معاونت علمی، فناوری و اقتصاد دانش‌بنیان ریاست جمهوری
ستاد توسعه علوم و فناوری افتا

خبرنامه رویدادهای امنیتی

هسته امنیت شبکه، ارتباطات ثابت، سیار و مراکز داده

مرکز تخصصی آپا دانشگاه محقق اردبیلی

دی ماه ۱۴۰۴
شماره ۰۵

سخن سردبیر

مجموعه اخبار این شماره، تصویری روشن از تغییر ماهیت تهدیدات سایبری از نفوذهای ساده به سوءاستفاده‌های زنجیره‌ای، ماندگار و عمیق ارائه می‌دهد. از دور زدن احراز هویت دومرحله‌ای در فایروال‌ها و API ها گرفته تا بهره‌برداری فعال از تجهیزات خارج از پشتیبانی، ضعف در مدیریت هویت و چرخه عمر دارایی‌ها همچنان یکی از مهم‌ترین نقاط شکست امنیتی سازمان‌هاست. در کنار این تهدیدات زیرساختی، حملات زنجیره تأمین نرم‌افزار نیز با سوءاستفاده از اعتماد توسعه‌دهندگان، چه در قالب افزونه‌های پیشنهادی IDE ها و چه از طریق بدافزارهای سرقت اطلاعات و دسترسی به سرویس‌های ابری سازمانی، ابعاد نگران‌کننده‌تری به خود گرفته‌اند. افشای داده‌های حجیم سازمانی و دولتی در این حملات، پیامدهایی فراتر از نشت اطلاعات و تا سطح ریسک‌های امنیت ملی دارد. هم‌زمان، گزارش‌ها از فعالیت بازیگران پیشرفته دولتی با استفاده از روت‌کیت‌های امضاشده در سطح کرنل و گسترش بات‌نت‌ها از طریق آسیب‌پذیری‌های نوظهور نشان می‌دهد که مهاجمان به‌دنبال پایداری، اختفا و مقیاس‌پذیری بیشتر هستند. پیام مشترک این رویدادها روشن است: امنیت مؤثر، بدون اجرای سخت‌گیرانه MFA ، به‌روزرسانی مستمر، حذف تجهیزات EoL ، پایش رفتارها و آموزش کاربران، دیگر قابل تصور نیست. این بولتن تلاشی است برای برجسته‌سازی همین نقاط بحرانی و کمک به تصمیم‌گیری آگاهانه‌تر مدیران و تیم‌های فنی.

مهم ترین اخبار و مطالب هفته

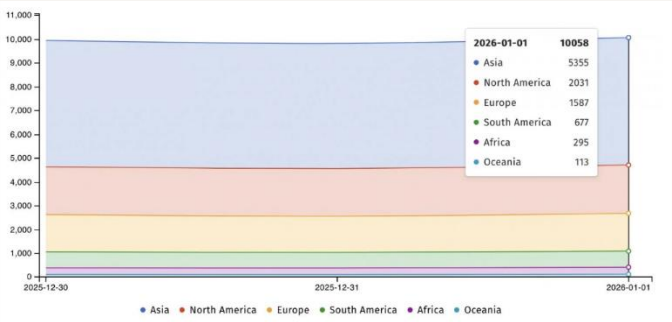
- ده‌هزار فایروال Fortinet در خطر دور زدن 2FA ادامه خبر
- هشدار IBM در باره آسیب‌پذیری دور زدن احراز هویت در API Connect ادامه خبر
- استفاده از روت‌کیت امضا شده در حالت کرنل برای بارگذاری در پشتی TONESHELL ادامه خبر
- گسترش بات‌نت RondoDox از طریق Reace2Shell ادامه خبر
- افزایش حملات سرقت‌داده از طریق سرویس‌های اشتراک‌گذاری فایل ابری ادامه خبر
- نسخه‌های فورک‌شده VSCode و خطر حملات از طریق افزونه‌های پیشنهادی ادامه خبر
- آسیب‌پذیری جدید در روترهای قدیمی DSL دی‌لینک و سوءاستفاده فعال ادامه خبر

[۱] ده‌هزار فایروال Fortinet در خطر دور زدن 2FA

بیش از ۱۰ هزار فایروال Fortinet همچنان به صورت آنلاین در دسترس بوده و در معرض حملات فعال قرار دارند که از یک آسیب‌پذیری پنج ساله در دور زدن احراز هویت دو عاملی (2FA) سوءاستفاده می‌کنند.

Fortinet در ژوئیه ۲۰۲۰ نسخه‌های ۶.۴.۱، ۶.۲.۴ و ۶.۰.۱۰ از FortiOS را برای رفع نقص با شناسه CVE-2020-12812 منتشر کرد و به مدیرانی که نمی‌توانستند بلافاصله به‌روزرسانی کنند توصیه کرد حساسیت به حروف نام‌کاربری را غیرفعال کنند تا تلاش‌های دور زدن FA2 مسدود شود. این نقص امنیتی، که شدت آن ۹.۸ از ۱۰ ارزیابی شده است، در FortiGate SSL VPN یافت شده و به مهاجمان اجازه می‌دهد بدون ارائه فاکتور دوم احراز هویت (FortiToken) وارد فایروال‌های بدون وصله شوند، به شرطی که حروف نام‌کاربری تغییر داده شود.

