتی (DNS (DNS Recursion آسیب‌پذیر منجر به DOS می‌شود که با CVSS : CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/ C:N/I:N/A:H و اسکور 7.5 را به خودش اختصاص داده است که در ادامه به توضیح DNS Recursion و نوع حمله خواهیم داشت؛ با ما همراه همراه باشید ...

درباره Elefnica Brasil Vivo Play

Telefônica Brasil Vivo Play یک سرویس IPTV تلویزیون پروتکل اینترنت است که توسط شرکت مخابراتی بزرگ برزیلی Telefônica Brasil ارائه می‌شود. این سرویس به کاربران اجازه می‌دهد تا محتوای تلویزیونی و ویدیویی را از طریق اینترنت پخش کنند و دسترسی به مجموعه‌ای از کانال‌های زنده و برنامه‌های درخواستی را فراهم می‌کند. Vivo Play با ارائه گزینه‌های متنوع و کیفیت بالا، یکی از خدمات محبوب در بازار سرگرمی‌های دیجیتال در برزیل است.



TL;DR

حمله بازگشت DNS (DNS recursion) به عنوان یک نوع از حملات DDoS، به عنوان یک تهدید جدید برای سرورهای DNS مطرح است. در این حمله، مهاجم با جعل منبع در بسته‌های UDP، سعی می‌کند سرور DNS را فریب دهد تا پاسخ را به یک سرور دیگر (سرور مهاجم) ارسال کند به جای ارسال پاسخ به سرور DNS اصلی.

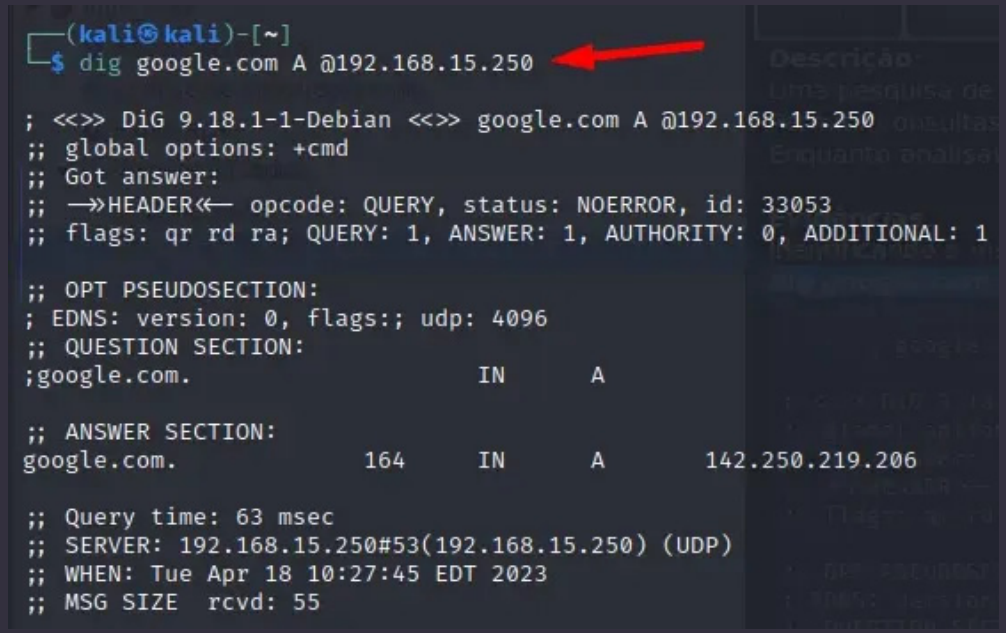
برای انجام این حمله، مهاجم از ویژگی بازگشت (recursion) سرور DNS استفاده می‌کند. وقتی که یک سرور DNS بازگشت را فعال می‌کند، به این معناست که اگر اطلاعات مورد نیاز در دیتابیس خود نباشد، به صورت خودکار از سرور DNS دیگری برای گرفتن این اطلاعات پرس‌وجو می‌کند. این عملیات به عنوان بازگشت در DNS شناخته می‌شود.

