خبرنامه الکترونیکی ۵۵

مرکز تخصصی آپا دانشگاه سمنان

شماره پنجاه و پنجم، سال پنجم، دی ۱۴۰۱ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

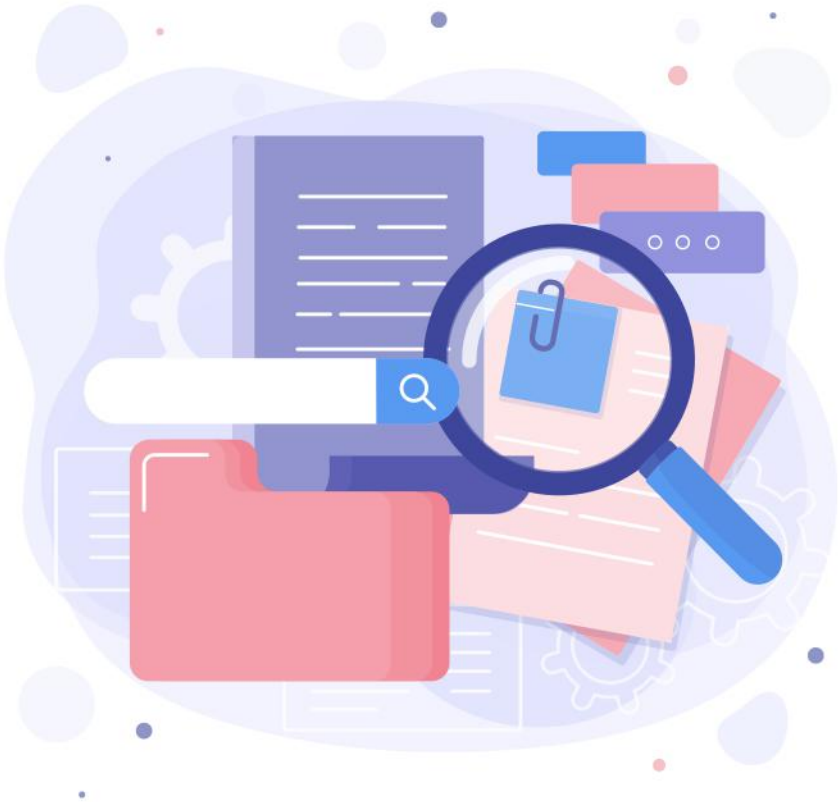
https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

"تنها سیستمی که به معنی واقعی امن محسوب می‌شود، سیستمی است که خاموش بوده، از اتصال برق کشیده شده، داخل یک گاوصندوق تیتانیومی قرار داده شده، در یک محفظه بتنی دفن شده باشد و پیرامون آن با گاز کشنده اعصاب و محافظین زبده محصور شده باشد. حتی با این شرایط، حاضر نیستم روی امنیت این سیستم شرط‌بندی کنم."

"گِن اسپافورد"
مدیر بخش عملیات کامپیوتری
و تکنولوژی امنیت دانشگاه پُردو

مرکز آپا دانشگاه سمنان

فهرست



مرکز آپا دانشگاه سمنان

خبر

بدافزار جدید لینوکس

از ۳۰ اکسپلویت پلاگین برای backdoor سایت‌های وردپرس استفاده می‌کند

یک بدافزار لینوکس که قبلا ناشناخته بود، از ۳۰ آسیب‌پذیری در چندین افزونه[1] و تم های قدیمی وردپرس برای تزریق کد جاوا اسکریپت مخرب سوء استفاده کرده است.

