APJ. 5(1):12-23, Spring 2024

Arman Process Journal (APJ)

Homepage: armanprocessjournal.ir

Securing the Internet of Things Network by Detecting and Countering Distributed Denial of Service Attacks

M. Birjandi [*,1]

[1] *Computer Engineering Department, Islamic Azad University, Electronic Branch, Tehran, Iran*

Received: 25 January 2023
Accepted: 9 May 2024

KEYWORDS:
Denial of Service Attacks,
Internet of Things,
Block Chain,
Intrusion Detection System,

[1] Corresponding author
m.birjandi1@gmail.com

ABSTRACT

Nowadays, the Internet of Things (IoT) has emerged as an effective and innovative technology for developing the infrastructure of many hardware and related software applications. Moreover, blockchain technology has emerged as the backbone for the development of IoT-based applications. The use of blockchain in the Internet of Things as a reliable and safe system can help improve the security and quality of the Internet of Things network and in the long run lead to energy savings and improve the efficiency of these systems. However, security challenges, including distributed service breach attacks, have revealed a fundamental fault line within the blockchain-based IoT network. Therefore, according to the necessity of the problem, in this article, we intend to first examine the types of security challenges and denial of service attacks in Internet of Things networks based on block chains and then examine and propose solutions for identifying, managing and dealing with these attacks. Certainly, the correct use of such security approaches can be effective toward securing Internet of Things environments and create more quality and reliable services and increase users' acceptance of these services.

NUMBER OF REFERENCES **27**

NUMBER OF FIGURES **0**

NUMBER OF TABLES **1**

نشریه تخصصی آرمان پردازش، دوره ۵، شماره ۱، بهار ۱۴۰۳

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

ایمن سازی شبکه اینترنت اشیا با شناسایی و مقابله با حملات انکار سرویس توزیع شده

محمد بیرجندی*[1]

دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد الکترونیک، تهران، ایران

چکیده

امروزه اینترنت اشیا به عنوان تکنولوژی موثر و نوینی برای توسعه زیر ساخت بسیاری از سخت افزارها و برنامه های کاربردی مرتبط، ظاهر شده است. همچنین، فناوری زنجیره های بلوکی به عنوان ستون فقراتی برای توسعه برنامه های کاربردی بر پایه اینترنت اشیا پدیدار شده است. استفاده از بلاکچین در اینترنت اشیا به عنوان یک سیستم قابل اعتماد و امن، می‌تواند به بهبود امنیت و کیفیت شبکه اینترنت اشیا کمک کند و در طولانی مدت منجر به صرفه‌جویی در مصرف انرژی و بهبود کارایی این سیستم‌ها شود. هرچند، چالش های امنیتی از جمله تهاجم نقض سرویس توزیع شده، خط گسله ای اساسی در میان شبکه ی اینترنت اشیای دارای زنجیره ی بلوکی را نمایان کرده است. لذا بنا به ضرورت مساله، در این مقاله قصد داریم ابتدا انواع چالش های امنیتی و حملات انکار سرویس در شبکه های اینترنت اشیا مبتنی بر زنجیره های بلوکی را بررسی نموده وسپس راهکارهای شناسائی، مدیریت و مقابله با این حملات را بررسی و پیشنهاد نمائیم. مسلما بهره گیری صحیح از چنین رویکردهای امنیتی می تواند در جهت ایمن سازی محیط های اینترنت اشیاء موثر بوده و خدمات با کیفیت تر و قابل اطمینان تری را ایجاد نماید و استقبال کاربران از این خدمات را افزایش دهد.

واژگان کلیدی:
حمله ی انکار سرویس توزیع شده،
اینترنت اشیا،
زنجیره ی بلوکی،
سیستم تشخیص تهاجم،

تعداد جداول	تعداد شکل ها	تعداد مراجع
۱	۰	۲۷

مقدمه

امروزه اینترنت اشیا یا IoT[1] به عنوان فناوری جدیدی که با پیشرفت اینترنت، با زندگی روزمره ی ما ادغام شده است ظهور نموده است. برنامه های بر پایه IoT از جمله مدیریت زنجیره تامین، بهداشت و درمان و سیستم مدیریت هویت مبتنی بر RFID[2] به طور مستقیم باعث ارتقای افراد و خدمات در جوامع فناور محور می شوند و پیشرفت در حوزه توسعه مبتنی بر IoT موجب رشد بخش های مختلفی در دولت های الکترونیک می گردد [۱]. اگرچه، برنامه های ساخته شده توسط سیستم های مبتنی بر IoT بیشتر بر روی ذخیره سازی متمرکز و معماری کامپیوتر کار می کند،اما مدل ذخیره سازی متمرکز دارای نقص های امنیتی و حریم خصوصی بسیاری است. مدل کارکردی زیربنایی دارای محدودیت هایی برای تسهیل توسعه سیستم مبتنی بر IoT در آینده ی نزدیک است. از این رو، برای رسیدگی به این مشکلات، نیاز به مدل ذخیره سازی غیر متمرکز یا توزیع شده وجود دارد. یکی از معماری های نوظهور بر پایه سیستم ذخیره و بازیابی غیرمتمرکز، فناوری زنجیره های بلوکی[3] است. زنجیره های بلوکی، مدل ذخیره سازی غیر متمرکز و تغییر ناپذیر است که شامل تمامی جزئیات نقل و انتقالاتی که توسط گره ی همتا در شبکه آغاز شده است. مفهوم ذخیره سازی غیر متمرکز، دفتر کل توزیع شده نامیده می شود [۲]. هر انتقالی که در دفترکل اعمال می شود، از طریق موافقت اکثریت مشارکت کنندگان در شبکه تایید می شود. بیت کوین، بی درنگ محبوب ترین پیاده سازی فناوری زنجیره های بلوکی است. یکپارچگی زنجیره های بلوکی و IoT می تواند مزایای بسیاری داشته باشد که از جمله میتوان به قابلیت مدل ذخیره سازی غیر متمرکز زنجیره های بلوکی به منظور انطباق دستگاه های IoT و ارائه ی داده ی زمان برای هر گره ی IoT اشاره کرد. این مدل یکپارچه سازی زیر بنایی، وابستگی به شخص ثالث و نقطه ی آسیب پذیری مرکزی را حذف می کند. علاوه بر این، یکپارچه سازی IoT با زنجیره های بلوکی می تواند پیام رسانی همتا به همتا، اشتراک گذاری فایل و داده ی زمان و ارتباط مستقل بین گره های IoT را بدون نیاز به مدل مشتری-سرور متمرکز، فراهم آورد [۴-۳].

با وجود قابل تایید و غیرقابل تغییر بودن زنجیره های بلوکی ، اما هنوز در مقابل حملات مختلف آسیب پذیر است. یکپارچه سازی IoT و زنجیره های بلوکی در زمینه ی تغییر اساسی برنامه های خود اتکای IoT، رشد بزرگی را تجربه کرده است. هرچند که متناسب با آن، تعداد حملات هم افزایش یافته است.