Fortinet به مشتریان خود هشدار داد که مهاجمان همچنان از آسیب‌پذیری CVE-2020-12812 سوءاستفاده می‌کنند و فایروال‌هایی را هدف قرار می‌دهند که دارای پیکربندی آسیب‌پذیر هستند و نیاز به فعال بودن LDAP (پروتکل دسترسی سبک به دایرکتوری) دارند. این شرکت اعلام کرد :اخیراً سوءاستفاده از آسیب‌پذیری جولای ۲۰۲۰ با شناسه FG-IR-19-283 / CVE-2020-12812 را در فضای واقعی و بر اساس پیکربندی‌های مشخص مشاهده کرده است. سازمان نظارت بر امنیت اینترنت Shadowserver گزارش داد در حال حاضر بیش از ۱۰ هزار فایروال Fortinet در اینترنت هنوز در معرض خطر هستند و نسبت به CVE-2020-12812 وصله نشده‌اند و آسیب‌پذیر به حملات جاری هستند، که بیش از ۱،۳۰۰ آدرس آی‌پی از این تعداد در ایالات متحده قرار دارند.



فایروال‌های Fortinet در معرض حملات CVE-2020-12812 (Shadowserver)

در آوریل ۲۰۲۱، CISA و FBI هشدار دادند که گروه‌های هک حمایت‌شده توسط دولت، نسخه‌های FortiOS فایروال‌های Fortinet را با بهره‌جویی از چندین آسیب‌پذیری هدف قرار می‌دهند، از جمله یکی که با استفاده از CVE-2020-12812 احراز هویت دو عاملی (2FA) را دور می‌زند. هفت ماه بعد، CISA این آسیب‌پذیری را به فهرست آسیب‌پذیری‌های شناخته‌شده در حال بهره‌برداری افزود و آن را به‌عنوان آسیب‌پذیری مورد استفاده در حملات باج‌افزاری علامت‌گذاری کرد و دستور داد که آژانس‌های فدرال ایالات متحده تا مه ۲۰۲۲ سیستم‌های خود را ایمن کنند. آسیب‌پذیری‌های Fortinet اغلب در حملات سوءاستفاده می‌شوند و گاهی به‌عنوان آسیب‌پذیری روز صفر (zero-day) مورد بهره‌برداری قرار می‌گیرند.

نکات امنیتی پیشنهادی برای فایروال‌های Fortinet

- به‌روزرسانی فوری فایروال‌ها به آخرین نسخه‌های FortiOS و FortiWeb.
- فعال‌سازی و بررسی صحیح MFA/2FA و غیرفعال کردن حساسیت به حروف نام‌کاربری در صورت نیاز.

- بازبینی پیکربندی‌های LDAP و SSO و محدود کردن دسترسی‌های غیرضروری.
- نظارت مداوم بر لاگ‌ها و فعالیت‌های شبکه برای شناسایی حملات مشکوک.
- محدود کردن دسترسی اینترنتی به فایروال‌ها و استفاده از شبکه امن یا VPN.
- آمادگی برای پاسخ به حادثه و نسخه پشتیبان از پیکربندی‌ها.

[۲] هشدار IBM درباره آسیب‌پذیری دور زدن احراز هویت در API Connect

IBM از مشتریان خود خواست تا آسیب‌پذیری حیاتی دور زدن احراز هویت در پلتفرم سازمانی API Connect را وصله کنند، نقصی که می‌تواند به مهاجمان اجازه دهد به‌صورت راه دور به برنامه‌ها دسترسی پیدا کنند.

API Connect یک دروازه واسط برنامه‌نویسی کاربردی است که به سازمان‌ها امکان توسعه، تست و مدیریت APIها و ارائه دسترسی کنترل‌شده به سرویس‌های داخلی برای برنامه‌ها، شرکای تجاری و توسعه‌دهندگان خارجی را می‌دهد.

این پلتفرم در محیط‌های محلی، ابری یا ترکیبی در دسترس است و توسط صدها شرکت در بخش‌های بانکداری، سلامت، خرده‌فروشی و مخابرات استفاده می‌شود.

این آسیب‌پذیری دور زدن احراز هویت با شناسه CVE-2025-13915 ثبت شده و شدت آن ۹.۸ از ۱۰ ارزیابی شده است. این نقص بر نسخه‌های IBM API Connect 10.0.11.0 و ۱۰.۰.۸.۰ تا ۱۰.۰.۸.۵ تأثیر می‌گذارد. بهره‌برداری موفق از این آسیب‌پذیری به مهاجمان غیرمجاز اجازه می‌دهد تا بدون احراز هویت و از راه دور به برنامه‌های آسیب‌پذیر دسترسی پیدا کنند؛ این حملات کم‌پیچیدگی بوده و نیاز به تعامل کاربر ندارند. IBM از مدیران سیستم خواسته است تا نصب‌های آسیب‌پذیر را به آخرین نسخه ارتقا دهند تا از حملات احتمالی جلوگیری شود و برای کسانی که قادر به اعمال فوری به‌روزرسانی نیستند، راهکارهای کاهش ریسک ارائه کرده است. این شرکت اعلام کرد IBM API Connect می‌تواند به مهاجم از راه دور اجازه دهد مکانیزم‌های احراز هویت را دور زده و به برنامه دسترسی غیرمجاز پیدا کند.

توصیه شدید می‌شود این آسیب‌پذیری هم‌اکنون با ارتقا برطرف شود. همچنین برای مشتریانی که قادر به نصب فوری نیستند، غیرفعال کردن ثبت‌نام خودکار در Developer Portal می‌تواند سطح قرارگیری در معرض این آسیب‌پذیری را کاهش دهد. راهنمای دقیق اعمال وصله CVE-2025-13915 در محیط‌های VMware، OCP و Kubernetes در سند پشتیبانی IBM موجود است.

