روباه‌آهنی

راهکار پکپارچه و برخط برای شناسایی و مسدودکردن
بات‌های لایه برنامه‌های کاربری تحت‌وب

IronFox

Real-Time Web Application Layer & API Protection

طراحی و توسعه:

Innovera Technology

https://innovera.ir

نگارش سند

5 سپتامبر 2020

مقدمه

با رشد فناوری و پیچیدگی حملات سایبری، تکنولوژی‌های سنتی و راهکارهای فعلی در امنیت پاسخگو نیستند. تا چند وقت پیش فایروالهای لایه شبکه و سیستمهای کشف نفوذ مبتنی نسل اول تا حد قابل قبولی پاسخگویی نیازمندی امنیت کسب و کارهای بزرگ و کوچک بود، نسل دوم محصولات و راهکارهای امنیتی شامل فایروالهای برنامه کاربردی تحت وب و سیستمهای کشف و دفع حملات نیز توانستند تا حد قابل قبولی فضای سایبر را امن کنند. امنیت کسب و کارهای آنلاین و برنامه‌های کاربردی تحت وب و اپلیکیشنهای موبایل اهمیت بالایی دارد و حتی با ظهور نسل دوم و سوم (NGF/ IDS/ IDP) راهکارها و تجهیزات امنیتی، هنوز بات‌ها و حملات مرتبط با شبکه بات‌ها همچون حملات منع‌سرویس و منع سرویس توزیع شده (DoS/DDoS) به عنوان چالشی در فضای سایبر و امنیت کسب و کارهای آنلاین مطرح است.

ربات‌ها و شبکه‌های مبتنی بر بات(botnetها) از ابتدای پیداش تا الان، به عنوان چالشی در فضای وب و کسب وکارهای آنلاین مطرح بوده و در گزارش‌های متعددی که منتشر شده است حملات بات‌نت‌ها و یا سواستفاده از شبکه‌های مبتنی بر بات، باعث ایراد خسارات جبران ناپذیری به کسب و کارهای آنلاین شده و فضای تبادل اطلاعات است. بات‌ها نسل جدید حملات هوشمندی هستند که کشف و شناسایی آنها اهمیت و پیچیدگی بالایی دارد.

راهکارها و مقالات متعددی برای مقابله با بات‌ها و شبکه مبتنی بر بات‌ها مطرح و منتشر شده است، برای مثال در حملات مبتنی بر منع سرویس و منع‌سرویس توزیع شده (DoS/ DDoS) راهکارهایی از قبیل ردگیری منبع حملات (Master) و غیر فعال‌کردن Slaveها (بات‌ها) بیان شده است، اما در واقعیت عمل در اجرا دشوار و در بیشتر موارد تقریبا غیرممکن است.

روباه آهنی یک سامانه با توان پردازشی بالا (High Performance) و هوشمند برای شناسایی و مسدود کردن بات‌های لایه برنامه کاربردی تحت وب(Layer 7)، با رویکردی نوین برای استفاده و بکارگیری در سرویس‌های عملیاتی و محیط‌های اجرایی به صورت برخط است و در این مقاله مروری بر بات‌ها، ساختار بات‌ها و حملات مرتبط و راهکار طراحی و توسعه‌داده شده برای آن معرفی و بیان خواهد شد.

بات چیست؟

بات‌ها نرم‌افزاری هستند که برای اهداف مختلفی طراحی و توسعه داده می‌شوند. بات‌ها کاربردهای مختلفی دارند، برای مثال در موتورهای جستجو، مولفه خزشگر در نقش یک بات وظیفه خزش صفحات و گردآوری اطلاعات را بر عهده دارد، باتها بر اساس عملکرد خود می‌توانند نقشی خوب یا در مقابل آن مهاجم را بازی کنند، برای مثال خزشگرهای موتورهای جستجو همانند Google به عنوان یک بات خوب عمل میکنند و در مقابل آن خزشگری که از مکانیزم احراز هویت (Broken Authentication)ـ یا کنترل دسترسی (Access List)ـ ضعیف یک برنامه کاربردی تحت وب یا سرویس آنلاین بهره‌برداری و سواستفاده می‌کند به عنوان یک بات مخرب داده‌های سرور را واکشی و به سرقت میبرند و یا با ایجاد ترافیک آلوده باعث ایجاد فشار کاری در سمت سرور شده و منابع سرور و سرویس‌ها به صورت کامل از دسترس خارج می‌شوند، بات‌های مخرب میتوانند یک آسیب‌پذیری را برای هزاران مقصد به صورت مکانیزه تست و اکسپلویت کنند و مثال‌های دیگری که می‌توان در این خصوص بیان کرد. ساختار داخلی بات‌ها میتواند از ساختار داخلی یک بات ساده تا یک بات هوشمند و پیچیده بوده و بر اساس ماموریتی که برای آن طراحی و توسعه داده می‌شوند، ساختار متفاوتی را دارند.

