رونوشت:

- دبیرخانه محترم شورای عالی فضای مجازی (نسخه سیاستی)
- معاونت محترم فنی شرکت ارتباطات زیرساخت

گزارش فنی کلیدهای حیاتی در طراحی و اجرای سانسور هوشمند و پایدار اینترنت پیشنهاد مدل گشایش مرحله‌ای کنترل‌شده، شناسایی حفره‌های فنی و راهکارهای بستن آن‌ها

تهیه‌کننده :تیم تحقیقاتی دکتر رسول جلیلی – گروه فنی امن‌افزار گستر شریف

تاریخ: شهریور ماه ۱۴۰۴

نسخه :۲.۲

چکیده :

مدیریت جریان ترافیک اینترنت خارجی نیازمند تعادل دقیق میان تسهیل دسترسی مشروع و حفظ حاکمیت سایبری است. تنها راهکار پایدار، اجرای گشایش مرحله‌ای و کاملاً کنترل‌شده می‌باشد. این گزارش چهار مرحله گشایش را به عنوان مدل پیشنهادی ارائه می‌دهد که هر مرحله دارای هدف فنی و عملیاتی مشخص است. حفره‌های فنی هر مرحله با signature های اختصاصی، محدودسازی‌های کاربردی و مسدود سازی پروتکل‌های غیرضروری مسدود می‌گردد. پیشنهادهای کلیدی شامل محدودسازی ارسال فایل در پیام‌رسان‌های داخلی، ممنوعیت ارسال فایل بدون احراز هویت در آپلودرهای ایرانی، مسدود سازی کامل IPv6، UDPوICMP به سمت خارج، اولویت‌دهی گشایش سایت‌های حیاتی ابتدا به اپراتورهای همراه و الزام ۱۰۰ درصدی سایت‌ها و خدمات ایرانی به شبکه توزیع محتوا ملی است. اجرای این مدل، بر اساس شبیه‌سازی‌های انجام‌شده، نشت ترافیک غیرمجاز را تا ۹۷ درصد کاهش خواهد داد.

مقدمه :

تجربه عملیاتی سال‌های ۱۴۰۱ تا ۱۴۰۳ نشان داده است که گشایش ناگهانی و بدون پیش‌تحلیل فنی، به سرعت به اصلی‌ترین عامل فعال‌سازی ابزارهای دورزدن لایه ۴ و ۵ تبدیل می‌شود. تیم تحقیقاتی با دسترسی به داده‌های خام شبکه ملی اطلاعات،این الگوی تکرارشونده را شناسایی کرده است. مدل پیشنهادی حاضر، چهارمرحله‌ای گشایش تدریجی است که در هر مرحله هدف دقیق اعلام می‌شود، حفره‌های فنی پیش‌بینی و signature های مربوطه آماده‌سازی می‌گردد و مکانیسم نظارت بلادرنگ و بازگشت فعال می‌باشد.

مرحله اول: کاهش محدودیت‌ها در اپلیکیشن‌ها و خدمات ملی: این مرحله با هدف بهبود کیفیت تجربه کاربری خدمات داخلی بدون ایجاد هیچ مسیر مستقیمی به اینترنت خارجی اجرا می‌شود. تمرکز صرفاً بر ترافیک داخل شبکه ملی اطلاعات است. در این مرحله، امکان پنهان‌سازی ترافیک تونلینگ داخل جریان‌های مجاز پیام‌رسان‌ها و خدمات بانکی وجود دارد. برای مقابله با این حفره، اعمال DPI نسل سوم با signature های رفتاری و مبتنی بر payload ضروری است. همچنین ارسال فایل در پیام‌رسان‌های داخلی باید به حداکثر ۵ مگابایت در هر جلسه محدود شود، اسکن بدافزار سمت سرور الزامی گردد و فرمت‌های اجرایی به طور کامل ممنوع اعلام شود. نظارت لحظه‌ای بر آنتروپی ترافیک و توزیع اندازه بسته‌ها نیز باید به صورت پیوسته انجام گیرد.