طی چهار سال گذشته، آژانس امنیت سایبری و زیرساخت‌های ایالات متحده (CISA) چندین آسیب‌پذیر IBM را به فهرست آسیب‌پذیری‌های شناخته‌شده و مورد بهره‌برداری اضافه کرده و آن‌ها را به‌عنوان نقص‌هایی که در فضای واقعی فعالانه سوءاستفاده می‌شوند، علامت‌گذاری کرده است و دستور داده است که آژانس‌های فدرال سیستم‌های خود را مطابق دستور عملیاتی اجباری (BOD 22-01) ایمن کنند.

دو مورد از این نقص‌ها، شامل یک نقص اجرای کد در IBM Aspera Faspex (CVE-2022-47986) و یک نقص ورودی نامعتبر در IBM InfoSphere BigInsights (CVE-2013-3993) نیز توسط این آژانس به‌عنوان آسیب‌پذیری‌هایی که در حملات باج‌افزاری مورد سوءاستفاده قرار گرفته‌اند، گزارش شده‌اند.

[۳] استفاده از روت‌کیت امضاشده در حالت کرنل برای بارگذاری در پشتی TONESHELL

گروه هکری چینی موسوم به Mustang Panda با نام دیگر HoneyMyte در یک حمله سایبری شناسایی‌شده در اواسط سال ۲۰۲۵ علیه یک نهاد نامشخص در آسیا، از یک درایور روت‌کیت در سطح کرنل که پیش‌تر مستندسازی نشده بود برای انتشار نسخه‌ای جدید از درب پشتی TONESHELL استفاده کرده است. این یافته‌ها توسط شرکت Kaspersky گزارش شده است. کاسپرسکی اعلام کرده این نسخه جدید از بک‌دور در چارچوب کارزارهای جاسوسی سایبری این گروه علیه سازمان‌های دولتی در جنوب‌شرق و شرق آسیا، به‌ویژه میانمار و تایلند مشاهده شده است. به گفته این شرکت، فایل درایور با یک گواهی دیجیتال قدیمی، سرقت‌شده یا افشاشده، امضا شده و به‌عنوان یک درایور مینی‌فیلتر روی سیستم‌های آلوده ثبت می‌شود. هدف نهایی آن تزریق یک تروجان درِ پشتی به پردازش‌های سیستمی و فراهم کردن حفاظت برای فایل‌های مخرب، پردازش‌های سطح کاربر و کلیدهای رجیستری است. محموله نهایی این حمله TONESHELL است؛ ایمپلنتی که قابلیت‌های Reverse Shell و Downloader دارد و می‌تواند بدافزارهای مرحله بعدی را روی سیستم‌های آلوده دریافت کند. استفاده از TONESHELL دست‌کم از اواخر سال ۲۰۲۲ به گروه Mustang Panda نسبت داده شده است.

همچنین در سپتامبر ۲۰۲۵، این عامل تهدید به حملاتی علیه نهادهای تایلندی نسبت داده شد که در آن‌ها از TONESHELL و یک کرم USB به نام TONEDISK با نام دیگر WispRider استفاده شده بود؛ بدافزاری که از دستگاه‌های قابل‌حمل به‌عنوان بردار انتشار برای یک بک‌دور با نام Yokai بهره می‌برد. بر اساس گزارش‌ها، زیرساخت فرماندهی و کنترل (C2) مورد استفاده برای TONESHELL در سپتامبر ۲۰۲۴ ایجاد شده، هرچند شواهد نشان می‌دهد خود کارزار تا فوریه ۲۰۲۵ آغاز نشده است. مسیر دقیق دسترسی اولیه در این حمله مشخص نیست، اما گمان می‌رود مهاجمان از سیستم‌هایی که پیش‌تر به خطر افتاده بودند برای استقرار درایور مخرب استفاده کرده باشند.

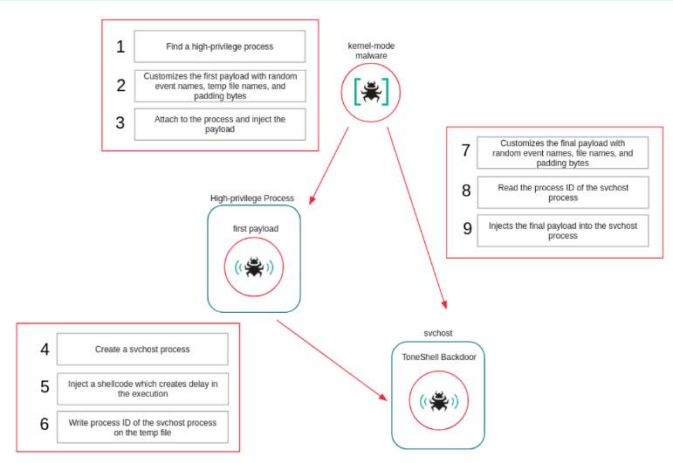
فایل درایور مخرب با نام ProjectConfiguration.sys با یک گواهی دیجیتال متعلق به شرکت چینی Guangzhou Kingteller Technology Co., Ltd امضا شده است؛ شرکتی که در حوزه توزیع و راه‌اندازی دستگاه‌های خودپرداز (ATM) فعالیت دارد. این گواهی دیجیتال در بازه زمانی اوت ۲۰۱۲ تا ۲۰۱۵ معتبر بوده است. با توجه به این‌که نمونه‌های مخرب دیگریِ نامرتبط نیز با همین گواهی دیجیتال امضا شده‌اند، ارزیابی‌ها نشان می‌دهد که عاملان تهدید به احتمال زیاد از یک گواهی افشاشده یا سرقت‌شده برای رسیدن به اهداف خود استفاده کرده‌اند. درایور مخرب شامل دو شِل‌کُد در سطح user-mode است که در بخش data. فایل باینری جاسازی شده‌اند و هرکدام به‌صورت رشته‌های اجرایی (thread) جداگانه در user-mode اجرا می‌شوند.کاسپرسکی در این‌باره اعلام کرده است: قابلیت روت‌کیت باعث محافظت از ماژول خود درایور و همچنین پردازش‌های سطح کاربری می‌شود که کد بک‌دور در آن‌ها تزریق شده است و دسترسی هرگونه پردازش دیگر در سیستم به آن‌ها را مسدود می‌کند. این درایور دارای مجموعه‌ای از قابلیت‌های زیر است:

- در زمان اجرا، APIهای موردنیاز کرنل را به‌صورت پویا و با استفاده از یک الگوریتم هش برای تطبیق آدرس‌APIها شناسایی و بارگذاری می‌کند .
- عملیات حذف و تغییر نام فایل‌ها را پایش می‌کند تا از حذف یا تغییر نام خود جلوگیری کند .
- با راه‌اندازی یک روال RegistryCallback و تنظیم آن در ارتفاع 330024 (altitude) یا بالاتر، تلاش‌ها برای ایجاد یا باز کردن کلیدهای رجیستری منطبق با یک فهرست محافظت‌شده را مسدود می‌کند .
- در ارتفاع اختصاص‌یافته به WdFilter.sys درایور Microsoft Defender دستکاری ایجاد کرده و آن را به صفر تغییر می‌دهد

(در حالی که مقدار پیش‌فرض آن 328010 است) و به این ترتیب مانع بارگذاری آن در پشته ورودی/خروجی (I/O stack) می‌شود.

- عملیات مرتبط با پردازش‌ها (processes) را رهگیری کرده و در صورتی که اقدام موردنظر متوجه هر یک از پردازش‌های دارای شناسه‌های محافظت‌شده باشد، دسترسی را مسدود می‌کند .
- پس از پایان اجرای این پردازش‌ها، محافظت روت‌کیتی اعمال‌شده برای آن‌ها را حذف می‌کند.

کسپرسکی در توضیح این سازوکار اعلام کرده است: مایکروسافت بازه ارتفاع ۳۲۰۰۰۰ تا ۳۲۹۹۹۹ را برای گروه بارگذاری فیلترهای ضدویروس (FSFilter Anti-Virus Load Order Group) در نظر گرفته است. ارتفاع انتخاب‌شده توسط بدافزار فراتر از این بازه است. از آنجا که فیلترهایی با ارتفاع کمتر، عمیق‌تر در پشته I/O قرار می‌گیرند، درایور مخرب پیش از فیلترهای قانونی با ارتفاع پایین‌تر، مانند اجزای آنتی‌ویروس، عملیات فایل را رهگیری می‌کند و به این ترتیب می‌تواند بررسی‌های امنیتی را دور بزند.



این درایور در نهایت برای رهاسازی (drop) دو محموله در سطح user-mode طراحی شده است. یکی از این محموله‌ها یک پردازش svchost.exe ایجاد کرده و یک شِل‌کُد ایجادکننده تأخیر کوتاه را به آن تزریق می‌کند. محموله دوم، بک‌دور TONESHELL است که به همان پردازش svchost.exe تزریق می‌شود. پس از اجرا، این بک‌دور از طریق TCP روی پورت ۴۴۳ با سرور فرماندهی و کنترل با دامنه‌های avocadomechanism[.]com یا potherbreference[.]com ارتباط برقرار می‌کند و از این کانال برای دریافت دستورات زیر استفاده می‌کند:

- ایجاد فایل موقت برای داده‌های ورودی(0x1)
- دانلود فایل(0x2 / 0x3)
- لغو عملیات دانلود (0x4)
- برقراری شل از راه دور از طریق(0x7) pipe
- دریافت دستور از اپراتور(0x8)
- خاتمه دادن به شل(0x9)
- بارگذاری (آپلود) فایل(0xA / 0xB)
- لغو عملیات آپلود(0xC)
- بستن اتصال(0xD)

این تحول نشان‌دهنده اولین باری است که TONESHELL از طریق یک لودر در سطح کرنل توزیع می‌شود؛ روشی که عملاً به آن امکان می‌دهد فعالیت‌های خود را از ابزارهای امنیتی پنهان کند. یافته‌ها نشان می‌دهد این درایور، جدیدترین مؤلفه از یک مجموعه ابزار بزرگ‌تر و در حال تکامل است که توسط گروه Mustang Panda برای ایجاد ماندگاری (persistence) و مخفی‌سازی بک‌دور مورد استفاده قرار می‌گیرد.