حمله محروم‌سازی از سرویس یا به اختصار DoS[4]، تلاش برای خارج کردن ماشین و منابع شبکه از دسترس کاربران مجازش است. در واقع هر حمله‌ای علیه دسترس پذیری به عنوان حمله منع سرویس تلقی می‌شود. اگرچه منظور از حمله DoS و انگیزه انجام آن ممکن است متفاوت باشد، اما به‌طور کلی شامل تلاش برای قطع موقت یا دائمی یا تعلیق خدمات یک میزبان متصل به اینترنت است. اگر مهاجم برای حمله از یک میزبان استفاده کند به این نوع حمله DoS می‌گوییم ولی حمله DDoS[5]زمانی اتفاق می‌افتد که چندین سیستم به‌طور هم‌زمان پهنای باند یا منابع سیستم مورد هدف را با بسته‌های سیل‌آسا مورد حمله قرار دهند [۵]. وقتی سروری با اتصالات زیادی دچار سربار شود، دیگر نمی‌تواند اتصالات جدیدی را بپذیرد. مزیت عمده‌ای که استفاده از حمله منع سرویس توزیع شده برای مهاجم دارد این است که ماشین‌های چندگانه می‌توانند ترافیک بیشتری را نسبت به یک ماشین تولید کنند و همچنین مسدود کردن منبع حمله را به علت وجود منابع متعدد در حمله غیرممکن می‌سازد. در روش DDoS تمام رایانه‌ها هم‌زمان با هم عمل می‌کنند به‌طوری‌که ممکن است در برخی موارد خسارات جبران‌ناپذیری به بار آورند. در این روش معمولاً مهاجم سیستم‌های زیادی را آلوده کرده و به آن‌ها هم‌زمان فرمان می‌دهد. به سیستم‌های آلوده شده زامبی (zombie) و به شبکه‌ای از این سیستم‌ها که تحت کنترل یک شخص هستند، botnet گفته می‌شود. حملات DDoS[6] که اغلب توسط سیل بر روی استخر حافظه در شبکه زنجیره های بلوکی ایجاد می شوند، پیامدهای شدیدی بر کاربران قانونی دارند [۶].

در شبکه های زنجیره های بلوکی موجود، حملات DDoS بیشتر استخراج کنندگان (استخر حافظه)، کاربران و واسط ارتباطی آن ها را مورد هدف قرار می دهند. در سیستم نظیر به نظیر، DDoS ممکن است به صورتی متفاوت مانند خود راه اندازی شبکه ی زنجیره های بلوکی، کاربران و استخراج کنندگان به سوی شبکه های ساختگی و تقلبی از طریق رد کردن دسترسی به شبکه ی اصلی، اجرا شود. این فرآیند ممکن است توسط هکر از طریق دزدیدن تعدادی پیشوند قرارداد دروازه مرزی اجرایی گردد [۷]. راه دیگر هدف گذاری حمله ی DDoS در شبکه ی زنجیره های بلوکی از طریق سیل حملات بر استخر حافظه با انتقالات هرز توسط مهاجم در شبکه است. در زنجیره بلوکی، استخر حافظه به عنوان مخزن تراکنشی که در آن تمامی انتقالات به اشتراک گذاشته شده توسط همتایان در ابتدا ثبت شده و در انتظار تایید هستند، عمل می کند. به محض اینکه گره IoT انتقالات را به وجود آورد، در بین همه ی گره های همتای IoT همگام شده، انتشار می یابد. تراکنش های افزایش یافته برای تایید در استخر حافظه، منتظر می مانند. هنگامی که حجم استخر حافظه توسط تراکنش های تایید نشده افزایش می یابد، کاربران واقعی باید هزینه ی استخراج بیشتری برای در اولویت قرار گرفته شدن تراکنش های تایید نشده ی خود بپردازند و این موقعیت به فرصتی برای مهاجمان تبدیل می شود. علاوه بر این، یک ساز و کار ایمن

[1] Internet of Thing (IoT)
[2] Radio Frequency Identification (RFID)
[3] BlockChain
[4] Denial of Service attack (DoS)
[5] Distributed Denial of Service attack (DDoS)
[6] Distributed Denial-of-Service (DDoS) Attack

و امنیتی با ثبات برای شناسایی حملات DDoS، مورد نیاز است. از طرف دیگر، داده های ایجاد شده توسط این برنامه ها، حجیم بوده و باعث ایجاد مشکلاتی مربوط به ابر داده ها می شوند. از این رو، برای رسیدگی به این مشکل، عموما هوش مصنوعی به عنوان ابزاری تحلیلی عمل کرده و اطلاعات سودمندی را به منظور تصمیم گیری، طبقه بندی، پیش بینی و شناسایی اقدامات آتی در شبکه ی IoT دارای زنجیره های بلوکی، ارائه می دهد [۸].

بر اساس تحقیقات مرتبط، تعداد زیادی مشکلات و چالش های امنیتی در استخر استخراج شبکه ی IoT دارای زنجیره ی بلوکی رخ داده است. افزایش حملات DDoS در اکوسیستم زنجیره ی بلوکی IoT، کل شبکه ی IoT دارای زنجیره ی بلوکی را آسیب پذیر می کند. چالش های اصلی در زیر ذکر شده است [۱۱-۹]:

- تضمین کردن چارچوب امنیتی توزیع شده برای شبکه ی IoT دارای زنجیره ی بلوکی کار چالش برانگیزی است.
- اطمینان از یک مکانیسم امنیتی که از ابزار تحلیلی مناسب در معماری کاری توزیع شده، استفاده کند و توانایی مدیریت ابر داده های تولید شده توسط دستگاه های IoT به شیوه ای توزیع شده را دارا باشد.
- ساخت IDS موثر که بتواند تراکنش های معمولی و حمله را از هم متمایز سازد، کاری دشوار است. تحقیقات زیادی برای مکانیسم امنیتی کاهش دادن حملات DDoS در برابر استخرهای استخراج در شبکه ی IoT دارای زنجیره ی بلوکی پس از قرارگیری مدل ، قابل مشاهده نیست.

لذا بنا به ضرورت تحقیق در این حوزه، در این مقاله قصد داریم به چالش های امنیتی مرتبط پرداخته و راهکارهای موثر را بررسی نمائیم. دریخش بعدی ابتدا خطرات امنیت سایبری اینترنت اشیا را بررسی خواهیم نمود.

خطرات امنیت سایبری اینترنت اشیا

در حال حاضر، دستگاه‌های IoT طوفانی کامل از آسیب‌پذیری امنیت سایبری هستند. لذا پیاده سازی امنیت در اینترنت اشیا دشوار است و دسترسی به امنیت در دستگاه‌های IoT دشوار است. برنامه نویسی خود دستگاه با برنامه نویسی رابط کاربری برنامه بسیار متفاوت است و همه این موارد معمولاً باید روی سیستم عامل بالقوه اختصاصی و کم مصرف کار کنند. این به معنای قدرت محاسباتی محدود برای هر نوع رمزگذاری، رمزگشایی یا سایر فرآیندهای ابتدایی مبتنی بر امنیت است. بسیاری از دستگاه های اینترنت اشیا با لاگین های پیش فرض ارسال می شوند. به جای دادن یک نام کاربری و رمز عبور منحصر به فرد به هر دستگاه، دادن رمز عبور و لاگین پیش فرض به آنها بسیار ساده تر است. این امر ورود هکر ها به آنها را بسیار آسان می کند. تا زمانی که بتوانند آنها را پیدا کنند. دستگاه های اینترنت اشیا میزبان بدافزار های عالی هستند. از آنجایی که امنیت آنها مشکوک است، دستگاه های اینترنت اشیا اغلب می توانند برای میزبانی و اجرای بدافزارهای ابتدایی استفاده شوند. همچنین آنها در حملات DDoS بسیار مفید هستند، که نیاز به انبوهی از دستگاه‌هایی دارند که از ربات‌های ساده استفاده می‌کنند تا اهداف خود را باتلاق کنند.