مهاجم می‌تواند با جعل منبع بسته‌های UDP، سرور DNS را فریب دهد و پاسخ را به یک سرور قربانی ارسال کند. اگر سرور DNS فریبنده دستورات ANY یا DNSSEC را نیز پشتیبانی کند، مهاجم می‌تواند از این رکوردها برای ارسال پاسخ‌های بزرگ به سرور قربانی استفاده کند.

برای بررسی اینکه آیا یک سرور DNS از بازگشت پشتیبانی می‌کند یا خیر، می‌توانید یک دامنه را پرس‌وجو کنید و در پاسخ دریافتی، بررسی کنید که آیا فلگ ra بازگشت موجود است یا خیر. اگر پرچم موجود باشد، این نشان دهنده پشتیبانی از بازگشت است و این ممکن است یک نقطه ضعف امنیتی باشد که باید بررسی شود برای مطالعه بیشتر میتونید به دو لینک CVE-2023-31893 , ?DNS recursivo مراجعه کنید.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-31893

/https://www.cloudflare.com/pt-br/learning/dns/what-is-recursive-dns



درباره DNS Recursion و مانیتورنیگ لاگ ها

DNS Recursion فرآیندی در سیستم DNS (Domain Name System) است که طی آن یک DNS Resolver درخواست کاربر را برای تبدیل نام دامنه به آدرس IP به صورت بازگشتی پیگیری می‌کند. این فرآیند با ارسال درخواست به سرورهای ریشه (Root Servers) آغاز می‌شود. سرورهای روت اطلاعاتی درباره سرورهای دامنه TLD)) را برمی‌گردانند. سپس DNS Resolver به سرورهای TLD مربوطه مراجعه می‌کند تا آدرس سرورهای Authoritative Name Servers)) دامنه مورد نظر را دریافت کند. در نهایت، DNS Resolver با مراجعه به سرورهای (ANS)، آدرس IP نهایی را به دست آورده و آن را به کاربر برمی‌گرداند. این فرآیند تضمین می‌کند که کاربر نیاز ندارد تمام مراحل را خودش انجام دهد، بلکه DNS Resolver

تمام مراحل را به صورت خودکار انجام می‌دهد. DNS Recursion برای افزایش کارایی و سهولت استفاده از اینترنت استفاده می‌شود.

مزایا و معایب DNS Recursion

مزایا:

- کارآمدی: کاربر نیاز ندارد تا تمام مراحل پرس و جو را خودش انجام دهد. DNS Resolver این کار را به صورت اتوماتیک انجام می‌دهد.
- کاهش بار روی سرورها: به دلیل استفاده از کش Cache، تعداد پرس و جوهای لازم کاهش می‌یابد.
- پایداری و قابلیت اعتماد: به دلیل استفاده از مکانیزم‌های توزیع شده و سلسله‌مراتبی، DNS به شدت پایدار و قابل اعتماد است.

معایب:

- انواع حملات DNS Amplification: این نوع حملات با سواستفاده از ویژگی‌های Recursion می‌تواند ترافیک زیادی ایجاد کرده و باعث حملات منع سرویسDDoS شود.
- تاخیر اولیه: ممکن است تاخیر اولیه برای کاربر کمی بیشتر باشد زیرا DNS Resolver باید چندین پرس‌وجو انجام دهد.

تفاوت بین Recursive و Iterative Queries

- Recursive Queries: در این نوع پرس‌وجو، DNS Resolver تمام کارهای لازم برای پیدا کردن آدرس IP نهایی را انجام می‌دهد و به کاربر پاسخ نهایی را برمی‌گرداند. کاربر تنها یک پرس‌وجو به DNS Resolver ارسال می‌کند.
- Iterative Queries در این نوع پرس و جو، DNS Resolver تنها اطلاعاتی که دارد یا می‌تواند از منابع بالاتر بدست آورد را برمی‌گرداند و کاربر یا کلاینت DNS باید خود مراحل بعدی را پیگیری کند.