در دنیای امروز و با رشد کسب و کارها، مجبور هستیم با اپیدمی بات‌ها سازگاری داشته باشیم و راه‌حلی برای شناسایی و دسته‌بندی بات‌ها طراحی و توسعه داده شود، برای مثال امروزه نمی‌توانیم با تکنیک‌هایی همانند چالش تصویری (Captcha)ـ خزشگرهای موتورهای جستجو همانند Google را از خزش و ایندکس کردن صفحات وب‌سایت خود محروم کنیم و در مقابل آن در صورتی که به بات‌های مخرب اجازه فعالیت داده شود سرویس‌های آنلاین ممکن است با اختلات و افت شدید کیفیت (QoS)ـ همراه شوند یا در شرایطی از دسترس کاربران به صورت کامل خارج شود. لذا لازم است تا راهکاری ارایه شود که فعالیت‌های بات‌های خوب و بد را تشخیص و حملات مربوط به آنها شناسایی و مسدود شود.

بات‌ها و حملات مبتنی بر شبکه بات‌ها

بات‌ها طیف وسیعی از حملات را راه‌اندازی و اجرا می‌کنند. موارد زیر نمونه‌ای از حملات بات‌ها و شبکه‌بات‌ها می‌باشد.

1. پویش آسیب‌پذیری و اجرای کد مخرب برای اکسپلویت کردن هدف (مثلا یک ماژول آسیب‌پذیر wordpress)
2. خزش و سرقت اطلاعات، بات‌ها به صورت اتوماتیک و مکانیزه دادها را خزش و به سرقت میبرند. یک کاربر عادی نمیتواند به اندازه سرعت اجرای یک بات داده‌ها را مشاهده و به سرقت ببرد. بات‌ها مکانیزه هستند.
3. تولید درخواست و اجرای حملات منع سرویس، شبکه بات‌ها میتوانند با تولید درخواست و اجرای حمله منع سرویس و منع‌سرویس توزیع شده(DoS/ DDoS) باعث هدر رفتن منابع در سرور و سرویس شده و آن را به صورت کامل از دسترس کاربران خارج کنند. برای مثال در سامانه‌های خرید و فروش و بورس به راحتی میتوان با تولید ترافیک و درخواست جعلی، فرآیند خرید و فروش را که به فاکتور زمانی وابستگی زیادی دارد از دسترس کاربران واقعی آن خارج کرد.
4. باتها به راحتی برای اجرای تقلب مورد استفاده قرار میگیرند. برای مثال در یک سامانه نظرسنجی یا موارد مشابه بات‌ها میتوانند همانند کاربر عمل کرده و به صورت اتوماتیک از فرآیند ثبت نام تا رای دادن را اجرا کنند، برای تولید چنین بات‌هایی به راحتی میتوان از کتابخانه‌ها و فریم‌ورک‌هایی همانند Selenium یا موارد مشابه دیگر با چند ده خط کد بات مربوطه را طراحی و توسعه داد.
5. جعل هویت، بات‌ها به راحتی میتوانند عملکردی همانند کاربر عادی داشته وسناریوهای جعل هویت را به راحتی پیاده‌ی‌سازی و اجرا کنند.
6. اجرای روال‌های تکراری و بی‌وقفه، بات‌ها به راحتی میتوانند روال‌های تکراری را به صورت مکانیزه و بی‌وقفه ارسال کنند، به راحتی میتوانند APIهایی که توسط یک برنامه موبایل استاندارد (Mobile Application) فراخوانی می‌شوند را صدا بزنند و اصلاحا API مربوطه را Abuse کنند

و موارد متعدد دیگری که قادر به اجرای آن هستند.