حتی اگر دستگاه اینترنت اشیا شما کاملاً ایمن باشد، خطر بزرگ دیگری وجود دارد: نقض حریم خصوصی. این دستگاه ها برای جمع آوری داده ها برای سازندگانشان بدنام هستند. این داده‌ها ظاهراً فقط برای بهبود دستگاه‌هایشان استفاده می‌شوند، اما تعداد کمی از سازمان ها و شرکت‌ها می‌توانند در برابر قیمتی که اطلاعات دقیق کاربر می‌تواند دریافت کند، مقاومت کنند [۱۲].

حملات IoT یک جرم سایبری علیه دستگاه های اینترنت اشیا است. این دستگاه‌ها می‌توانند به دلیل تدابیر امنیتی ضعیف اینترنت اشیا، سیستم عامل قدیمی و طراحی ضعیف سیستم، در معرض ربودن قرار بگیرند. در این قسمت برخی از رایج ترین انواع حملات اینترنت اشیا آورده شده است [۱۴-۱۳]:

- جعل : دستگاه نوعی حمله که در آن یک دستگاه مخرب آدرس IP، آدرس MAC یا سایر اطلاعات شناسایی یک دستگاه معتبر را دستکاری می‌کند و وانمود می‌کند که یک مورد قانونی است.
- حملات Man-in-the-Middle (MitM) : مفهوم حمله MitMشامل رهگیری ارتباط بین دو سیستم توسط هکر است. مهاجم فرستنده اصلی را جعل می کند تا طرف مقابل را فریب دهد تا فکر کند در حال دریافت یک پیام قانونی است. MitM معمولا برای استخراج اطلاعات حساس و ایجاد اختلال در خدمات انجام می شود.
- حملات انکار سرویس توزیع شده (DDoS) : حملات DDoS به دستگاه‌های اینترنت اشیا، شبکه را با پر کردن ترافیک ثابت، مانند درخواست‌های جعلی، بیش از حد بار می‌کنند. به این ترتیب، یک مهاجم سیستم را تحت الشعاع قرار می دهد، آن را از کار می اندازد و باعث انکار سرویس به کاربران قانونی می شود.
- استراق سمع : عوامل تهدید برای رهگیری و گوش دادن یا نظارت بر ارتباطات بین دستگاه‌های اینترنت اشیا، استراق سمع انجام می‌دهند، که به آن استراق سمع یا جاسوسی نیز می‌گویند.
- حملات بدافزار: مجرمان سایبری برای دسترسی غیرمجاز به داده های محرمانه و حساس، کنترل دستگاه یا جاسوسی از فعالیت های شبکه یا مکالمات، نرم افزارهای مخرب را روی دستگاه های اینترنت اشیا نصب می کنند.
- حملات روز صفر : در طول یک حمله روز صفر، یک هکر از آسیب‌پذیری‌های اصلاح‌نشده در نرم‌افزار دستگاه‌های اینترنت اشیا که قبلاً برای مهندسان امنیت سایبری ناشناخته بود، سوء استفاده می‌کند. چنین حملاتی خطرناک هستند زیرا هیچ راه حلی در طول حمله وجود ندارد.

- شکستن رمز عبور : هکرها از روش‌های مختلفی مانند حملات Brute Force برای رمزگشایی رمزهای عبور سیستم و دسترسی به دستگاه‌های IoT استفاده می‌کنند. هرچه کلمات رمز و گذرواژه‌های پیش‌فرض و شیوه‌های رمز عبور ضعیف‌تر باشند، نفوذ کردن سیستم‌های IoT برای مهاجمان آسان‌تر است.
- دستکاری سیستم عامل : در این نوع حمله، یک مجرم سایبری سخت افزار دستگاه مبتنی بر اینترنت اشیا را تغییر می‌دهد تا عملکرد آن را تغییر دهد و اقدامات مخرب بیشتری انجام دهد.

وجود این حجم از رایج ترین حملات امنیتی در حوزه اینترنت اشیا بر اهمیت اقدامات امنیتی قوی مانند به روز رسانی منظم نرم افزار، رمزهای عبور ایمن و سیستم های تشخیص نفوذ (IDS) تاکید می کند. همچنین موارد زیر رایج ترین دلایلی هستند که چرا دستگاه های IoT ممکن است به یک شکار شیرین برای هکرها تبدیل شوند [۱۵]:

- رمزهای عبور ضعیف: یکی از دلایل اساسی که دستگاه‌های اینترنت اشیا هدف اصلی عوامل تهدید هستند، گذرواژه‌های پیش‌فرض یا قابل حدس زدن آسان است که به آن‌ها اجازه می‌دهد با تلاش کمی وارد دستگاه شوند.
- ذخیره سازی ابری ناامن: عدم حفاظت در فضای ذخیره سازی ابری ممکن است به هکرها اجازه دهد تا داده های محرمانه شما را به راحتی دستکاری یا سرقت کنند.
- نرم افزار بدون وصله: از آنجایی که نرم‌افزار یا سخت‌افزارهای قدیمی اینترنت اشیا حاوی آسیب‌پذیری‌های شناخته‌شده است، برای عوامل تهدید راه‌حلی برای سوءاستفاده از نقاط ضعف فراهم می‌کند.
- اتصالات شبکه ناامن: شبکه‌های Wi-Fi عمومی یا ناامن خطر حمله به دستگاه‌ها را افزایش می‌دهند و روند کنترل هکرها بر آنها را تسهیل می‌کنند.
- عدم وجود تمهیدات امنیتی و رمزگذاری: هر کسی که ترافیک رمزگذاری نشده شما را رهگیری کند می تواند آن را بخواند. این برای هر ترافیکی که انتخاب می‌کنید خارج از تونل VPN ایمن رها کنید صدق می‌کند، افشای اطلاعات حساس یک خطر بزرگ امنیتی تونل سازی است.
- دستکاری فیزیکی: دسترسی فیزیکی به یک دستگاه اینترنت اشیا ممکن است به مهاجمان اجازه دهد داده های حساس را استخراج کنند، سیستم عامل مخرب را نصب کنند و امنیت دستگاه های اینترنت اشیا شما را به خطر بیندازند.
- اعتماد و اتکای فزاینده به دستگاه‌های اینترنت اشیا: بسیار مهم است که مراقب این تهدیدات امنیتی باشیم. لازم است همواره اطمینان حاصل کنیم که تمام اقدامات لازم را برای محافظت از دستگاه های IoT خود در برابر تهدیدات احتمالی و فعال کردن عملکرد امن آنها انجام می دهیم.

از آنجایی که دستگاه های اینترنت اشیا (IoT) بخشی از زیرساخت های عظیم هستند، عواقب آن در صورت هک شدن می تواند میلیون ها نفر را تحت تاثیر قرار دهد.