این شرکت در جمع‌بندی خود اعلام کرد: «عملیات‌های HoneyMyte در سال ۲۰۲۵ نشان‌دهنده یک تکامل قابل توجه به‌سوی استفاده از تزریق‌کننده‌های سطح کرنل برای استقرار TONESHELL است؛ رویکردی که هم پنهان‌کاری (stealth) و هم تاب‌آوری (resilience) را بهبود می‌بخشد.» همچنین برای پنهان‌سازی بیشتر فعالیت‌ها، این درایور ابتدا یک مولفه کوچک در سطح user-mode را مستقر می‌کند که مرحله نهایی تزریق را انجام می‌دهد. علاوه بر این، از چندین تکنیک مبهم‌سازی، روال‌های callbackو مکانیزم‌های اعلان برای مخفی کردن نحوه استفاده از

APIها و ردیابی فعالیت‌های مربوط به پردازش‌ها و رجیستری استفاده می‌کند که در نهایت موجب تقویت سازوکارهای دفاعی بک‌دور می‌شود.

[۴] گسترش باتنت RondoDox از طریق React2Shell

کارشناسان امنیت سایبری اعلام کرده‌اند آسیب‌پذیری React2Shell به ابزاری کلیدی برای نفوذ به سرورها و جذب آن‌ها به باتنت RondoDox تبدیل شده است.

به گزارش افتانا، پژوهشگران امنیت سایبری جزئیات یک کارزار گسترده و مداوم را فاش کرده‌اند که طی حدود ۹ ماه، دستگاه‌های اینترنت اشیا و وب‌سرورها را هدف قرار داده و آن‌ها را به باتنتی با نام RondoDox آلوده کرده است.

بر اساس تحلیلی که شرکت CloudSEK منتشر کرده، این فعالیت مخرب تا پایان دسامبر ۲۰۲۵ از آسیب‌پذیری بسیار خطرناک React2Shell با شناسه CVE-2025-55182 و امتیاز ۱۰ از ۱۰ به‌عنوان مسیر اولیه نفوذ استفاده کرده است. این نقص امنیتی که به‌تازگی افشا شده، در React Server Components و فریم‌ورک Next.js وجود دارد و به مهاجمان بدون نیاز به احراز هویت اجازه می‌دهد کد دلخواه خود را از راه دور روی سامانه‌های آسیب‌پذیر اجرا کنند.

طبق آمار بنیاد Shadowserver ، تا تاریخ ۳۱ دسامبر ۲۰۲۵ حدود ۹۰ هزار و ۳۰۰ نمونه از این آسیب‌پذیری همچنان در معرض سوءاستفاده قرار داشتند. از این تعداد، بیش از ۶۸ هزار مورد در ایالات متحده شناسایی شده و پس از آن آلمان، فرانسه و هند در رتبه‌های بعدی قرار دارند.

باتنت RondoDox که اوایل سال ۲۰۲۵ برای نخستین بار شناسایی شد، به‌تدریج دامنه فعالیت خود را گسترش داده و با افزودن آسیب‌پذیری‌های موسوم به N-day به مجموعه ابزارهایش، حملات خود را تقویت کرده است. از جمله این نقص‌ها می‌توان به CVE-2023-1389 و CVE-2025-24893 اشاره کرد. پیش از این نیز شرکت‌هایی مانند Darktrace، Kaspersky و VulnCheck نسبت به سوءاستفاده از React2Shell برای گسترش این باتنت هشدار داده بودند.

ارزیابی‌ها نشان می‌دهد این کارزار پیش از بهره‌برداری از آسیب‌پذیر React2Shell ، سه مرحله مشخص را پشت سر گذاشته است. در ماه‌های مارس و آوریل ۲۰۲۵، مهاجمان به شناسایی اولیه و اسکن دستی آسیب‌پذیری‌ها پرداختند. سپس از آوریل تا ژوئن همان سال، اسکن‌های انبوه و روزانه‌ای علیه وب‌اپلیکیشن‌هایی مانند وردپرس، دروپال و Struts2 و همچنین دستگاه‌های اینترنت اشیا از جمله روترهای Wavlink انجام دادند. از ماه ژوئیه تا اوایل دسامبر ۲۰۲۵ نیز این حملات به شکل خودکار و در مقیاس بسیار بزرگ، به‌صورت ساعتی اجرا شده است.

در حملاتی که در دسامبر ۲۰۲۵ شناسایی شدند، مهاجمان ابتدا سرورهای آسیب‌پذیر Next.js را اسکن کرده و سپس تلاش کرده‌اند روی دستگاه‌های آلوده، استخراج‌کننده‌های ارز دیجیتال، یک بارگذار و ابزار بررسی سلامت باتنت و همچنین گونه‌ای از باتنت Mirai را نصب کنند. یکی از این ابزارها پیش از دانلود بدافزار اصلی، بدافزارها و ماینرهای رقیب را حذف می‌کند و با پاک‌سازی آثار حملات قبلی و ایجاد سازوکار ماندگاری در سیستم، کنترل دستگاه را در اختیار می‌گیرد. این ابزار به‌طور مداوم پردازش‌های در حال اجرا را بررسی کرده و هر فرایندی را که در فهرست مجاز نباشد، در بازه‌های زمانی کوتاه متوقف می‌کند تا از نفوذ دوباره مهاجمان دیگر جلوگیری شود.

توصیه‌های پیشنهادی:

کارشناسان برای کاهش خطر ناشی از این تهدید توصیه کرده‌اند سازمان‌ها هرچه سریع‌تر نسخه‌های اصلاح‌شده Next.js را نصب کنند، دستگاه‌های اینترنت اشیا را در شبکه‌های جداگانه قرار دهند، از دیواره‌های آتش مخصوص وب استفاده کنند، اجرای

پردازش‌های مشکوک را زیر نظر بگیرند و ارتباط با زیرساخت‌های شناخته‌شده فرماندهی و کنترل این بات‌نت را مسدود کنند.