مرحله دوم: وایت‌لیست کردن سایت‌های حیاتی: این مرحله برای جلوگیری از اختلال در کسب‌وکارهای قانونی و ارتباطات رسمی طراحی شده است. در اینجا، باز شدن resolver های DNS و AnyCast شبکه توزیع محتواها

می‌تواند امکان domain fronting و مسیریابی ترافیک VPN را فراهم کند. راهکار تیم، وایت‌لیست granular به صورت ترکیبی از FQDN، پیشوند نشانی IP و پورت است. گشایش سایت‌های حیاتی ابتدا باید فقط روی شبکه‌های اپراتورهای همراه انجام شود تا امکان مانیتورینگ دقیق‌تر و در صورت نیاز شناسایی فرد متخلف طی ۴۸ ساعت اولیه فراهم گردد. پس از تأیید عدم نشت، به اپراتورهای ثابت گسترش یابد. همزمان، تمام resolver ها باید به DNS ملی اجبار شوند و DoH/DoT ثالث مسدود گردد.

مرحله سوم: گشایش پلتفرم‌های سرویس هوش مصنوعی: این مرحله با هدف فراهم‌سازی دسترسی کنترل‌شده شرکت‌های دانش‌بنیان و کاربران احراز هویت‌شده به مدل‌های هوش مصنوعی اجرا می‌شود. تجربه واقعی تیر ماه ۱۴۰۴ نشان داد که باز کردن دسترسی به ChatGPT موجب فعال‌سازی همزمان سرویس Cloudflare WARP شد، زیرا هر دو از یک Anycast استفاده می‌کنند همچنین مسیریابی ترافیک از طریق شبکه آذربایجان برای رفع تحریم در بروز این مشکل نقش داشت. تیم فنی امن‌افزار گستر شریف ظرف ۷۲ ساعت signature اختصاصی WARP را بر اساس الگوی handshake اولیه، sequence number خاص و آنتروپی بسته طراحی کرد که اکنون قابلیت مسدود سازی ۱۰۰ درصدی بدون اختلال در ChatGPT را دارد. بنابراین گشایش این مرحله صرفاً پس از آماده‌سازی signature های اختصاصی و تست آزمایشگاهی انجام شود و دسترسی محدود به کاربران دارای احراز هویت دو مرحله‌ای و نشانی IP ثابت باشد.

مرحله چهارم: گشایش تدریجی پروتکل‌های شبکه: این مرحله صرفاً برای رفع مشکلات عیب‌یابی شبکه و پشتیبانی از پروتکل‌های مدرن در موارد عملیاتی کنترل‌شده پیش‌بینی شده است. در این مرحله، ICMP امکان تونلینگ و IPv6 امکان تونلینگ 6to4 و Teredo را ایجاد می‌کند. راهکار قطعی، مسدود سازی کامل و دائمی IPv6، UDPو ICMP به سمت خارج (به جز موارد استثنایی و کاملاً نرخ‌محدود است). فایروال stateful IPv6 با بررسی کامل extension headers پیاده‌سازی شود و Rate-Limiting ده بسته در ثانیه همراه با تشخیص ناهنجاری مبتنی بر یادگیری ماشین اعمال گردد. همینطور تعداد بسته های ICMP به خارج در هر نشست بیشتر از تعداد خاص (برای مثال ۳) نشود.

توصیه‌های سیاست‌گذاری الزامی:

ممنوعیت ارسال فایل بدون لاگین در تمام آپلودرهای ایرانی با الزام احراز هویت دو مرحله‌ای (SMS) ضروری است.

همچنین تمام سایت‌ها و خدمات ایرانی باید ۱۰۰ درصد پشت شبکه توزیع محتوا ملی قرار گیرند تا از خارج کشور صرفاً نشانی IP های شبکه توزیع محتوا ملی قابل مشاهده و دسترسی باشند.