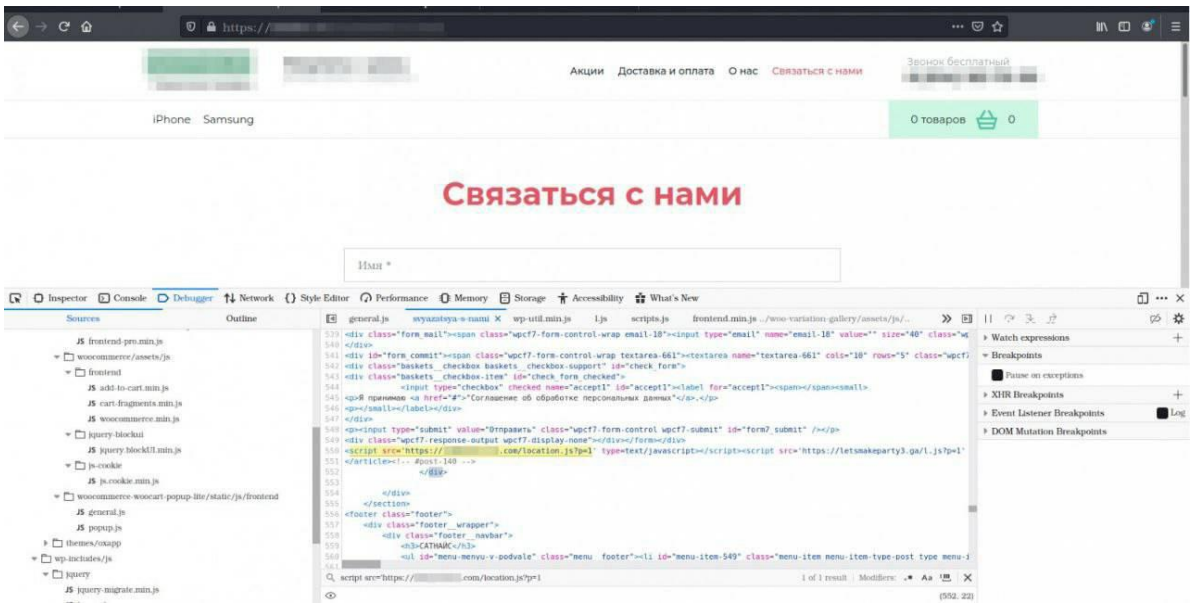
طبق گزارش فروشنده آنتی ویروس Dr.Web، این بدافزار سیستم‌های لینوکس ۳۲ بیتی و ٦٤ بیتی را هدف و به اپراتور خود قابلیت فرمان از راه دور را می‌دهد.

عملکرد اصلی تروجان هک کردن سایت‌های وردپرس با استفاده از مجموعه‌ای از اکسپلویت‌های کدگذاری شده است که به صورت متوالی اجرا می‌شوند، تا زمانی که یکی از آنها کار کند.

پلاگین‌ها و تم‌های مورد هدف به شرح زیر است:

WP Live Chat Support Plugin
WordPress – Yuzo Related Posts
Yellow Pencil Visual Theme Customizer Plugin
Easysmtp
WP GDPR Compliance Plugin
Newspaper Theme on WordPress Access Control (CVE-2016-10972)
Thim Core
Google Code Inserter
Total Donations Plugin
Post Custom Templates Lite
WP Quick Booking Manager
Faceboor Live Chat by Zotabox
Blog Designer WordPress Plugin
WordPress Ultimate FAQ (CVE-2019-17232 and CVE-2019-17233)
WP-Matomo Integration (WP-Piwik)
WordPress ND Shortcodes For Visual Composer
WP Live Chat
Coming Soon Page and Maintenance Mode
Hybrid

اگر وب‌سایت مورد نظر یک نسخه قدیمی و آسیب‌پذیر از هر یک از موارد بالا را اجرا کند، بدافزار به طور خودکار جاوا اسکریپت مخرب را از سرور فرمان و کنترل خود (C۲) دریافت می‌کند و اسکریپت را به سایت تزریق می‌کند.



۱-پلاگین

صفحاتی که کد در آنها تزریق شده به عنوان یک هدایت‌کننده به مکانی که هکر می‌خواهد عمل می‌کنند، در نتیجه این فرایند در سایت‌هایی که متروکه هستند بهترین عملکرد را دارد.

این تغییر مسیرها ممکن است در کمپین‌های فیشینگ، توزیع بدافزار و موارد دیگر برای کمک به فرار از شناسایی و مسدود شدن فرد مهاجم استفاده شود. با این حال، اپراتورهای تزریق خودکار کد ممکن است خدمات خود را به مجرمان سایبری دیگر بفروشند.

طی آپدیت جدیدی که Dr.Web از payloadها منتشر کرد، افزونه‌های زیر نیز مورد هدف واقع شده است:

WP Live Chat Support Plugin
WordPress – Yuzo Related Posts
Yellow Pencil Visual Theme Customizer Plugin
Easysmtp
WP GDPR Compliance Plugin
Newspaper Theme on WordPress Access Control (CVE-2016-10972)
Thim Core
Google Code Inserter
Total Donations Plugin
Post Custom Templates Lite
WP Quick Booking Manager
Faceboor Live Chat by Zotabox
Blog Designer WordPress Plugin
WordPress Ultimate FAQ (CVE-2019-17232 and CVE-2019-17233)
WP-Matomo Integration (WP-Piwik)
WordPress ND Shortcodes For Visual Composer
WP Live Chat
Coming Soon Page and Maintenance Mode Hybrid

افزونه‌های جدید که مورد هدف قرار گرفتند نشانگر این است که توسعه backdoorها شروع شده است.