[۵] افزایش حملات سرقت داده از طریق سرویس‌های اشتراک‌گذاری فایل ابری

یک عامل تهدید با نام Zestix در حال عرضه برای فروش داده‌های سازمانی سرقت‌شده از ده‌ها شرکت است؛ داده‌هایی که به‌احتمال زیاد پس از نفوذ به نمونه‌های ShareFile، Nextcloud و OwnCloud این سازمان‌ها به‌دست آمده‌اند. بر اساس گزارش شرکت اطلاعات جرایم سایبری Hudson Rock، دسترسی اولیه احتمالاً از طریق نام‌های کاربری و گذرواژه‌های سرقت‌شده توسط بدافزارهای سرقت اطلاعات (Infostealer) مانند RedLine، Lumma و Vidar که روی دستگاه‌های کارکنان اجرا شده‌اند، حاصل شده است. این سه بدافزار معمولاً از طریق کمپین‌های تبلیغات مخرب (Malvertising) یا حملات ClickFix توزیع می‌شوند و به‌طور رایج اطلاعات ذخیره‌شده در مرورگرهای وب (اعتبارنامه‌ها، اطلاعات کارت‌های بانکی و داده‌های شخصی)، برنامه‌های پیام‌رسان و کیف‌پول‌های رمزارزی را هدف قرار می‌دهند.

در صورت نبود احراز هویت چندمرحله‌ای (MFA)، یک عامل تهدید که به اعتبارنامه‌های معتبر دسترسی دارد می‌تواند به‌صورت غیرمجاز به سرویس‌هایی مانند پلتفرم‌های اشتراک‌گذاری فایل نفوذ کند. شرکت Hudson Rock در گزارش خود اعلام کرده است که برخی از اعتبارنامه‌های سرقت‌شده بررسی‌شده سال‌هاست در پایگاه‌های داده مجرمان سایبری وجود داشته‌اند؛ موضوعی که نشان‌دهنده عدم چرخش گذرواژه‌ها یا باطل‌نشدن نشست‌های فعال حتی پس از گذشت زمان‌های طولانی است.

نفوذهای متعدد و عرضه دسترسی در بازار زیرزمینی به‌گفته شرکت Hudson Rock، عامل تهدید Zestix به‌عنوان یک کارگزار دسترسی اولیهدر انجمن‌های زیرزمینی فعالیت می‌کند و دسترسی به پلتفرم‌های ابری سازمانی با ارزش بالا را به فروش می‌رساند.

این شرکت امنیت سایبری اعلام کرده است که مهاجمان موفق به نفوذ به محیط‌های ShareFile، Nextcloud و ownCloud مورد استفاده سازمان‌ها در بخش‌های مختلفی از جمله هوانوردی، دفاعی، بهداشت و درمان، خدمات عمومی (Utilities) ، حمل‌ونقل عمومی، مخابرات، حقوقی، املاک و مستغلات و نهادهای دولتی شده‌اند.

پس از تحلیل لاگ‌های بدافزارهای سرقت اطلاعات و با تمرکز مشخص بر نشانی‌های ابری سازمانی مانند ShareFile و Nextcloud، عامل تهدید در مواردی که احراز هویت چندمرحله‌ای (MFA) فعال نبوده است، با استفاده از نام کاربری و گذرواژه معتبر وارد سرویس‌های اشتراک‌گذاری فایل می‌شود.

شرکت Hudson Rock اعلام کرد با تطبیق داده‌های بدافزارهای سرقت اطلاعات با تصاویر عمومی، متادیتا و منابع متن‌باز، نقاط احتمالی نفوذ را شناسایی کرده است. در دست‌کم ۱۵ مورد، مشخص شد که اعتبارنامه‌های کارکنان سرویس‌های اشتراک‌گذاری فایل ابری توسط Infostealerها جمع‌آوری شده‌اند.

با این حال، این بررسی یک‌طرفه بوده و به‌جز مورد احتمالی Iberia، تاکنون تأیید عمومی از سوی شرکت‌های نام‌برده‌شده درباره وقوع نفوذ منتشر نشده است.

به‌گفته Hudson Rock ، عامل تهدید Zestix حجم‌هایی از داده‌های سرقت‌شده از چند ده گیگابایت تا چند ترابایت را برای فروش عرضه کرده که شامل اسناد فنی هواپیما، داده‌های دفاعی و مهندسی، پایگاه‌های داده مشتریان، پرونده‌های سلامت، نقشه‌های

زیرساخت حمل‌ونقل، داده‌های شبکه مخابراتی، اطلاعات پروژه‌های ماهواره‌ای، کد منبع ERP، قراردادهای دولتی و اسناد حقوقی است.

بسیاری از فایل‌های سرقت‌شده می‌توانند سازمان‌ها را در معرض خطرات امنیتی، حریم خصوصی و جاسوسی صنعتی قرار دهند، در حالی که افشای قراردادهای دولتی می‌تواند ملاحظات امنیت ملی را برانگیزد.