حملات انکار سرویس توزیع شده

حمله انکار سرویس توزیع شده یا انکار سرویس توزیع شده، نوعی حمله سایبری است که سعی می‌کند یک وب‌سایت یا منبع شبکه را با پر کردن ترافیک مخرب از دسترس خارج کند و عملکرد آن را مختل نماید. در حمله انکار سرویس توزیع شده، مهاجم هدف خود را با ترافیک اینترنتی ناخواسته غرق می‌کند تا ترافیک عادی نتواند به مقصد مورد نظر خود برسد. بنابراین، زمانی که درخواست‌ها برای دستیابی به اطلاعات و داده‌های یک سرور و یا شبکه بیش از حد باشد، حمله انکار سرویس توزیع شده موجب آسیب پذیر شدن سرور خواهد شد. در این‌گونه حمله، هکر به واسطه یک برنامه درخواست‌های متعددی را از بسته های TCP به سرور هدف ارسال می‌کند تا بدین وسیله دسترسی به شبکه را از وب سرور مختل نماید و باعث جلوگیری از دسترسی کاربران به وب‌سایت‌ها شود. حمله انکار سرویس توزیع شده می‌توانند باعث خرابی وب سایت، برنامه وب، APIها، شبکه و زیرساخت مرکز داده یک شرکت شوند و از خرید محصولات، استفاده از یک سرویس، دریافت اطلاعات یا هر گونه دسترسی دیگر توسط کاربران قانونی جلوگیری کنند .حمله انکار سرویس توزیع شده را می‌توان مانند یک ترافیک غیر منتظره در نظر گرفت که بزرگراه را مسدود می‌کند و از رسیدن ترافیک منظم به مقصد جلوگیری می‌کند. هدف انکار سرویس توزیع شده، تخریب یا اختلال در ارائه خدمات یک وب‌سایت یا سرویس آنلاین است که می‌تواند برای کسب و کارها و سازمان‌ها، عواقب جدی و خطرناکی داشته باشد .از جمله این عواقب می‌توان به از دست دادن اعتماد کاربران، خسارت به سلامت عملکرد سازمانی و حتی از دست دادن اطلاعات حساس اشاره کرد. این حملات می تواند انواع سرویس دهنده‌های موجود در شبکه را تهدید کند [۱۶].

حملات انکار سرویس توزیع شده اجزای مختلف اتصال شبکه را هدف قرار می‌دهند. برای درک نحوه عملکرد حملات انکار سرویس توزیع شده، باید بدانیم که یک اتصال شبکه چگونه بوجود می‌آید. اتصال شبکه در اینترنت از اجزا یا لایه‌های مختلفی تشکیل شده است که هر لایه اهداف متفاوتی دارند. مدل ارتباطات باز (OSI) یک چارچوب لایه‌ای برای استانداردهای مختلف شبکه‌ها است که شامل هفت لایه متفاوت می‌باشد. این مسئله را می‌توان مانند ساختن یک خانه از پایه در نظر گرفت که هر لایه از اجزای متفاوتی تشکیل شده‌اند و اهداف متفاوتی دارند. مدلOSI ، نشان دهنده یک چارچوب مفهومی است که برای توصیف اتصال شبکه در ۷ لایه مجزا استفاده می‌شود. تقریباً تمام حملات انکار سرویس توزیع شده بر پایه افزایش ترافیک به یک دستگاه

یا شبکه هدف انجام می‌شوند. هدف همه حملات کاهش شدید یا جلوگیری از رسیدن ترافیک قانونی به مقصد مورد نظر است.

درسوی دیگر DoS یا Denial of Service یک نوع حمله ترافیکی است که سعی می‌کند سرور، شبکه یا سرویس مورد نظر را به حدی درگیر کند که توانایی پاسخ به درخواست کاربران را نداشته باشد و باعث از دسترس خارج شدن منبع شود. در این نوع حمله، مهاجم ممکن است از روش‌های مختلفی از جمله ارسال تعداد بسیار زیادی درخواست به سرویس مورد نظر یا بهره‌مندی از آسیب‌پذیری‌های امنیتی در سیستم‌ها برای اختلال در عملکرد آن‌ها استفاده کند. هدف اصلی حملات DoS اغلب تخریب عملکرد سیستم یا سرویس مورد نظر است، که می‌تواند منجر به از دست رفتن اطلاعات، اختلال در فرآیندهای کسب و کار، از دست رفتن اعتبار سازمان، و خسارات مالی شدید شود. تفاوت DoS و DDoSدر تعداد منابعی است که برای انجام حمله استفاده می‌شود. در حمله داس تنها یک منبع یا یک دستگاه مهاجم برای ارسال تعداد زیادی درخواست به هدف استفاده می‌شود. جدول زیر مشخصه های این دو نوع حمله را مقایسه می نماید [۱۸-۱۷]:

جدول۱. مقایسه مشخصه های حملات DoS و DDoS

عوامل	حملهDoS	حملهDDoS
نام کامل	Denial of Service	Distributed Denial Of Service
دستگاه	از یک دستگاه استفاده می‌شود	شامل تعدادی دستگاه است
سرعت	عموماً کند هستند	سریع‌تر از یک حملهDoS
شناسایی	راحت	بسیار دشوار
حجم	حجم ترافیک کمتر است	حجم ترافیک بسیار زیاد است
پیشگیری	می‌توان به راحتی جلوگیری کرد	بسیار دشوار به پیشگیری است
خسارت	از دست دادن درآمد و شهرت	از دست دادن درآمد، شهرت و هزینه‌های سربار برای بازیابی و امنیت
پیشگیری	حملات DoS می‌توانند به راحتی با استفاده از اقدامات امنیتی بهینه جلوگیری شوند	حملات DDoS به راحتی قابل پیشگیری نیستند، زیرا شامل دستگاه‌های دستکاری شده هستند که زیر کنترل قربانین می‌باشند
نحو اجرا	اجرا از یک دستگاه بوسیله اسکریپت یا نرم‌افزار	از یک سرور دستور و کنترل (C&C) استفاده می‌کند

بمنظور بررسی و پیشنهاد راهکارهای مناسب جهت مقابله با این چالش های امنیتی لازم است در بخش بعدی ابتدا ساختار و انواع حملات انکار سرویس توزیع شده را بررسی می نمائیم.

شناسائی انواع حملات انکار سرویس توزیع شده و راهکارها

اساسا حمله انکار سرویس توزیع شده عموماً به دو شکل اشباع باند پهنای باند و اشغال منابع صورت می‌گیرد. در حملاتی که پهنای باند مورد حمله قرار میگیرد، مهاجمان تعداد زیادی درخواست به یک هدف ارسال می‌کنند، به طوری که باند پهنای باند سیستم مقصد اشباع شده و دیگر ترافیک معمولی نمی‌تواند به آن سرور راه پیدا کند. معمولاً حمله انکار سرویس توزیع شده پهنای باند بر روی لایه سوم مدل OSI انجام می‌شوند و مهاجمان می‌توانند از تکنیک‌های مختلفی مانند UDP Flood، ICMP Flood، و SYN Flood استفاده کنند. نوع دیگر حملات انکار سرویس توزیع شده حملات اشغال منابع است. در این نوع حمله، هکران سعی می‌کنند منابع سیستم مقصد مانند پردازنده، حافظه، و اتصالات شبکه را اشغال کنند. این حملات دی داس معمولاً بر روی لایه هفتم OSI انجام می‌شوند و می‌توانند شامل حملات HTTP Flood،Slowloris و DNS Amplification باشند. هدف حمله انکار سرویس توزیع شده با توجه به اهداف هکران ممکن است متغیر باشد. اما در کل، اهداف اصلی حملات انکار سرویس توزیع شده شامل موارد زیر می‌شود:

- ایجاد اختلال در سرویس‌دهی
- تخریب سیستم‌ها
- سرقت اطلاعات
- تأثیرگذاری بر عملکرد اقتصادی
- بدنام کردن شرکت مورد هدف

حملات انکار سرویس توزیع شده می‌توانند به مشکلات جدی برای سازمان‌ها، کسب و کارها، و حتی افرادی که هدف حملات هستند، منجر شوند. برخی از این مشکلات عبارتند از قطعی سرویس، افزایش هزینه‌ها برای مقابله با حملات، افزایش تاخیر و کاهش عملکرد و آسیب به سازمان‌ها و افراد.