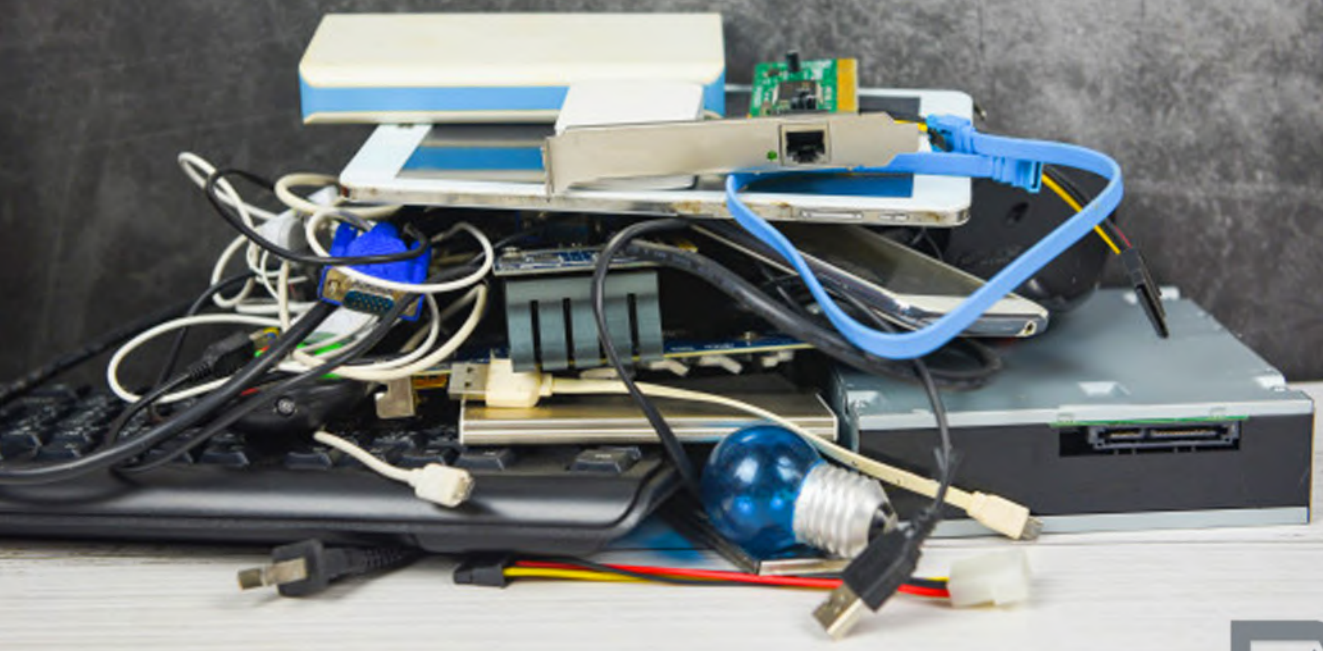
Dr.Web همچنین اشاره می‌کند که هر دو نوع افزونه‌هایی که بالا به آن اشاره شده دارای عملکردی هستند که در حال حاضر غیرفعال است که امکان حملات بی‌رحمانه علیه حساب‌های مدیر وب‌سایت را فراهم می‌کند .

برای دفاع در برابر این تهدید، مدیران وب‌سایت‌های وردپرس باید تم‌ها و افزونه‌های در حال اجرا در وب‌سایت را به آخرین نسخه موجود به‌روزرسانی کنند و آن‌هایی را که دیگر توسعه نمی‌یابند با جایگزین‌هایی که پشتیبانی می‌شوند جایگزین کنند.

استفاده از رمزهای عبور قوی و فعال کردن مکانیسم احراز هویت دو مرحله‌ای می‌بایست از محافظت در برابر حملات brute-force اطمینان حاصل کند.

نگذارید!

دیگران زباله ها؟
شما را بازیافت و
به طلا (اطلاعات)
تبدیل کنند.



مرکز آپا دانشگاه سمنان

مرکز آپا دانشگاه سمنان

آموزش

مدیریت Regex در XDP در حفاظت از حمله DDoS

در حفاظت از حمله DDoS، Gcore از پک نرم‌افزار XDP و عبارات منظم[1] استفاده می‌کند. این مقاله توضیح خواهد داد که چرا Gcore شروع به استفاده از این راه حل (regex در XDP) کرد و چگونه آنها را متصل به یک موتور شخص ثالث و توسعه API کرد.

علاوه بر این، ما همچنین راه حل منبع باز آنها را برای مدیریت regex در XDP و نتایج بنچمارک توضیح خواهیم داد.