آناتومی و ساختار بات‌ها

بات‌های مبتنی بر برنامه کاربردی تحت وب، در حالت کلی به چهار دسته زیر تقسیم می‌شوند:

- بات‌های نسل اول : بات‌های نسل اول ساختار ساده‌ای داشته و روال‌های اتوماتیک ساده را میتوانند اجرا کنند. چنین بات‌هایی درکی از مفاهیم پایه وب همانند Cookie و Session نداشته و به راحتی قابل کشف و بلاک‌کردن هستند. برای مثالی از بات‌های نسل اول می توان یک اسکریپت ساده که محتوای وب یا یک API را با متد GET فراخوانی میکند را نام برد. کشف و بلاک کردن بات‌های نسل اول کمترین هزینه و پیچیدگی را داشته و به راحتی قابل انجام است.
- بات‌های نسل دوم : بات‌های نسل دوم ساختاری ساده همانند بات‌های نسل اول دارند اما کمی بهبود یافته است. بات‌های نسل دوم توان رندرکردن و اجرای کدهای جاوا اسکریپت را نداشته و Stack آنها همانند یک مرورگر کامل نیست. چالش‌های مبتنی بر جاوااسکریپت همانند Set کردن Cookie و موارد مشابه این دست برای شناسایی و بلاک کردن بات‌های نسل دوم کافی است. ابزارهایی همانند Scrapy نمونه‌ای از بات‌های نسل دوم است.
- بات‌های نسل سوم : بات‌های نسل سوم تا حدی چالش برانگیز هستند. بات‌های نسل سوم همانند بات‌هایی که در فریمورک‌هایی همانند PhantomJs یا Selenium توسعه داده می‌شوند، توانایی اجرای گام به گام درخواست‌ها و چالش‌هایی که برای مقابله با بات‌های نسل اول و دوم کفایت ارایه می‌شوند را دارند ولی در Run-time سرعت اجرای کمتری نسبت به بات‌های نسل اول و دوم دارند. شناسایی و بلاک کردن بات‌های نسل سوم به واسطه بکارگیری تکنیک‌هایی همچون آزمونهای چالشی همانند Captcha قابل انجام است.
- بات‌های نسل چهارم : قادر هستند رفتار یک کاربر واقعی با Stack یک مرورگر Embed را به صورت کامل شبیه‌سازی کنند و درخواست‌های ارسالی از سمت چنین بات‌هایی رفتاری همچون رفتار یک کاربر عادی دارد. مرورگرheadless همانند مرورگر Chromium نمونه‌ای از بات‌های نسل چهارم هستند و راهکار مقابله با چنین بات‌هایی بکارگیری تکنیک‌های پیچیده و مبتنی بر هوش مصنوعی است.

چالش بات‌ها و راهکارهای دفاعی فعلی

فایروال‌ها و سیستم‌های کشف نفوذ بی شک به عنوان یکی از مولفه‌های مهم در خط دفاعی و مقابله با حملات سایبری است ولی اساسا چنین سیستمهایی پایش حملات را بر اساس الگوی حملات، تحلیل رفتار و بررسی درخواست‌ها انجام می‌دهند و فهمی از منبع تولید کننده آن درخواست‌ها به صورت کامل ندارند و قادر به تمیز کردن اینکه درخواست ارسالی از سمت کاربر است یا یک ربات را ندارند. بررسی و شناسایی بات‌ها و بلاک کردن آنها ممکن است در برخی موارد توسط چنین سیستم‌هایی بتواند با موفقیت همراه باشد ولی در موارد پیشرفته و در مواجه با بات‌های نسل سوم و چهارم عملا قادر به کشف و بلاک‌کردن چنین حملات و تفکیک منبع تولید کننده درخواست‌ها از کاربر عادی یا یک ربات به صورت کامل نیستند و به راحتی بات‌ها میتوانند مکانیزم کشف و بلاک کردن چنین تجهیزاتی را دور بزنند.

کشف، شناسایی و بلاک کردن بات‌های لایه 7 در معماری امنیتی و در زمان استقرار در توپولوژی شبکه، یک لایه پیش‌تر از تجهیزات امنیتی همانند فایروال‌های برنامه‌های کاربردی تحت وب (همانند WAF) و یا سرورها/ سرویس‌های آنلاین و معمولا بعد از تجهیزات شبکه مستقر در لایه 3/4 است. در چنین معماری تنها درخواست‌های کاربران واقعی به سمت لایه‌ها و سرویس‌های مستقر شده بعدی ارسال می‌شود و درخواست‌های بات‌ها تماما مسدود و پایش می‌شود.

حملات بات‌ها و شکل توزیع شده آن، به راحتی می‌توانند تجهیزات امنیتی همانند فایروالهای برنامه کاربردی تحت‌وب و سیستم‌های کشف نفوذ لایه ۷ را از مدار خارج کنند و یا با ایجاد درخواستهای بالا باعث ایجاد Race Condition یا افت شدید QoS در عملکرد چنین سیستم‌هایی شوند. لازم است ابتدا درخواستهای کاربر از ترافیک آلوده تفکیک و پایش شده و تنها درخواست کاربران واقعی به لایه بعدی و زنجیره پردازشی منتقل شود.