VICTIM ENTITY	DATA VOLUME	RISK
Pickett	139.1 GB	Critical Utility Maps & LiDAR
Maida Health	2.3 TB	Military Police Health Records
Intecro	11.5 GB	Defense/ITAR Robotics Data
Iberia	77 GB	Aircraft Manuals (AMP/ALS)
K3G	192 GB	ISP Network Topology
CRRC MA	Complete Server	Mass Transit Schematics & Security
Burris Macomber	18.3 GB	Mercedes-Benz Litigation & Customer PII
ThermoEx	170 GB	Industrial Heat Exchanger Designs
CiberC	103 GB	Government Contract Data
GreenBills	39.5 GB	Patient Health (PHI)
Total ETO	28.95 GB	ERP Source Code & Customer DBs
Hydratec	81 GB	Fire Protection CAD Software
Degewo AG	5.5 GB	Berlin Housing Architectural Plans
Voltras	Internal Archive	Financial Data & Airline Invoices
IFLUSAC	22 GB	Engineering Plans & Payroll
Aion Law Partners	38 GB	Legal/Financial/Immigration Docs
NMCV Business	47 GB	Medical Records & PHI
PT Pasifik Satelit (PSN)	92 GB	Satellite/Aerospace Data
VYTL-SFT (Verahealth)	3.65 GB	Clinical Notes & Patient SSNs

حجم و نوع داده‌های افشا شده

شرکت Hudson Rock مجموعه‌ای دیگر از ۳۰ قربانی را شناسایی کرده که عامل تهدید Zestix تحت نام مستعار «Sentap» برای فروش عرضه می‌کند، اما این موارد به‌طور کامل تأیید نشده‌اند. به گزارش محققان، داده‌های تهدید آن‌ها نشان می‌دهد که افشای داده‌های ابری یک مشکل سیستمی و گسترده است که ناشی از رعایت نکردن شیوه‌های امنیتی مناسب توسط سازمان‌ها است. آن‌ها همچنین هزاران کامپیوتر آلوده را شناسایی کرده‌اند که برخی از آن‌ها متعلق به شرکت‌هایی مانند Deloitte، KPMG، Samsung، Honeywell و Walmart بوده است. شرکت Hudson Rock به وب‌سایت BleepingComputer اعلام کرده که ShareFile را در جریان گذاشته و همچنین Nextcloud و OwnCloud را از موارد تأییدشده مطلع خواهد کرد تا اقدامات مناسب امنیتی را انجام دهند.

راهکار پیشنهادی:

- فعال‌سازی احراز هویت چندمرحله‌ای (MFA) برای تمام سرویس‌های ابری سازمانی
- چرخش منظم گذرواژه‌ها و غیرفعال‌سازی نشست‌های قدیمی
- نظارت و شناسایی رفتارهای مشکوک در دسترسی به فایل‌ها
- آموزش کارکنان برای شناسایی حملات فیشینگ و بدافزارهای سرقت اطلاعات

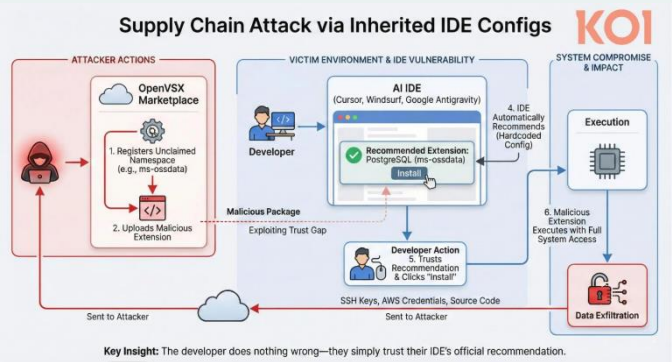
[۶] نسخه‌های فورک‌شده VSCode و خطر حملات از طریق افزونه‌های پیشنهادی

راهکارهای محبوب توسعه یکپارچه با پشتیبانی هوش مصنوعی مانند Cursor، Windsurf، Google Antigravity و Trae، افزونه‌هایی را پیشنهاد می‌کنند که در رجیستری OpenVSX وجود ندارند. این موضوع به عاملان تهدید اجازه می‌دهد نام این افزونه‌ها را ثبت کرده و افزونه‌های مخرب بارگذاری کنند. این IDE های مبتنی بر هوش مصنوعی از Microsoft VSCode فورک شده‌اند، اما به دلیل محدودیت‌های مجوز، نمی‌توانند از افزونه‌های فروشگاه رسمی استفاده کنند و به جای آن از OpenVSX به عنوان بازار متن‌باز جایگزین پشتیبانی می‌شوند. در نتیجه، با فورک شدن، این IDE ها فهرست افزونه‌های رسمی پیشنهادی را که در فایل‌های پیکربندی سخت‌کد شده است به ارث می‌برند، که به بازار Visual Studio

مایکروسافت اشاره دارد. این افزونه‌های پیشنهادی به دو شکل ارائه می‌شوند:

- **مبتنی بر فایل:** هنگام باز کردن فایلی مانند azure-pipelines.yaml، افزونه Azure Pipelines پیشنهاد می‌شود.
- **مبتنی بر نرم‌افزار:** هنگام شناسایی نصب PostgreSQL روی سیستم توسعه‌دهنده، افزونه مربوط به PostgreSQLتوصیه می‌شود.

با این حال، همه افزونه‌های پیشنهادی در OpenVSX وجود ندارند و در نتیجه نام فضاهای ناشر مربوطه ثبت نشده‌اند. محققان شرکت Koi در حوزه امنیت زنجیره تأمین اعلام کرده‌اند که عاملان تهدید می‌توانند از اعتماد کاربران به افزونه‌های پیشنهادی سوءاستفاده کرده و نام فضاهای خالی را ثبت کرده تا بدافزار توزیع کنند.