شبکه توزیع محتوا های خارجی به عنوان عامل اصلی و شناخته‌شده دسترسی غیر مجاز محسوب می‌شوند؛ زیرا تعداد بسیار زیادی از سایت‌های خارجی — از جمله برخی خدمات ضروری — پشت این زیرساخت‌ها قرار دارند. بر اساس تجربیات عملیاتی تیم تحقیقاتی، در مرحله اول گشایش، از باز کردن هرگونه دسترسی به این شبکه توزیع محتواها به طور کامل صرف‌نظر شود تا از ایجاد حفره‌های گسترده جلوگیری گردد. در صورت اجبار و ضرورت در مرحله دوم، گشایش باید به صورت بسیار محدود و با اعمال وایت‌لیست دقیق بر مبنای پورت و پیشوند IP خاص، همراه با DPI کامل

و مبتنی بر امضا بر روی تمام جریان‌های ترافیک آن شبکه توزیع محتوا و مسدود سازی فوری هرگونه اتصال شبیه‌سازی‌شده VPN مانند QUIC، WireGuard یا WARP انجام گیرد تا دسترسی مشروع حفظ شود و همزمان مسیرهای دورزدن مسدود بماند.

رویه اجرایی در حالت بحران

در شرایط بحران (مانند اختلالات گسترده یا فشار خارجی شدید)، تمام مراحل گشایش به حالت تعلیق کامل درمی‌آید. مسدود سازی فوری و بدون استثنا IPv6، UDP و ICMP و سایر پروتکل های غیر لازم اعمال می‌شود، ارسال فایل در همه پیام‌رسان‌های داخلی و آپلودرها متوقف می‌گردد (یا با محدودیت شدید و حجم حداقلی) اعمال می‌شود. برای جلوگیری از گسترش سرویس‌های غیرمجاز، دسترسی به سایت‌های حیاتی به حداقل (فقط ایمیل و جستجوی پایه) و در صورت عدم بروز فشار بر سکوهای داخلی، متوقف می‌شود. نظارت DPI به حالت حداکثری و بلادرنگ ارتقا یافته و هرگونه ترافیک مشکوک به صورت خودکار drop می‌شود.

رویه اجرایی در حالت خروج از بحران

پس از بازگشت به شرایط عادی، گشایش مرحله به مرحله و با رعایت دقیق ترتیب چهارمرحله‌ای از سر گرفته می‌شود. ابتدا مرحله اول (خدمات ملی) فعال شده و محدودیت کاهش می یابد و پس از ۷۲ ساعت مانیتورینگ و تأیید عدم نشت، مرحله دوم آغاز می‌گردد. Signature های به‌روز و پروتکل‌ها مجدداً تست و اعمال می‌شوند. محدودسازی‌های ارسال فایل به حالت عادی (۵ مگابایت با اسکن) بازمی‌گردد و شبکه توزیع محتوا ملی به عنوان لایه حفاظتی اصلی حفظ می‌شود. این روند به تیم های تحقیقاتی امکان شناسایی و از کار انداختن روش های باقی مانده ارتباط غیر مجاز را میدهد و امکان شناسایی کاربر مورد استفاده را اسان تر مینماید.

مدل چهارمرحله‌ای گشایش کنترل‌شده، تنها رویکرد علمی و عملی برای حفظ تعادل میان دسترسی مشروع و امنیت ملی است. اجرای موفق آن نیازمند همکاری نزدیک شرکت ارتباطات زیرساخت با تیم فنی امن‌افزار گستر شریف است. اینجانب آماده ارائه گزارش فنی جامع، فایل signature ها، گزارش کامل شبیه‌سازی و طرح پیاده‌سازی دقیق در سطح درگاه های مرزی هستم.

پایان گزارش