روباه آهنی به عنوان یک سامانه برای کشف و بلاک کردن بات‌ها با توان پردازشی بالا و مقیاس‌پذیر است که توانایی بررسی منبع ارسال کننده درخواست و تفکیک آن به کاربر واقعی یا ربات را کاملا Agent-Less و به صورت برخط داشته و تنها درخواستهای کاربر انسانی به سمت تجهیزات امنیتی لایه 7 یا سرویس‌های Back-End ارسال خواهد شد.

یک نکته قابل توجه آن است که ماموریت فایروالهای امنیتی و سیستم های کشف نفوذ و در یک جمله راهکارهای امنیتی لایه 7 متفاوت با ماموریت سامانه روباه‌آهنی نیست ولی پیچیدگی حملات مبتنی بر بات‌ها و تحلیل منبع ارسال کننده آن حملات و تحلیل درخواست‌ها، موضوعی پیچیده بوده و از عهده فایروالها و سیستم تشخیص نفوذ لایه ۷ خارج است و امکان افت شدید در عملکرد، False Positive و Bypassشدن چنین تجهیزاتی امکان‌پذیر است.

راهکاری تجاری و متن‌باز

شرکت DataDome به عنوان یکی از مدعیان و پیشرویان فناوری در حوزه تکنولوژی کشف و بلاک‌کردن بات‌ها در کشور فرانسه می‌باشد. راهکارهای تجاری این شرکت مبتنی بر هوش مصنوعی می‌باشد و خدمات BOT Protection As a Service را ارایه می‌دهند. همچنین شرکت‌های مطرحی همانند CloudFlare و Imperva سرویس خدمات CDN را به همراه حفاظت از کسب و کارهای آنلاین ارایه می‌دهند. محصولات F5 نیز شامل ماژول‌هایی برای کشف و بلاک‌کردن بات‌ها و حفاظت از APIهای سمت سرور را فراهم می‌کند.

راهکارهای متن‌باز همانند ماژول تست کوکی که که به عنوان یک ماژول ساده و کاربردی برای Nginx طراحی و توسعه داده شده است، با ایجاد چالش JavaScript و Set کردن کوکی در مرورگر کاربر تلاش میکند تا درخواست‌های نامعتبر را به واسطه بررسی کوکی اعتبار سنجی و درخواستهای نامعتبر را مسدود کنند. این راهکار به راحتی قابل دور زدن توسط بات‌های نسل اول است و مهاجم میتواند با Dump کردن هدرهای درخواست ابتدایی (تنها برای یکبار) و رمزگشایی و Set کردن کوکی استخراج شده ، در دفعات بعدی همان مقادیر را در درخواستهای ارسالی به سمت سرور ارسال کند (همانند حمله CSRF شامل هدرهای نخستین درخواست و اطلاعات کوکی). از آنجایی که در دفعات بعدی اطلاعات صحیح و درخواست معتبر به سمت سرور ارسال می‌شود به راحتی می‌توان چنین تکنیک‌هایی را Bypass کرد.

در فایروال‌ها و سیستم‌های کشف نفوذ تولید داخل و صنعتی خارجی با تکنیک‌هایی همانند بررسی کردن Agent و یا آدرس IP و موارد دیگرهمانند الگوی حملات (Database of Attacks Pattern) تلاش میشود که درخواست‌های مربوط به بات‌ها شناسایی و مسدود گردد. این تکنیک‌ها و استراتژی‌های بکار رفته به راحتی قابل دور زدن است و هیچ پیچیدگی برای مهاجم ندارد.

روباه آهنی

روباه‌آهنی یک سامانه نرم‌افزاری و کاملا اختصاصی برای کشف و بلاک‌کردن بات‌های برنامه کاربردی تحت وب و حفاظت از سرویس‌های آنلاین طراحی و توسعه داده شده است و قابلیت استقرار در یک سخت‌افزار فیزیکی(Hardware Appliance) و یا در یک ماشین مجازی (Virtual Appliance) به عنوان یک سامانه مستقل بوده و در حالت استقرار در توپولوژی شبکه در مد پروکسی معکوس (Reverse Proxy) و بر خط (In-Line) ترافیک شبکه را پایش و درخواست‌های ارسالی از سمت مهاجمین (بات)ها را شناسایی و مسدود خواهد کرد.