دلیل استفاده از XDP framework

در روزهای اولیه خدمات حفاظتی DDoS، آنها بر روی تعداد کمی از سرورهای اختصاصی (گره‌ها) که DPDK (یک framework لینوکس برای پردازش سریع داده ها) را اجرا می‌کردند و ترافیک را با عبارات منظم فیلتر می‌کردند، کار می‌کردند. با استفاده از این فناوری، آنها با موفقیت از برنامه های مشتریان خود به لطف این bundle محافظت می کنند. با این حال، از آنجایی که ظرفیت حملات DDoS از 300 گیگابیت بر ثانیه در سال 2021 به 700 گیگابیت در ثانیه در سال 2022 افزایش یافت، در نهایت زیرساخت های زیربنایی ناکافی بودند.

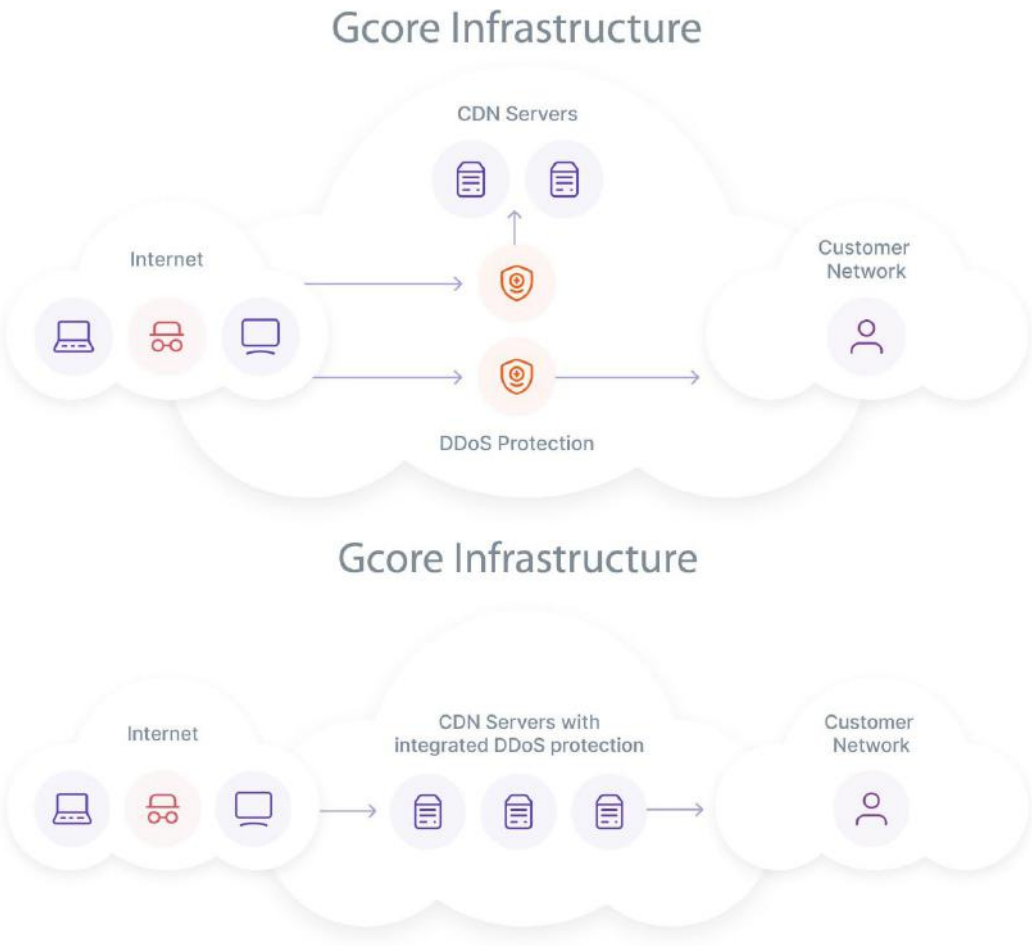
DPDK برای عملکرد مؤثر به دسترسی آداپتور شبکه انحصاری نیاز دارد. به این ترتیب، ادغام آن با سایر کاربردها بسیار دشوار (و غیر معقول) و تا حدی غیرممکن است. اگر بخواهیم زیرساخت موجود بدون تغییر رشد کند، این نیاز به دستیابی به گره‌های اختصاصی جدید برای DPDK دارد. Gcore به این نتیجه رسید که این گزینه مقرون به صرفه نیست و به دنبال یافتن راه کاری جدید شد.

علاوه بر خدمات حفاظتی از DDoS، Gcore زیرساخت شبکه تحویل محتوا[2] متشکل از بیش از هزار گره CDN را نیز ارائه می‌کند. بنابراین، منطقی است که آنها شروع به استفاده از آن برای توزیع محتوا و غربالگری ترافیک کنند، زیرا گره های بیشتر به معنای امنیت بهتر در برابر مهاجمان قدرتمندتر است.