محققان این مشکل را در نوامبر ۲۰۲۵ به شرکت‌های Google، Windsurfو Cursor گزارش کردند. Cursor در اول دسامبر مشکل را رفع کرد و Google نیز ۱۳ افزونه پیشنهادی خود را در ۲۶ دسامبر حذف و یکم ژانویه مسئله را برطرف اعلام کرد Windsurf هنوز پاسخی نداده است.

محققان Koi برای جلوگیری از سوءاستفاده، نام‌فضاهای افزونه‌های مهم را ثبت و افزونه‌های غیرعملی جایگزین کردند که عملکرد واقعی ندارند اما جلوی حملات زنجیره تأمین را می‌گیرند. همچنین با Eclipse Foundation، اپراتور OpenVSX، همکاری کرده‌اند تا نام فضاهای باقی‌مانده را بررسی، مشارکت‌کنندگان غیررسمی را حذف و تدابیر حفاظتی گسترده‌تری در سطح رجیستری اعمال کنند.

تا کنون هیچ نشانه‌ای از سوءاستفاده عاملان تهدید قبل از اقدام محققان Koi مشاهده نشده است. به کاربران IDE های فورک‌شده توصیه می‌شود همیشه افزونه‌های پیشنهادی را از طریق رجیستری OpenVSX بررسی کنند و اطمینان حاصل کنند که ناشر آن معتبر است.

[۷] آسیب‌پذیری جدید در روترهای قدیمی DSL دی‌لینک و سوء استفاده فعال

عاملان تهدید در حال سوءاستفاده از یک آسیب‌پذیری تازه کشف‌شده تزریق دستور (Command Injection) هستند که چندین روتر DSL قدیمی دی‌لینک را که سال‌ها از پشتیبانی خارج شده‌اند، تحت تأثیر قرار می‌دهد. این آسیب‌پذیری با شناسه CVE-2026-0625 رصد شده و به دلیل عدم پاک‌سازی ورودی در کتابخانه CGI در نقطه دسترسی dnscfg.cgi ایجاد شده است. مهاجم بدون احراز هویت می‌تواند با استفاده از پارامترهای پیکربندی DNS دستورات از راه دور اجرا کند. شرکت VulnCheck این مشکل را در ۱۵ دسامبر به دی‌لینک گزارش داد، پس از آن که The Shadowserver Foundation تلاش برای بهره‌برداری از آسیب‌پذیری در یکی از هانی‌پات‌های خود را مشاهده کرده بود.

شرکت VulnCheck به BleepingComputer اعلام کرده است که تکنیکی که توسط Shadowserver شناسایی شده، ظاهراً تاکنون مستند عمومی نداشته است. بر اساس اطلاعیه امنیتی VulnCheck، یک حمله‌کننده از راه دور و بدون احراز هویت می‌تواند دستورات دلخواه شل را تزریق و اجرا کند که منجر به اجرای کد از راه دور (RCE) می‌شود.

در همکاری با VulnCheck، شرکت D-Link تأیید کرده است که مدل‌ها و نسخه‌های فریمور زیر تحت تأثیر CVE-2026-0625 قرار دارند:

- DSL-526B ≤ 2.01
- DSL-2640B ≤ 1.07
- DSL-2740R < 1.17
- DSL-2780B ≤ 1.01.14

این دستگاه‌ها از سال ۲۰۲۰ به پایان عمر (EoL) رسیده‌اند و به‌روزرسانی فریمور برای رفع آسیب‌پذیری دریافت نمی‌کنند. بنابراین، توصیه شدید شرکت سازنده، بازنشسته کردن و جایگزینی این دستگاه‌ها با مدل‌های پشتیبانی‌شده است.

شرکت D-Link هنوز در حال بررسی است که آیا محصولات دیگری نیز تحت تأثیر CVE-2026-0625 قرار دارند یا خیر و برای این منظور نسخه‌های مختلف فریمور را تحلیل می‌کند. به گفته این شرکت، شناسایی دقیق تمام مدل‌های آسیب‌پذیر پیچیده است زیرا هر نسل محصول و فریمور ممکن است تفاوت‌های خاصی داشته باشد. تحلیل فعلی نشان می‌دهد که هیچ روش مطمئن شناسایی مدل به جز بررسی مستقیم فریمور وجود ندارد و به همین دلیل D-Link در حال اعتبارسنجی نسخه‌های فریمور روی پلتفرم‌های قدیمی و پشتیبانی‌شده است. در حال حاضر مشخص نیست که چه کسی از این آسیب‌پذیری سوءاستفاده می‌کند و اهداف حملات چه هستند. با این حال، VulnCheck اعلام کرده که اکثر روترهای مصرفی تنها دسترسی LAN به نقاط مدیریتی CGI مانند dnscfg.cgi را فراهم می‌کنند.

بهره‌برداری از آسیب‌پذیری CVE-2026-0625 معمولاً مستلزم حمله مبتنی بر مرورگر یا پیکربندی دستگاه هدف برای مدیریت از راه دور است. به کاربران روترها و تجهیزات شبکه خارج از چرخه پشتیبانی (EoL) توصیه می‌شود این دستگاه‌ها را با مدل‌های دارای پشتیبانی فعال جایگزین کنند یا در صورت اجبار، آن‌ها را فقط در شبکه‌های غیرحیاتی و بخش‌بندی‌شده با آخرین نسخه firmware موجود و تنظیمات امنیتی محدودکننده به‌کار بگیرند. شرکت D-Link هشدار داده است که دستگاه‌های EoL هیچ‌گونه به‌روزرسانی firmware، وصله امنیتی یا پشتیبانی نگهداری دریافت نمی‌کنند.