سامانه نرم‌افزاری روباه‌آهنی یک راهکار یکپارچه با توان پردازشی بالا و مقیاس‌پذیر (کلاستر شدن) است و در مد توزیع‌شدگی با Latency نزدیک به صفر، توان پردازش میلیون‌ها نشست/ثانیه واقعی و به صورت In-Line را دارد. این محصول در داخل کشور هیچ نمونه مشابه تجاری یا متن‌بازی نداشته و برخی از شاخص‌ها و مزیت رقابتی این محصول با نمونه‌های خارجی و تجاری می‌تواند شامل موارد زیر باشد:

- ✔ **دانش بومی و امکان بهبود و شخصی سازی**
  - محصول توسعه داده شده و فناوری آن در حوزه تخصصی آن در لبه دانش است و دارای تکنولوژی اختصاصی برای کشف و بلاک‌کردن حملات است. تمامی محصول در داخل کشور و تیم مربوط به پروژه توسعه و نگهداری شده و امکان بهبود، رفع ایراد و شخصی‌سازی آن به صورت کامل و همیشه ممکن خواهد بود.
- ✔ **امکان Integrated شدن با بقیه محصولات و خدمات**
  - محصولاتی که بتوانند با محصولات و خدمات دیگر ادغام شوند شانس موفقیت و عملیاتی شدن بالایی را دارند. معماری، ساختار هسته و ماژوهای روباه‌آهنی به گونه‌ای طراحی و انتخاب شده است که با حداقل هزینه اجرایی و توسعه، بتوان سرویس‌های هسته روباه‌آهنی را برای فراخوانی در Third Party ادغام کرد. این کار به واسطه API ها و کتابخانه‌هایی است که توسط سامانه در دسترس برنامه‌نویسان و توسعه‌دهندگان قرار میگیرد.
- ✔ **هزینه پایین و عدم خروج ارز از کشور**
  - در مقایسه با محصولات و راهکارهای تجاری موجود، کل هزینه تولید و نگهداری و همچنین پشتیبانی سامانه بات‌گارد ده‌ها برابر کمتر از نمونه‌های خارجی آن است.

- ✔ **ارایه سرویس، خدمات و مقابله با حملات سایبری در داخل:**
  - به عنوان یک محصول داخلی با شرح خدمات معیین، امکان استقرار و ارایه خدمات و سرویس‌ها به صورت بومی و در داخل کشور کاملا میسر است، برای مثال، دیگری نیازی به روتینگ ترافیک به سمت CDNهای سرویس خارجی مثلا DataDome نبوده و مساله محرمانگی و امنیت داده به صورت محلی و بومی مدیریت و پایش خواهد شد.
- ✔ **محصولی با توان پردازشی بالا و با کمترین هزینه پیکربندی و نگهداری**
  - امروزه بات‌ها آنقدر بهبود یافته و بروزشده هستند که دیگر با مکانیزم حفاظت مربوط به فناوری‌های نسل دوم و سوم محصولات امنیتی همچون دیواره آتش لایه شبکه (Network Firewalls/ IDS/ IDP) و یا حتی فایروال‌های وب (WAF) امکان حفاظت کامل از سرویس‌ها و سرورها در مقابل فعالیت‌ها و حملات بات‌ها به صورت کامل وجود ندارد. نگهداری و بروز کردن بانک اطلاعتی و ایجاد رول‌های امنیتی برای چنین تجهیزاتی هزینه زمانی، مالی و اجرایی با امکان خطای انسانی به همراه دارد. روباه‌آهنی رویکردی جدید به حل مساله بات‌ها دارد و با حداقل هزینه پیکربندی و نگهداری وظیفه خود را اجرا خواهد کرد. روباه‌آهنی مبتنی بر بانک‌اطلاعاتی یا الگوی شنناسایی حملات نبوده و با نگرشی جدید مساله را حل میکند.
- ✔ **بهبود خدمات و خلق نسل جدیدی از محصولات امنیتی**
  - با انتقال دانش و ادغام آن در محصولات امنیتی دیگر همانند فایروالهای کاربردی تحت وب (WAF) یا ارایه دهنده‌گان سرویس‌های آنلاین همانند سرویس‌دهنده‌های خدمات ابری، می‌توان به نسل جدیدی از محصولات،خدمات امنیتی و سرویس‌های پایدار دست پیدا کرد که بتواند نیاز امنیتی فضای تبادل اطلاعات کشور را به شکل مناسبی پوشش دهد.