امنیت در DNS Recursion

امنیت در DNS Recursion یکی از مسائل حیاتی در امنیت شبکه است. DNS Recursion به طور بالقوه می‌تواند نقاط ضعف و آسیب‌پذیری‌هایی را معرفی کند که مهاجمان می‌توانند از آن‌ها سوءاستفاده کنند. در ادامه به برخی از مهم‌ترین تهدیدها و روش‌های مقابله با آن‌ها پرداخته خواهد شد.

تهدیدهای امنیتی در DNS Recursion

1. DNS Cache Poisoning

در این حمله، مهاجم تلاش می‌کند تا اطلاعات نادرستی را وارد کش DNS Resolver کند. اگر این اطلاعات نادرست وارد کش شود، کاربران بعدی که به همان DNS Resolver مراجعه می‌کنند، به سایت‌های جعلی هدایت می‌شوند.

روش‌های مقابله:

- استفاده از: DNSSEC (DNS Security Extensions) فرآیند DNSSEC به امضای دیجیتال داده‌های DNS می‌پردازد و اصالت داده‌ها را تضمین می‌کند.
- اعتبارسنجی پاسخ‌ها: بررسی اصالت و درستی پاسخ‌های دریافتی از سرورها توسط DNS Resolver

2. حملات منع سرویس DDoS مبتنی بر DNS Amplification

DNS Amplification Attack یکی از انواع حملات DDoS (Distributed Denial of Service) است که از ویژگی‌های بازگشتی DNS (DNS Recursion) برای تقویت ترافیک و حمله به سرور هدف استفاده می‌کند. در این نوع حمله، مهاجم درخواست‌های کوچک DNS را به یک DNS Resolver ارسال می‌کند که منجر به تولید پاسخ‌های بزرگ می‌شود و این پاسخ‌ها به آدرس IP قربانی ارسال می‌شود، باعث افزایش حجم ترافیک و ایجاد بار زیاد روی سرور قربانی می‌گردد.

روش‌های مقابله:

- پیکربندی صحیح سرورهای DNS: جلوگیری از پاسخ‌دهی به درخواست‌های بازگشتی غیرمجاز.
- استفاده از فیلترهای ترافیک: تشخیص و مسدود کردن ترافیک‌های مشکوک.

3. حملات DNS Spoofing

در این حمله، مهاجم تلاش می‌کند تا کاربران را به سمت سرورهای جعلی هدایت کند. این کار معمولاً با پاسخ‌های جعلی به درخواست‌های DNS انجام می‌شود.

روش‌های مقابله:

- استفاده از DNSSEC: اطمینان از صحت و اعتبار پاسخ‌های DNS
- نظارت و مانیتورینگ ترافیک: تشخیص و پاسخ به فعالیت‌های مشکوک در شبکه

این بخش که توضیحاتی درمورد مانیتوریگ و لاگ برداری از DNS recursion را از پست خانوم ShiRiN Mortaz Hejri برداشته شده است .

DNS Recursion و لاگ‌برداری و مانیتورینگ آن‌ها

برای مانیتورینگ و دریافت لاگ‌های مرتبط با DNS Recursion، می‌توانید از لاگ‌های زیر استفاده کنید:

- DNS Query Logs: لاگ‌های مربوط به درخواست‌های DNS
- DNS Response Logs: لاگ‌های مربوط به پاسخ‌های DNS
- DNS Recursive Query Logs: لاگ‌های مربوط به درخواست‌های بازگشتی DNS

مثال‌های تنظیم لاگ

اگر از UF (Universal Forwarder) استفاده می‌کنید و مدیریت ارسال لاگ‌ها را انجام داده‌اید، می‌توانید از تنظیمات زیر استفاده کنید:

```
[monitor:///var/log/named/query.log]
sourcetype = dns_query_logs
index = dns_logs

[monitor:///var/log/named/response.log]
sourcetype = dns_response_logs
index = dns_logs
```

تشخیص حملات با استفاده از SPL

در اینجا دو مثال از دستورات SPL (Search Processing Language) برای تشخیص حملات DNS Amplification و Cache Poisoning آورده شده است. توجه داشته باشید که این دستورات باید در محیط‌های تحلیل لاگ مانند Splunk استفاده شوند.