از آنجایی که DPDK نمی تواند با گره های CDN کار کند (به گره های اختصاصی نیاز دارد)، Gcore ترجیح داده است به جای آن ازXDP framework استفاده کند. آنها ادعا می کنند که پیشرفت اصلی نسبت به نسخه قبلی این است که چگونه به خوبی در پشته(داده) با سایر برنامه‌ها ادغام می‌شود.

1-regex
2-CDN

DDoS Protection قبلا فقط در سرورهای اختصاصی با DPDK در دسترس بود (شکل 1)، اما اکنون می‌توان آن را در سرورهای CDN ادغام کرد (شکل 2) که امکان مقیاس‌پذیری بیشتر را فراهم می‌کند.



شکل 2: حفاظت از حمله DDoS ادغام شده در سرورهای CDN (XDP)

چرا Gcore XDP را مفید می‌داند:

- بهره‌وری در هزینه. این فریم ورک را می‌توان بر روی سرورهایی با هر برنامه کاربردی edge-network، مانند سرورهای وب و سرورهای DNS نصب کرد، بنابراین نیازی به تجهیزات اختصاصی گران قیمت ندارد، و توسعه‌دهندگان نیازی به صرف ساعت‌ها برای ادغام سایر برنامه‌ها با XDP ندارند.
- سرعت تشخیص حمله. این فریم ورک را می‌توان بر روی صدها سرور CDN نصب کرد. این بدان معناست که DDoS Protection به برنامه‌های مشتری و منابع ترافیک مخرب نزدیک‌تر است. در نتیجه، حملات سریعتر متوقف می‌شوند و به عمق زیرساخت نمی‌روند.

اما چندین ایراد نیز دارد:

- عملکرد پایین‌تر. گره های جدا شده با XDP در مقایسه با DPDK عملکرد پایین تری دارند، اما به دلیل ادغام گره های بیشتر، کارایی کلی راه حل در نهایت بالاتر است.
- ناتوانی در کنترل regex . XDP هیچ موتور داخلی برای مدیریت عبارات منظم ندارد، بنابراین آنها مجبور بودند راه حلی برای تطبیق پردازش عبارت منظم با آن بیابند.

چرا Gcore به استفاده از regex برای فیلتر کردن ترافیک ادامه داد؟

دو رویکرد برای فیلتر کردن ترافیک مخرب در DDoS Protection وجود دارد: تجزیه کننده های بسته و مدیریت عبارات منظم (regex).

تجزیه کننده‌های داده فیلترهایی هستند که به صورت دستی نوشته شده‌اند که برای شناسایی و مسدود کردن فعالیت‌های مشکوک در برنامه‌ها با استفاده از یک پروتکل خاص برنامه‌ریزی شده‌اند. نوشتن چنین تجزیه کننده‌های بسته نیازمند برنامه‌نویسی زیادی است، به خصوص اگر Protection DDoS نیاز به پذیرش سریع پروتکل‌های جدید داشته باشد.

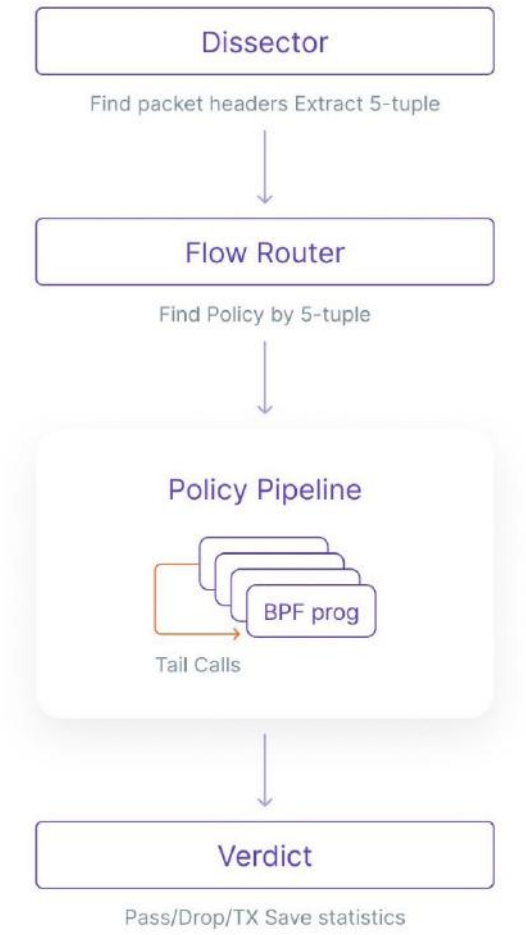
مدیریت regex بر اساس تجزیه و تحلیل ترافیک داده‌ها، زمان لازم برای ایجاد فیلترها را در مقابل رویکرد تجزیه کننده داده را کاهش می‌دهد. علاوه بر این، این یک رویکرد انعطاف‌پذیرتر است که به داده‌ها اجازه می‌دهد با کارآمدی بیشتری با ترافیک هسته کمتر پردازش شوند.