ساختار کلی حملات انکار سرویس توزیع شده به شرح زیر می‌باشد:

شبکه‌های زامبی[1]:

[1] Botnets

باتنت مجموعه‌ای از دستگاه‌های متصل به اینترنت هستند که شامل رایانه‌های شخصی، سرورها، دستگاه‌های تلفن همراه و دستگاه‌های اینترنت اشیا (IoT) می‌باشند که توسط یک نوع رایج بدافزار آلوده و توسط هکر کنترل می‌شوند. Botnets بدون اطلاع یا موافقت کاربران، توسط نرم‌افزارهای مخربی که معمولاً به عنوان تروجان‌ها یا ویروس‌ها شناخته می‌شوند، مورد استفاده قرار می‌گیرند. با استفاده از بات نت‌ها هکران می‌توانند ترافیک‌های فیک و تقلبی برای سرورهای قربانی و مورد هدف ارسال کنند و باعث افزایش ترافیک بار سرور و در نتیجه از دسترس خارج شدن آن شوند.

سیستم کنترل و دستور[1]:

C&C مربوط به سرورها یا سیستم‌هایی است که مهاجمان برای کنترل باتنت خود استفاده می‌کنند. این سیستم‌ها می‌توانند اقداماتی مانند ارسال دستورات به کامپیوترهای زامبی یا جمع‌آوری اطلاعات در مورد حملات را انجام دهند.

سرورهای بازتابنده[2]:

این بخش شامل سرورهایی است که مخربین از آن‌ها برای تقویت حجم حملات استفاده می‌کنند. به عنوان مثال، از سرورهای Reflector برای تقویت اطلاعات و ارسال تعداد زیادی از کامپیوترهای زامبی برای افزایش قدرت حمله استفاده می‌شود.

سرور قربانی:

این بخش از سیستم مربوط به سرور یا سرویسی است که هدف اصلی حمله است. این سرور به دلیل حجم بالای ترافیک درخواستی که از سوی باتنت و سرورهای Reflector فرستاده می‌شود، ممکن است از دسترس خارج شود و بنابراین خدماتی که ارائه می‌دهد قطع شود.

در ادامه این بخش به بررسی انواع حملات داس و انکار سرویس توزیع شده خواهیم پرداخت [۲۲-۱۹]:

حمله Syn Flood

در این حمله دی داس تعداد زیادی درخواست HTTP به سرور ارسال می‌شود و سرور را تحت تاثیر قرار می‌دهد. این حمله را می‌توان به دو نوع ساده و پیچیده تقسیم‌بندی کرد. در حملات ساده سرور از طریق یک IP مورد حمله قرار می‌گیرد. در حالی که در حملات پیچیده URL های تصادفی مورد هدف قرار می‌گیرند و در نهایت باعث انکار سرویس (DoS)یا انکار سرویس توزیع‌شده (DDoS) می‌شوند.

برای جلوگیری از حمله انکار سرویس توزیع شده از نوع syn flood ، می‌توان از روش‌های مختلف استفاده کرد از جمله:

- پیکربندی سرور به نحوی که با درخواست‌های غیرمعمول مانند تعداد بیش از حد از یک IP آدرس خاص مقابله کند
- استفاده از فایروال‌ها و سیستم‌های تشخیص حملات (IDS/IPS)برای شناسایی و مسدود کردن ترافیک مشکوک
- استفاده از سیستم‌های کنترل دسترسی (ACL) برای محدود کردن دسترسی به سرویس‌های حساس
- استفاده از CDN (شبکه توزیع محتوا) برای توزیع ترافیک و تخفیف بار بر روی سرورها
- به روزرسانی نرم‌افزار سرور و استفاده از تکنولوژی‌های امنیتی برای مقاوم ساختن سرور در برابر حملات

حمله Icmp Flood

حمله ICMP Floodیک نوع حمله انکار سرویس (DoS) است که با استفاده از پروتکل ICMP (Internet Control Message Protocol) انجام می‌شود. در این نوع حمله، مهاجمان با ارسال تعداد بسیار زیادی درخواست) ICMP معمولاً درخواست‌های (pingبه سرور یا دستگاه هدف، سعی در اشباع باند پهنای باند شبکه یا مصرف منابع دستگاه هدف دارند. هدف اصلی از حمله ICMP Flood ، ایجاد ازدحام و ایجاد انکار سرویس است. با ارسال تعداد زیادی درخواستICMP ، منابع سرور یا دستگاه هدف، از جمله پردازشگر و پهنای باند، مصرف می‌شوند و به دسترسی کاربران مورد نظر ممکن است اختلال وارد شود یا به صورت کلی از دسترس خارج شوند. برای جلوگیری از حملات انکار سرویس توزیع شده ICMP Flood ، می‌توان از روش‌های زیر استفاده کرد:

- استفاده از فایروال‌ها وIDS/IPS
- استفاده از محدودیت‌های دسترسی به سرورها و شبکه
- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها
- استفاده از لایه‌های مانیتورینگ و لاگ‌گیری
- استفاده از راهکارهای مبتنی بر QoS (کیفیت خدمات) و مدیریت ترافیک

حمله UDP Flood

یکی دیگر از حملات منع سرویس دهی حمله udp flood می‌باشد که با استفاده از پروتکل UDP (User Datagram Protocol) انجام می‌شود. در این نوع حمله، مهاجمان با ارسال تعداد بسیار زیادی پکت‌های UDP به یک سرور یا دستگاه هدف، سعی در اشباع باند پهنای باند شبکه یا مصرف منابع دستگاه هدف دارند. هدف اصلی از حمله UDP Flood ، ایجاد ازدحام در سرویس است [۲۳].

برای جلوگیری از حملات UDP Flood ، می‌توان از روش‌های زیر استفاده کرد:

- استفاده از فایروال‌ها وIDS/IPS
- استفاده از محدودیت‌های دسترسی به سرویس‌ها و شبکه:
- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها
- استفاده از لایه‌های مانیتورینگ و لاگ‌گیری
- استفاده از راهکارهای مبتنی بر QoS (کیفیت خدمات) و مدیریت ترافیک

حمله Dns Flood

حمله DNS Floodیک نوع حمله انکار سرویس (DoS) است که با استفاده از پروتکل DNS (Domain Name System) صورت می‌گیرد. در این نوع حمله، مهاجمان با ارسال تعداد زیادی درخواست DNS به سرور

[1] Command and Control (C&C)

[2] Reflector Servers

DNSهدف، سعی در استفاده بیش از حد از قابلیت پهنای باند شبکه یا مصرف منابع سرور دی ان اس دارند. هدف اصلی از این نوع حمله داس DNS Flood، ایجاد ازدحام و انکار سرویس است. زیرا سرور دی ان اس مسئول تبدیل نام‌های دامنه به آدرس‌های IP است و ارسال تعداد زیادی درخواست DNS می‌تواند باعث پر شدن تکمیل ظرفیت پهنای باند شبکه و مصرف منابع سرور شود تا کاربران نتوانند به نشانی‌های وب مورد نظر خود دسترسی پیدا کنند. برای جلوگیری از حملاتDNS Flood ، می‌توان از روش‌های زیر استفاده کرد:

- استفاده از فایروال‌ها وIDS/IPS
- استفاده از محدودیت‌های دسترسی به سرویس‌ها و شبکه
- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها
- استفاده از لایه‌های مانیتورینگ و لاگ‌گیری
- استفاده از راهکارهای مبتنی بر QoS (کیفیت خدمات) و مدیریت ترافیک

حمله Protocol

در این حملات محروم سازی از سرویس، پروتکل‌های مورد استفاده در انتقال داده‌ها، برای تخریب یک سیستم مورد هدف قرار می‌گیرند. مصرف بیش از حد منابع سرور و یا تجهیزات شبکه مانند فایروال‌ها منجر به ایجاد اختلال در سرویس‌ها می‌شوند. حملات پروتکل، از نقاط ضعف لایه ۳ و ۴ از پشته پروتکل استفاده می‌کنند تا هدف غیرقابل دسترس را به دست آوردند.این اختلال می‌تواند منجر به انکار سرویس یا انکار سرویس توزیع‌شده شود، که هر دو منجر به عدم دسترسی کاربران به سرویس مورد نظر می‌شوند. یکی از شایع‌ترین حملات پروتکل در انکار سرویس توزیع شده، syn floodاست که با ارسال حجم زیادی از بسته‌هایSYN ، به فرایند ساخت یک اتصال TCP/IP حمله می‌کند و منجر می‌شود کاربر منتظر اتصالی بماند که هرگز اتفاق نمی‌افتد. برای جلوگیری از حمله انکار سرویس توزیع شده از نوع Protocol، می‌توان از روش‌هایی مانند روش های زیر استفاده نمود [۲۴]:

- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها
- استفاده از فایروال‌ها وIDS/IPS
- استفاده از محدودیت‌های دسترسی
- استفاده از راهکارهای مانیتورینگ و لاگ‌گیری
- استفاده از راهکارهای حفاظتی مبتنی بر پروتکل

حمله Volumetric

در این نوع حمله، حجم بالایی از داده‌ها به سمت هدف ارسال می‌شود به گونه‌ای که پهنای باند موجود بین هدف و اینترنت به سرعت پر شده و سرویس مورد نظر قطع یا ضعیف می‌شود. هدف اصلی از حمله انکار سرویس توزیع شده از نوعVolumetric ، ایجاد اختلال در سرویس‌دهی است، به‌طوری‌که کاربران نتوانند به منابع یا سرویس‌های مورد نظر خود دسترسی پیدا کنند. این حملات معمولاً با استفاده از تکنیک‌های تقویت سیگنال یا سایر روش‌هایی که به ایجاد ترافیک بزرگ کمک می‌کنند، مانند استفاده از شبکه‌های باتن، صورت می‌گیرند. بمنظور جلوگیری از انکار سرویس توزیع شده از نوع Volumetric، می‌توان از روش‌های زیر استفاده کرد:

- استفاده از فایروال‌ها و سیستم‌های شناسایی نفوذ (IDS/IPS)برای شناسایی و مسدود کردن ترافیک مشکوک
- استفاده از خطوط ارتباطات با پهنای باند بیشتر و سیستم‌های مبتنی بر شبکه‌های CDN (شبکه توزیع محتوا) برای توزیع ترافیک و کاهش فشار روی سرورها
- استفاده از سیستم‌های تشخیص حمله DDoS (حملات توزیع شده به ازدحام) و سیستم‌های مانیتورینگ ترافیک برای شناسایی حملات و اتخاذ اقدامات دفاعی
- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها برای رفع ضعف‌ها و آسیب‌پذیری‌های امنیتی

حمله Slowloris

یکی دیگر از انواع حملات انکار سرویس توزیع شده از نوع Slowloris است که این امکان را برای وب سرور بوجود می‌آورد تا بدون تحت تاثیر قرار دادن سایر سرویس‌ها و پورت‌ها عملکرد سرور را مختل نماید و از کار بی‌اندازد. در این روش اتصالات تقلبی بسیاری توسط ابزار Slowlorisایجاد می‌شود و در نتیجه توانایی پاسخگویی به درخواست‌های واقعی را از دست می‌دهد. هدف اصلی از حمله Slowloris، مصرف منابع سرور است تا سرور نتواند به درخواست‌های واقعی کاربران پاسخ دهد. این حمله انکار سرویس توزیع شده می‌تواند به شیوه‌های مختلفی انجام شود، اما عمدتاً با ارسال درخواست‌های HTTPناقص یا بسیار کوچک به سرور هدف صورت می‌گیرد. برای جلوگیری از انکار سرویس توزیع شدهSlowloris ، می‌توان از روش‌های زیر استفاده کرد:

- تنظیم صحیح سرور
- استفاده از فایروال‌ها وIDS/IPS
- استفاده از لایه‌های مانیتورینگ و لاگ‌گیری
- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها
- استفاده از سیستم‌های مانیتورینگ ترافیک و تنظیم محدودیت‌های دسترسی به سرور برای مدیریت منابع

حمله NTP Amplification

حمله NTP Amplification یک نوع حمله توزیع شده به خدمات انکار سرویس توزیع شده است که از پروتکل NTP [1] برای افزایش حجم ترافیک استفاده می‌کند. در این نوع حمله، مهاجمان با ارسال درخواست‌های جعلی به سرورهایNTP ، سعی در ایجاد پاسخ‌های با حجم بسیار بزرگ به درخواست‌ها دارند. سپس این پاسخ‌های بزرگ به سمت هدف ارسال می‌شوند و سرور هدف با مصرف منابع زیادی مواجه می‌شود که ممکن است منجر به از دست رفتن دسترسی به سرویس یا قطعی اینترنتی

[1] Network Time Protocol

شود. هدف اصلی از حمله NTP Amplification ، ایجاد ازدحام و ایجاد انکار سرویس است، به طوری که سرویس مورد نظر قابل دسترسی نباشد و از کار افتد. مصرف بیش از حد پهنای باند شبکه و منابع سرور موجب تخلیه منابع و ایجاد ناپایداری در سرویس می‌شود. برای جلوگیری این نوع از حمله ddos ، می‌توان از روش‌های زیر استفاده کرد:

- تنظیمات امنیتی در سرورهای NTP
- استفاده از فایروال‌ها و IDS/IPS
- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها
- استفاده از محدودیت‌های دسترسی به سرورها و شبکه

حمله Thermox

حمله ترموکس یا Thermox با استفاده از تکنیک‌های تقلب در شبکه spoofing و تکمیل ظرفیت منابع resource exhaustion برای حمله به سیستم‌های مخابراتی و شبکه‌های ارتباطی استفاده می‌کند. این حمله به طور خاص بر روی سیستم‌های VoIP تأثیرگذار است. هدف اصلی از این نوع حمله دی داس، ایجاد اختلال در خدمات VoIP است، به طوری که کاربران نتوانند از طریق این سیستم‌ها تماس برقرار کنند یا صدای کیفیت مناسبی را دریافت کنند. این حمله می تواند باعث قطع مکالمات، افزایش تاخیر در ارتباطات و کاهش کیفیت صدا شود. برای جلوگیری از حملات ترموکس، می‌توان از روش‌های زیر استفاده کرد:

- استفاده از تجهیزات امنیتی
- استفاده از محدودیت‌های دسترسی
- استفاده از راهکارهای امنیتی برای VoIP
- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها
- مانیتورینگ فعالیت‌ها و لاگ‌گیری

حمله انکار سرویس توزیع شده Rainbow

حمله انکار سرویس توزیع شده رینبو یا DDoS Rainbow یک نوع حمله انکار سرویس توزیع شده Distributed Denial of Service است که با استفاده از تنوع در تکنیک‌ها و منابع حمله انجام می‌شود. در این نوع حمله، مهاجمان از مجموعه‌ای از روش‌ها، منابع و تکنیک‌ها برای انجام حمله استفاده می‌کنند تا بر دفاع‌های سیستم‌های امنیتی ایجاد شده نیز نفوذ کنند. هدف اصلی از انجام حمله دی داس نوع Rainbow اشغال منابع سیستم و ایجاد اختلال در ارتباطات است. با فشرده سازی ترافیک از طریق مجموعه‌ای منابع و تکنیک‌ها این حمله می‌تواند باعث قطع سرویس‌ها، کاهش کارایی سیستم‌ها، افزایش تاخیر در ارتباطات و کاهش کیفیت خدمات شود. برای جلوگیری از حملات انکار سرویس توزیع شده رینبو، می‌توان از روش‌های زیر استفاده کرد:

- استفاده از سیستم‌های تشخیص حمله و جلوگیری از حمله برای شناسایی الگوهای حمله و جلوگیری از ورود ترافیک مشکوک به شبکه
- استفاده از فایروال‌ها و تجهیزات امنیتی پیشرفته برای فیلترینگ و مدیریت ترافیک ورودی به شبکه
- به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها به منظور رفع آسیب‌پذیری‌ها که ممکن است توسط حملات انکار سرویس توزیع شده رینبو بهره‌برده شود
- استفاده از راهکارهای مبتنی بر ابر (Cloud-based) برای تحلیل و فیلترینگ ترافیک ورودی و مقاومت در برابر حملات انکار سرویس توزیع شده
- مانیتورینگ فعالیت‌ها و لاگ‌گیری برای زمان‌بندی، شناسایی و پاسخگویی سریع به حملات

درخصوص سایر راهکارها و همچنین رویکردهای جلوگیری از حملات DDoS با استفاده از روش‌های مختلف سخت افزاری و نرم افزاری صورت می‌گیرد. در ادامه به برخی از راهکارهای موثر دیگر برای مدیریت و جلوگیری از تاثیر انکار سرویس توزیع شده خواهیم پرداخت [۲۷-۲۵]:

- استفاده از سیستم‌های مقاومت در برابر حملات DDoS برای تشخیص ترافیک مخرب و جلوگیری از ورود آن به شبکه و سرویس‌ها
- استفاده از فایروال‌های توزیع شده Distributed Firewalls برای مدیریت و کنترل بار ترافیک
- استفاده از خدمات محافظت در برابر DDoS ارائه دهندگان خدمات ابری
- بروزرسانی نرم‌افزارها و سیستم‌ها برای کاهش حملات منع سرویس دهی
- اعمال تنظیمات امنیتی در سرورها و شبکه‌ها برای مقابله با حملات انکار سرویس توزیع شده
- استفاده از سرویس‌های CDN برای توزیع محتوا از نزدیکترین سرور به کاربران و موثر در جلوگیری از حمله ddos
- یک راه حل موثر DDoS Mitigation باید قابلیت مقیاس پذیری و انطباق با الزامات یک کسب و کار در حال رشد و همچنین پاسخگویی به اندازه رو به رشد حملات DDoS را دارا باشد.
- قابلیت اطمینان نیز در راه حل کاهش DDoS برای اینکه یک استراتژی حفاظتی موفق باشد، ضروری است. این سرویس باید نرخ به‌روزرسانی بالایی داشته باشد و مهندسان سایت همیشه در پشتیبانی آن حضور داشته باشند تا اطمینان حاصل نمایند که شبکه آنلاین است و تهدیدهای جدید در کمترین زمان شناسایی می‌شوند.
- توانایی ایجاد خط‌مشی‌های انعطاف پذیر و الگوهای موردی و تک کاره به یک ویژگی وب اجازه می‌دهد، تا با تهدیدهای دریافتی در زمان واقعی سازگار شود. توانایی اجرای قوانین صفحه و اطمینان از این تغییرات در کل شبکه می‌تواند در حفظ کارکرد سایت در طول حمله بسیار مهم و موثر واقع شود.

- ظرفیت شبکه نیز اساسا مقیاس پذیری یک حمله را منعکس می‌کند و راهی عالی برای آزمایش یک سرویس DDoS Mitigationاست. بیشتر خدمات کاهش DDoS مبتنی بر ابر، ظرفیت شبکه چند ترابایتی را ارائه می‌کنند که فراتر از نیاز هر مشتری است. از سوی دیگر، سرویس‌های داخلی به‌طور پیش‌فرض با اندازه شبکه و ظرفیت سخت‌افزار داخلی سازمان محدود می‌شوند. شبکه‌های بزرگی که قابلیت‌های انتقال داده گسترده‌ای دارند، می‌توانند به یک ارائه‌دهنده Mitigation برای تحلیل و پاسخ موثر و سریع به حملات کمک کنند و اغلب از حملات پیش از وقوع آن‌ها جلوگیری می‌کنند.
- استفاده از تجهیزات سخت افزاری حفاظت و توزیع ترافیک[1] نیز راه حل موثر دیگر می باشد. این تجهیزات ترافیک را بین چندین سرور یا منطقه شبکه توزیع می‌کنند تا از بارزنی بیش از حد به یک منبع خاص جلوگیری شود و با مکانیزم های محافظتی اثرات حملات DDoS کاهش یابد.
- روش‌های نرم‌افزاری با استفاده از الگوریتم‌های پیشرفته و فناوری‌های تشخیصی، ترافیک مخرب را تشخیص می‌دهند و از ورود آن به شبکه و سرویس‌ها جلوگیری می‌کنند.
- سرویس‌های Anti-DDoS برای شناسایی و کاهش حملات DDoSدر زمان واقعی با تجزیه و تحلیل ترافیک شبکه و مسدود کردن ترافیک مخرب و تقلبی قبل از رسیدن به برنامه یا سرویس هدف طراحی شده‌اند. این سرویس با استفاده از تکنیک‌های مختلفی مانند فیلتر کردن ترافیک مخرب، انحراف ترافیک و یا پاکسازی ترافیک، ترافیک مخرب را شناسایی و مسدود می‌کند و در عین حال به ترافیک قانونی اجازه عبور می‌دهد.
- همچنین در آخر ممکن است از ترکیب روش‌های مختلف سخت‌افزاری و نرم‌افزاری برای بهبود مقاومت سیستم‌ها در برابر حملات DDoS استفاده شود. این ترکیبات می‌توانند به صورت اتوماتیک عمل کرده و سیستم‌ها را در مقابل حملات DDoSمحافظت کنند . محدودیت سرعت، افزای پهنای باند و انتشار شبکه ای از استراتژی های رایج دیگر می باشند.