1. DNS Amplification Attack Detection

```
# جستجوی لاگ‌های DNS
from index="dns_logs" sourcetype="dns_query_logs"
| eval query_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
| fields query_time, client_ip, query_domain, query_type

# جستجوی لاگ‌های جواب DNS
from index="dns_logs" sourcetype="dns_response_logs"
| eval response_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
| fields response_time, client_ip, query_domain, response_type, response_size

# ترکیب لاگ‌ها
| join client_ip, query_domain [
 from index="dns_logs" sourcetype="dns_query_logs"
 | fields client_ip, query_domain, query_time
]
| join client_ip, query_domain [
 from index="dns_logs" sourcetype="dns_response_logs"
 | fields client_ip, query_domain, response_time, response_size
]

# فیلتر برای پاسخ‌های بزرگ و درخواست‌های کوچک
| where response_size > 1000
| fieds query_time, client_ip, query_domain, query_type, response_time,
response_size
```

```
# جستجوی لاگ‌های DNS
from index="dns_logs" sourcetype="dns_query_logs"
| eval query_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
| fields query_time, client_ip, query_domain, query_type

# جستجوی لاگ‌های جواب DNS
from index="dns_logs" sourcetype="dns_response_logs"
| eval response_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
| fields response_time, client_ip, query_domain, response_type, response_data

# ترکیب لاگ‌ها
| join client_ip, query_domain [
 from index="dns_logs" sourcetype="dns_query_logs"
 | fields client_ip, query_domain, query_time
]
| join client_ip, query_domain [
 from index="dns_logs" sourcetype="dns_response_logs"
 | fields client_ip, query_domain, response_time, response_data
]

# فیلتر برای شناسایی پاسخ‌های نادرست
| where response_data matches ".*unexpected_domain.*"
| fields query_time, client_ip, query_domain, query_type, response_time,
response_data
```

با استفاده از BIND 9 هم می‌توانید مشکل سرورهای DNS بازگشتی رو به دو روش حل کنید که در ادامه به بررسی آنها می‌پردازیم.
استفاده از Views: در این روش، شما می‌توانید سرورهای DNS Recursion , Authoritative Name Server را در یک سرور اجرا کنید و از طریق Views آن‌ها را جدا کنید. Views در BIND 9 به شما امکان می‌دهد که بر اساس معیارهای مختلفی مانند آدرس IP کلاینت‌های‌تان، پاسخ‌های متفاوتی را ارائه دهید. این راه‌حل مناسب برای مواردی است که نیاز به اجرای هر دو نوع سرور (DNS Recursion , Authoritative Name Server) در یک سرور را دارید.

برای پیکربندی با استفاده ازViews، شما باید تعریف کنید که کدام نوع از کلاینت‌ها می‌توانند از سرویس بازگشتی استفاده کنند و کدام‌ها نه. این تنظیمات در فایل پیکربندی named.conf انجام می‌شود. مثلاً:

```
// تعریف ACL برای مشتریان مجاز
acl trusted_clients {
    localhost;
    192.168.1.0/24;
};

// تعریف view داخلی برای مشتریان مجاز
view "internal" {
    match-clients { trusted_clients; };
    recursion yes;  // اجازه بازگشتی برای مشتریان مجاز
    // تعریف مناطق معتبر اینجا
};

// تعریف view دیگر برای مشتریان عمومی
view "external" {
    match-clients { any; };
    recursion no;   // عدم اجازه بازگشتی برای مشتریان عمومی
    // تعریف مناطق معتبر اینجا
};
```

در این مثال، trusted_clients شامل localhost و زیرشبکه 24/192.168.1.0 است که می‌توانند از سرویس بازگشتی استفاده کنند. دو view به نام internal و external تعریف شده‌اند که هر کدام شرایط دسترسی و تنظیمات بازگشتی متفاوتی دارند.
می‌توانید دو سرویس را در دو سرور متفاوت نصب کنید و پیکربندی کنید.