بسته‌هایی که به برنامه‌های مشتریان ارسال می‌شوند در دو حالت بررسی می‌شوند:

- واکنش به حملات (حالت دستی). آنها ترافیک مخرب ایجاد شده توسط یک بار (الگو) خاص را تجزیه و تحلیل می‌کنند. سپس عبارات منظمی ایجاد می‌کنند که به این محموله اشاره دارد و آن را در ترافیک اعمال می‌کنند. تمام درخواست‌هایی که حاوی محموله مشابه هستند به‌طور خودکار فیلتر می‌شوند.
- حالت حفاظت از اتصال بازی. بسیاری از مشتریان Gcore ارائه دهندگان خدمات بازی آنلاین هستند که با درخواست‌هایی از طریق پروتکل UDP و اندازه بسته‌های کوچک مشخص می‌شوند. بسته‌هایی که به سرویس‌های بازی می‌آیند ساختار دقیقی دارند که می‌توان آن را با استفاده از عبارات منظم توصیف کرد. آنها عبارات منظمی را برای سرویس بازی هر مشتری ایجاد می‌کنند و از آن برای ایجاد لیست مجاز بسته‌ها استفاده می‌کنند. تمام بسته‌هایی که با عبارات منظم مطابقت دارند مجاز خواهند بود. اگر بسته‌ها متفاوت باشند، مسدود می‌شوند.

پردازش بسته هنگام استفاده از regex به صورت زیر مرتب می شود:

- هر بسته را تجزیه و تحلیل می‌کند و آن را به هدر تقسیم می‌کند.
- مسیریاب جریان. بسته‌ها را به نمایه حفاظتی مناسب هدایت می‌کند، که مجموعه‌ای از قوانین برای حفاظت از ترافیک است.
- Policy Pipeline. قوانین خاصی (اقدامات متقابل) را برای بسته‌های جدا شده به اجزا اعمال می‌کند. یکی از اقدامات متقابل استفاده از عبارات منظم است.
- verdict(قضاوت/نظر). بسته‌ای را بر اساس بررسی‌های اقدام متقابل رد یا مسدود می‌کند.



چگونه Gcore پردازش regex را در زمینه XDP تطبیق می‌دهد:

چالش ها و راه حل ها

کار با regex یک فرآیند فشرده منابع است و Gcore ادعا می‌کند که میلیون‌ها بسته را بررسی می‌کند و از عبارات منظم با پیچیدگی‌های مختلف استفاده می‌کند. این باعث شد که آنها به این نتیجه برسند که کارایی[1] یک نیاز ضروری برای یک موتور regex است.

بهترین موتور موجود Hyperscan است که توسط اینتل طراحی شده است. این منبع باز[2] با مجوز سازگار با GPL است که سریع عمل می‌کند زیرا از مجموعه دستورالعمل‌های AVX2/AVX512 استفاده می‌کند و به عنوان استاندارد صنعتی برای برنامه‌های DPI استفاده می‌شود.

برای تطبیق پردازش regex در XDP، آنها با چندین چالش مواجه شدند که در زیر توضیح داده شده است.

چالش ۱. محدودیت‌های eBPF اجازه نمی‌دهد که فیلترهای regex به عنوان بخشی از برنامه XDP اجرا شوند.

راه حل: Gcore موتور Hyperscan را به‌عنوان یک ماژول هسته لینوکس قابل بارگذاری که کمک‌های eBPF را ارائه می‌کند، بازسازی کرد. Hyperscan موتوری است که برای پردازش عبارات منظم در سیستم‌های DPI (بازرسی بسته عمیق) طراحی شده است و بررسی می‌کند که آیا بار بسته بسته با هر عبارت منظم از پیش تعریف شده مطابقت دارد یا خیر.

چالش 2. کمک‌کننده‌های eBPF از ماژول‌های قابل بارگیری، نمی‌توانند برای XDP ثبت شوند.

راه‌حل: کمک‌کنندگان eBPF در ماژول‌های قابل بارگذاری برای اولین بار در لینوکس 5.16 معرفی شدند، اما ثبت آنها برای XDP تا لینوکس 5.18 امکان‌پذیر نبود. از آنجایی که Gcore در طول توسعه فقط لینوکس 5.17 را داشت، آنها مجبور بودند این امکان را فراهم کنند. ساختار های هسته اصلی نیازی به این نوع تغییرات ندارند.

چالش 3. دستورات FPU قرار نبود در طول پردازش داده در هسته لینوکس استفاده شود.