درپایان لازم به ذکر است که هیچ روش دائمی برای جلوگیری از حملات DDoSوجود ندارد، و همواره هکر ها از روش ها و تکنیک های جدید تر برای اجرای حملات سنگین استفاده می کنند. پیگیری و تشخیص به موقع و داشتن مدیران سرور متخصص برای شرکت های هاستینگ بسیار مهم است، به نحوی که توانایی مقابله و رفع سریع حملات را داشته باشند.

نتیجه گیری

اخیرا با رشد اینترنت اشیا هر روزه تعداد بیشتری دستگاه به محیط اینترنت متصل می گردند. بزرگترین چالشی که در این رابطه ایجاد شده است، تامین امنیت این دستگاه ها می باشد. حملات انکار سرویس توزیع شده جز اتفاقات اجتناب‌ناپذیر در دنیای فناوری مرتبط با اینترنت اشیا هستند. این حملات با ایجاد اختلال در زیرساخت‌های سرورهای مختلف، در ترافیک اینترنت اشیا اختلال ایجاد می‌کنند و بدین صورت باعث ایجاد مشکلاتی همچون کندی عملکرد سایت می‌شوند. پیامدهای حمله انکار سرویس توزیع شده می‌تواند شامل از کارافتادگی سرویس، افت تجربه کاربری، افزایش هزینه‌های توسعه و نگهداری، و از دست دادن اعتماد مشتریان باشد. اما طبیعتا مانند هر مشکل دیگر این مشکل نیز دارای رویکردهای مقابله ای می باشد که بنا به ضرورت پژوهش در این حوزه، در این مقاله به این رویکردها پرداختیم. با بهره گیری از از راهکارهای حفاظتی شامل استفاده از فایروال، توزیع بار، وب اپلیکیشن فایروال و سایر رویکردهای ترکیبی می توان از حملات انکار سرویس توزیع شده محافظت ایجاد نمود. در واقع در این حملات، هدف مهاجمان ایجاد شرایطی پیچیده و غیرقابل‌حل برای سرور، شبکه و یا سایت است. حمله انکار سرویس توزیع شده به روش‌های مختلف رخ می‌دهد، پس لازم است برای جلوگیری از این حمله استراتژی‌های ترکیبی خاصی بکار برده شود. در این مقاله با موارد امنیتی و ابزار هایی که می توانیم قبل از بروز یا حین انجام حملات انکار سرویس توزیع شده از آن ها استفاده کنیم، آشنا شدیم. ارائه یک رویکرد ترکیبی و پیاده سازی رویکرد در محیط کاربردی اینترنت اشیا از رویکردهای آتی پژوهش حاضر می باشد.

مراجع

[1] Alaba FA, Othman M, Hashem IA, Alotaibi F. Internet of Things security: A survey. Journal of Network and Computer Applications. 2017 Jun 15;88:10-28.

[2] Conoscenti M, Vetro A, De Martin JC. Blockchain for the Internet of Things: A systematic literature review. In2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) 2016 Nov 29 (pp. 1-6). IEEE.

[3] Gazis V, Görtz M, Huber M, Leonardi A, Mathioudakis K, Wiesmaier A, Zeiger F, Vasilomanolakis E. A survey of technologies for the internet of things. In2015

[1] Traffic Distribution Appliances

In2022 5th Conference on Cloud and Internet of Things (CIoT) 2022 Mar 28 (pp. 32-39). IEEE.

[13] Aldhyani TH, Alkahtani H. Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model. Mathematics. 2023 Jan 3;11(1):233.

[14] Ali MH, Jaber MM, Abd SK, Rehman A, Awan MJ, Damaševičius R, Bahaj SA. Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). Electronics. 2022 Feb 8;11(3):494.

[15] Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences. 2021 May 17;11(10):4580.

[16] Kaur H, Behal S, Kumar K. Characterization and comparison of distributed denial of service attack tools. In2015 International Conference on Green Computing and Internet of Things (ICGCIoT) 2015 Oct 8 (pp. 1139-1145). IEEE.

[17] Manavi MT. Defense mechanisms against distributed denial of service attacks: A survey. Computers & Electrical Engineering. 2018 Nov 1;72:26-38.

[18] Dalmazo BL, Marques JA, Costa LR, Bonfim MS, Carvalho RN, da Silva AS, Fernandes S, Bordim JL, Alchieri E, Schaeffer-Filho A, Paschoal Gaspary L. A systematic review on distributed denial of service attack defense mechanisms in programmable networks. International Journal of Network Management. 2021 Nov;31(6):e2163.

[19] Cheema A, Tariq M, Hafiz A, Khan MM, Ahmad F, Anwar M. Prevention techniques against distributed denial of service attacks in heterogeneous networks: A systematic review. Security and Communication Networks. 2022 May 20;2022:1-5.

international wireless communications and mobile computing conference (IWCMC) 2015 Aug 24 (pp. 1090-1095). IEEE.

[4] Alamri M, Jhanjhi NZ, Humayun M. Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review. Int. J. Comput. Sci. Netw. Secur. 2019 May;19(1):244-58.

[5] Yu S. Distributed denial of service attack and defense. Springer New York; 2014 Jan 1.

[6] Kaur P, Kumar M, Bhandari A. A review of detection approaches for distributed denial of service attacks. Systems Science & Control Engineering. 2017 Jan 1;5(1):301-20.

[7] Shah Z, Ullah I, Li H, Levula A, Khurshid K. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors. 2022 Jan 31;22(3):1094.

[8] Arachchige KG, Branch P, But J. An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attacks. Sensors. 2024 May 12;24(10):3083.

[9] Wani S, Imthiyas M, Almohamedh H, Alhamed KM, Almotairi S, Gulzar Y. Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight. Symmetry. 2021 Jan 29;13(2):227.

[10] Kumar R, Kumar P, Tripathi R, Gupta GP, Garg S, Hassan MM. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. Journal of Parallel and Distributed Computing. 2022 Jun 1;164:55-68.

[11] Singh R, Tanwar S, Sharma TP. Utilization of blockchain for mitigating the distributed denial of service attacks. Security and Privacy. 2020 May;3(3):e96.

[12] Djuitcheu H, Debes M, Aumüller M, Seitz J. Recent review of distributed denial of service attacks in the internet of things.

[20] Varma SA, Reddy KG. A review of DDoS attacks and its countermeasures in cloud computing. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6). IEEE.

[21] Kumar R, Lal SP, Sharma A. Detecting denial of service attacks in the cloud. In2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) 2016 Aug 8 (pp. 309-316). IEEE.

[22] Kolhe TD, Kolhe MT. Distributed Denial Of Service Attack Techniques: Analysis, Implementation And Comparison.

[23] Karthikeyani R, Karthikeyan E. A Review on Distributed Denial of Service Attack. Asian Journal of Research in Computer Science. 2023 Oct 13;16(4):133-44.

[24] Adedeji KB, Abu-Mahfouz AM, Kurien AM. DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. Journal of Sensor and Actuator Networks. 2023 Jul 6;12(4):51.

[25] Salim MM, Rathore S, Park JH. Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing. 2020 Jul;76:5320-63.

[26] Suthar F, Patel N. A Survey on DDoS Detection and Prevention Mechanism. Journal of Advances in Information Technology. 2023;14(3).

[27] Wong F, Tan CX. A survey of trends in massive DDoS attacks and cloud-based mitigations. International Journal of Network Security & Its Applications. 2014 May 1;6(3):57.

تعارض منافع

«هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است»