نتیجه‌گیری

حملات DNS Amplification و Cache Poisoning از جمله تهدیدات جدی برای سیستم‌های DNS هستند که می‌توانند با استفاده از ویژگی‌های بازگشتی DNS، بار زیادی بر سرورها وارد کرده و اطلاعات نادرست را وارد کش کنند. با تنظیم صحیح لاگ‌ها و استفاده از دستورات SPL برای مانیتورینگ و تحلیل لاگ‌ها، می‌توان این حملات را شناسایی و از آن‌ها جلوگیری کرد. تنظیمات ارائه شده و دستورات SPL به شما کمک می‌کنند تا لاگ‌های مورد نیاز را جمع‌آوری و تحلیل کرده و امنیت سیستم DNS خود را افزایش دهید.

جزئیات و بهره برداری از آسیب پذیری

در زمان تجزیه و تحلیل دستگاه توسط مهاجمان یک جستجوی DNS بازگشتی رخ می‌دهد، زمانی که یک سرور DNS با دیگر سرورهای DNS تعامل برقرار کرده و یک آدرس IP را به کلاینت ارائه می‌دهد. اجازه دادن به درخواست‌های DNS بازگشتی در برابر سرورهای DNS باز یک آسیب‌پذیری امنیتی ایجاد می‌کند که می‌تواند به مهاجمان این امکان را بدهد که از سرور برای حملات تقویت DNS بهره ببرند. در این نوع حملات، مهاجمان درخواست‌های جعلی ارسال می‌کنند که به پاسخ‌های DNS بلند و غیرموردی منجر می‌شود، که می‌تواند سرور را بارگیری کند یا حتی آن را از کار انداخته و خراب کند. نسخه‌ای که در آن فریمور آزمایش شده است 2023.04.04.01.06.15 است .

جزییات آسیب‌پذیری:

- روش DNS بازگشتی فعال شده: این امر با استفاده از دستور زیر در ابتدای مقاله تأیید شده است.

```
dig google.com A @192.168.15.250
```

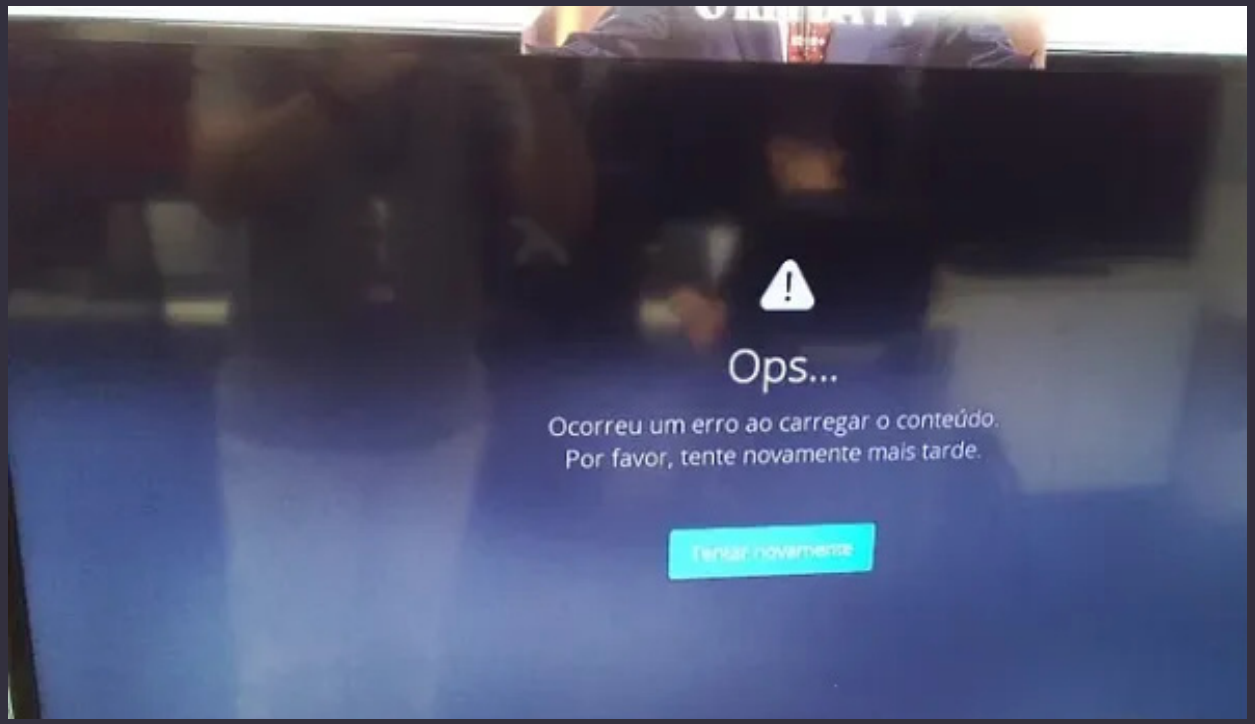
استفاده از ابزار حمله: در این تست از ابزار حمله به نام DDoS Ripper استفاده شد که با ارسال پاسخ‌های DNS، تارگت را با ترافیک هدف قرار می‌دهد.