راه حل: آنها با ورود به ماژول برای پردازش regex، وضعیت رجیسترهای FPU را ذخیره و بازیابی می کنند.

آنها این کار را در هر داده در صورت نیاز انجام می دهند بدون اینکه روی داده های دیگری که پردازش regex برای آنها نیازی نیست تأثیر بگذارند.

Gcore چه راه حل منبع باز به جامعه ارائه می‌دهد:

eBPF API برای مدیریت regex در XDP

اگر زیرساخت شما نیاز به مدیریت عبارات منظم در XDP دارد، می‌توانید به جای اینکه کار خود را سخت کنید، از یک راه‌حل آماده ارائه شده توسط توسعه‌دهندگان آن‌ها استفاده کنید.

کمک کننده سفارشی eBPF آنها "bpf_xdp_scan_bytes()" اکنون می‌تواند به همان روشی که سایر کمک کنندگان eBPF استفاده می‌شود.

```
echo '101:/foobar/' > patterns.txt
echo '201:/a{3,10}/' > patterns.txt
build/bin/hscollider -e patterns.txt -ao
out/ -nl

1.    dd if=$(echo out/".db) of=/sys/
kernel/config/rex/hello/database
```

برای ارزیابی regex دربرابر buffer داده، ابتدا یک regex را به ماژول قابل بارگیری اضافه کنید و هنگام فراخوانی eBPF helper به شناسه آن ارجاع دهید:

1. یک گره با استفاده از mkdir در /sys/kernel/con-fig/rex ایجاد کنید.
2. کامپایل پایگاه داده الگو:
3. Regex کامپایل شده را در /sys/kernel/config/rex/<node>/database آپلود کنید:
4. خواندن یا تنظیم یک شناسه regex جدید در /sys/kernel/config/rex/<node>/id
5. شناسه regex را به برنامه eBPF منتقل کنید و به عنوان آرگومان کمکی استفاده کنید.

کد منبع کامل در حساب Gcore GitHub در لینک زیر موجود است:

https://github.com/G-Core/linux-regex-module

1-performance

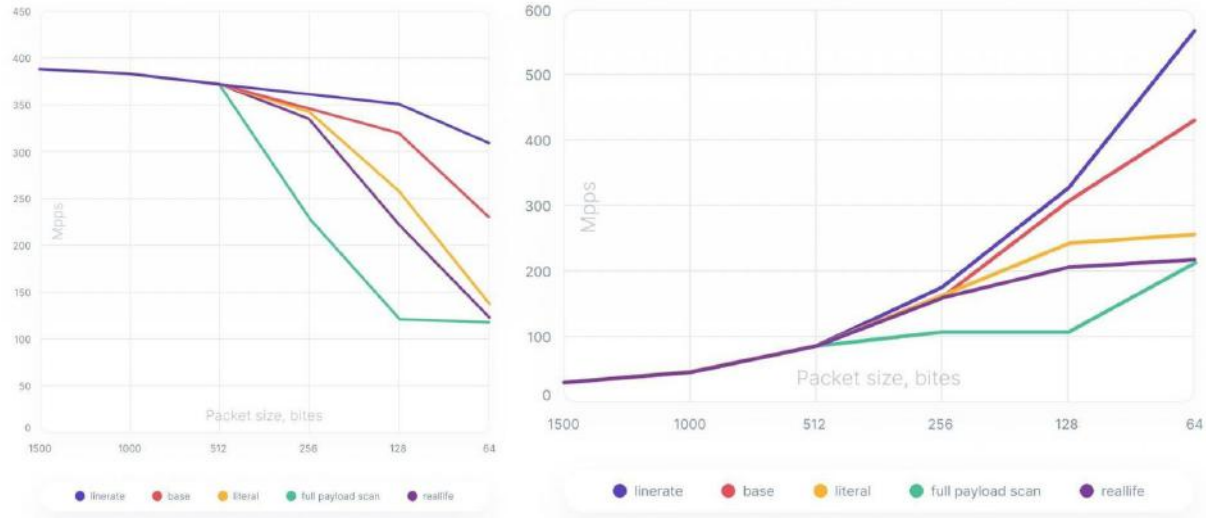
Gcore چه معیارهایی در استفاده از regex در XDP دارد:

راه‌حل فیلتر DDoS آنها مبتنی بر نسل سوم پردازنده‌های مقیاس‌پذیر Intel® Xeon® و آداپتور شبکه اترنت اینتل E810 با ظرفیت 100 گیگابایت است. Intel® Hyperscan تطبیق الگوی با کارایی بالا را در جریان های داده فعال کرد.

اینتل بینش تخصصی، از جمله در مورد فناوری XDP که برای فیلتر کردن بسته ها استفاده می شد، ارائه کرد.