- اثبات عملی PoC:

```
python3 DRipper.py -s 192.168.15.250 -t 135 -p 53
```

liangroup.net

اثرات: دستگاه پس از انجام حمله تجربه ناپایداری سیستم و قطع خدمات را تجربه کرد. این حملات به واسطه فرستادن درخواست‌های جعلی که پاسخ‌های DNS بلند و ناخواسته را درخواست می‌دهند، سرور را به مشکل می‌اندازند و به خرابی سرویس می‌انجامد.



جلوگیری

- مانیتورینگ و ریسپانس: رصد و مانیتورینگ فعالیت‌های شبکه و ترافیک DNS می‌تواند به شناسایی حملات در حال انجام و اقدامات پیش‌گیرانه کمک کند. همچنین، برنامه‌ریزی برای پاسخ‌گویی به حملات و اعمال تغییرات در تنظیمات به‌صورت سریع واکنش‌گر می‌تواند ضروری باشد.
- به‌روزرسانی نرم‌افزارها و تنظیمات امنیتی: به‌روزرسانی سیستم‌عامل، نرم‌افزارهای مربوط به سرور DNS و دیگر نرم‌افزارهای امنیتی می‌تواند به شما کمک کند تا از آسیب‌پذیری‌هایی که در نسخه‌های قدیمی وجود دارند، جلوگیری کنید.
- استفاده از Firewalls و IDS/IPS: استفاده از فایروال‌ها و سیستم‌های جلوگیری از نفوذ IDS/IPS می‌تواند به شناسایی و جلوگیری از حملات بازگشت DNS کمک کند. این سیستم‌ها می‌توانند قابلیت‌هایی مانند تشخیص الگوهای حمله، امضای شناخته شده حملات و محدودسازی ترافیک را ارائه دهند.
- تنظیمات امنیتی در سرور DNS: اعمال تنظیمات امنیتی مانند فیلترینگ و محدود کردن دسترسی به انواع پرس‌وجوهای DNS و همچنین محدود کردن حجم ترافیک می‌تواند کمک کننده باشد. همچنین، ممکن است از روش‌های مانند rate limiting برای محدود کردن تعداد پرس‌وجوهایی که یک مشتری می‌تواند انجام دهد، استفاده شود.

و در آخر همیشه بروز باشید و به توصیه‌های تیم امنیت خود گوش دهید به امید فردایی امن‌تر تا هفته‌های بعدی همراه ما باشید .

منابع

- https://www.linkedin.com/in/shirinmortaz/
- cert.br
- medium.com
- opencve.io
- amazon.com
- DDoS-Ripper


LIANGROUP.NET
021 9100 41 51 (300)