به گفته آنها، استفاده از نرم افزار جدید در آخرین نسل سوم پردازنده های Intel® Xeon® Scalable ظرفیت فیلتر را از 100 گیگابیت بر ثانیه به 400 گیگابیت در ثانیه یا 200 میلیون بسته در ثانیه افزایش داده است.

در نمودارهای زیر می توانید نتایج آزمایش را ببینید.



- خط آبی حداکثر توان عملیاتی شبکه 4 × 100 گیگابیت بر ثانیه است.
- پایه (خط قرمز) معیاری است که نشان می‌دهد XDP چگونه بدون استفاده از عبارات منظم آن را مدیریت می‌کند.
- سه خط پایین مربوط به مدیریت بسته‌ها هنگام استفاده از عبارات منظم است.

نتیجه: در یک بسته (داده) بزرگتر از 512 بایت، سیستم می تواند با سرعت خط کار کند و به طور موثر ترافیک را فیلتر کند. در بسته های کوچکتر از 512 بایت، نرخ بسته و فشار برای سیستم بسیار بالاتر است و سیستم نمی تواند عملکرد خطی را حفظ کند و تقریباً در 40 تا 50 درصد سرعت خط کار می کند.

Gcore واقعا از این نتایج راضی است. بر اساس داده‌های آنها، آنها برای ما مناسب هستند، حتی اگر عملکرد پردازش بسته‌های کوچک چندان بالا نباشد. از آنجایی که حملات DDoS واقعی تمایل به استفاده از بسته های بزرگ دارند، کارایی و سرعت آن به اندازه کافی قابل قبول است.

آزمایش‌ها نشان می‌دهند که استفاده از regex در XDP برای پردازش فرآیندهای سنگین مناسب است، که در حال حاظر سرعت کافی برای مدیریت ترافیک زیاد را دارد.

منبع:

https://www.bleepingcomputer.com/news/security/how-gcore-uses-regular-expressions-to-block-ddos-attacks/

مرکز آپا دانشگاه سمنان

خبر کوتاه

هوش مصنوعی جدید مایکروسافت پس از سه ثانیه تقلید صدا می‌کند!

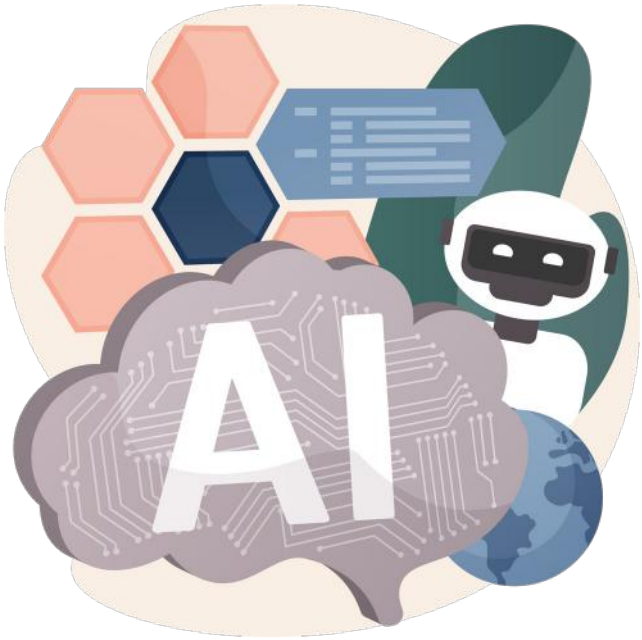
1

semCERT
@semcert

⭕ #هوش_مصنوعی جدید #مایکروسافت پس از سه ثانیه تقلید صدا می‌کند!

🔸 امروزه همواره ابزارهای هوش مصنوعی که تصاویر و متون را از هیچ می‌سازند موضوع روز هستند، که می‌توان به ChatGPT و DALL-E اشاره کرد.

Translate Tweet



2

semCERT
@semcert

جایی موضوع جالب می‌شود که ماکروسافت در هردو هوش‌مصنوعی ارائه شده دخیل بوده و حال Vall-E را عرضه می‌کند که صدا را تقلید می‌کند.

🔹 برای مدتی طولانی، هوش مصنوعی چیزی جز یک کلید واژه خالی برای توصیف یادگیری ماشینی نسبتاً پیش پا افتاده نبود ولی حال نقش آن پررنگ‌تر می‌شود.

Translate Tweet

3

semCERT
@semcert

✅ منبع:
isna.ir/news/140110211...ربات-جدید-مایکروسافت-هر-صدایی-را-تقلید-می-کند

@semcert ID

Translate Tweet

تلاش ما
حفظ امنیت
شماست...