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

فروردین ماه ۱۴۰۵
شماره ۰۶

سخن سردبیر

در این شماره از مجموعه خبرنامه رویدادهای امنیتی، آنچه بیش از همه به چشم می‌آید، گسترش دامنه و تنوع تهدیدات سایبری در لایه‌های مختلف فناوری است؛ از آسیب‌پذیری‌های بحرانی و روز-صفر گرفته تا حملات مبتنی بر هویت و سوءاستفاده از ابزارهای نوین.

سوءاستفاده از آسیب‌پذیری‌های RCE در حملات باج‌افزاری، هدف‌گیری حساب‌های کاربری از طریق وی‌فیشینگ، و بهره‌برداری از اعتبارنامه‌های سرقت‌شده، همگی نشان‌دهنده تمرکز مهاجمان بر دسترسی و هویت هستند. در کنار آن، افشای نقص‌ها در ابزارهای مدیریتی و حتی سامانه‌های مبتنی بر هوش مصنوعی، پیچیدگی‌های جدیدی به چشم‌انداز تهدید افزوده است.

در نهایت، این تحولات یک پیام روشن دارند: امنیت دیگر یک لایه افزوده نیست، بلکه باید به‌عنوان بخشی جدایی‌ناپذیر از طراحی، توسعه و بهره‌برداری از سیستم‌ها در نظر گرفته شود.

مهم ترین اخبار و مطالب هفته

- سواستفاده از آسیب‌پذیری اجرای کد از راه دور (RCE) در BeyondTrust در حملات باج‌افزاری ادامه خبر
- وصله نخستین آسیب‌پذیری روز-صفر Chrome در سال جاری توسط گوگل ادامه خبر
- هدف‌گیری حساب‌های Microsoft Entra در حملات وی‌فیشینگ با کد دستگاه ادامه خبر
- افشای آسیب‌پذیری بحرانی Windows Admin Center توسط مایکروسافت ادامه خبر
- مایکروسافت: نقص باعث خلاصه‌سازی ایمیل‌های محرمانه توسط Copilot ادامه خبر
- تبدیل اعتبارنامه‌های سرقت‌شده به هویت‌های واقعی توسط بدافزارهای Infostealer ادامه خبر
- آشکارسازی کلیدها در JavaScript از طریق ۵ میلیون اپلیکیشن ادامه خبر

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

[۱] سواستفاده از آسیب‌پذیری اجرای کد از راه دور (RCE) در BeyondTrust در حملات باج-افزاری

آژانس امنیت سایبری و زیرساخت‌های ایالات متحده (CISA) از سوءاستفاده فعال هکرها از آسیب‌پذیری CVE-2026-1731 در محصول BeyondTrust Remote Support هشدار داده است.

این مشکل امنیتی نسخه‌های Remote Support 25.3.1 (یا قدیمی‌تر) و Privileged Remote Access 24.3.4 (یا قدیمی‌تر) را تحت تأثیر قرار می‌دهد و امکان اجرای کد از راه دور را فراهم می‌کند.

CISA این آسیب‌پذیری را در تاریخ ۱۳ فوریه به فهرست آسیب‌پذیری‌های شناخته‌شده مورد سوءاستفاده (KEV) اضافه کرده و به نهادهای فدرال تنها سه روز فرصت داده تا به‌روزرسانی را اعمال کنند یا از محصول استفاده نکنند.

شرکت BeyondTrust در تاریخ ۶ فوریه، آسیب‌پذیری CVE-2026-1731 را افشا کرد. این هشدار امنیتی، آن را به‌عنوان یک آسیب‌پذیری اجرای کد از راه دور پیش از احراز هویت معرفی کرده که ناشی از ضعف تزریق دستور سیستم‌عامل بوده و از طریق درخواست‌های مشتری ویژه ارسال‌شده به نقاط آسیب‌پذیر قابل سوءاستفاده است.

نمونه‌های اثبات مفهوم (PoC) برای CVE-2026-1731 بلافاصله پس از افشا در دسترس قرار گرفت و سوءاستفاده واقعی در محیط‌های واقعی تقریباً بلافاصله آغاز شد.

در تاریخ ۱۳ فوریه، BeyondTrust بولتن را به‌روزرسانی کرده و اعلام نمود که سوءاستفاده از این آسیب‌پذیری از تاریخ ۳۱ ژانویه شناسایی شده است، بنابراین CVE-2026-1731 حداقل برای یک هفته یک آسیب‌پذیری روز-صفر (Zero-Day) بوده است.

همچنین اعلام کرده است که گزارش محقق Harsh Jaiswal و تیم Hacktron AI فعالیت غیرعادی شناسایی‌شده در یک دستگاه Remote Support را تأیید کرده است.

CISA اکنون نشانگر «شناخته‌شده در کمپین‌های باج‌افزاری» را در فهرست KEV فعال کرده است. برای مشتریان نسخه ابری (SaaS)، شرکت اعلام کرده که وصله به‌صورت خودکار در تاریخ ۲ فوریه اعمال شده و نیازی به اقدام دستی نیست.

مشتریان نسخه‌های خودمیزبان باید یا به‌روزرسانی خودکار را فعال کنند و از طریق رابط 'appliance/' تأیید کنند که وصله اعمال شده یا آن را به‌صورت دستی نصب نمایند.

برای Remote Support، توصیه می‌شود نسخه ۲۵.۳.۲ نصب شود. کاربران Privileged Remote Access باید به نسخه ۲۵.۱.۱ یا جدیدتر ارتقا یابند. برای کسانی که هنوز از RS نسخه ۲۱.۳ و PRA نسخه ۲۲.۱ استفاده می‌کنند، توصیه می‌شود قبل از اعمال وصله، به نسخه جدیدتری ارتقا دهند.

[۲] وصله نخستین آسیب‌پذیری روز-صفر Chrome در سال جاری توسط گوگل

شرکت گوگل به‌روزرسانی اضطراری برای رفع یک آسیب‌پذیری با شدت بالا در Google Chrome منتشر کرده است؛ نقصی که در حملات روز-صفر مورد سوءاستفاده قرار گرفته و نخستین آسیب‌پذیری از این نوع در سال جاری محسوب می‌شود.

گوگل در اطلاعیه امنیتی اعلام کرد که اکسپلویت مربوط به CVE-2026-2441 در حال بهره‌برداری در دنیای واقعی است. بر اساس تاریخچه تغییرات پروژه Chromium، این آسیب‌پذیری از نوع use-after-free بوده که توسط پژوهشگر امنیتی Shaheen Fazim گزارش شده است. ریشه مشکل به یک خطای «iterator invalidation» در مؤلفه CSSFontFeatureValuesMap مربوط می‌شود؛ بخشی از پیاده‌سازی ویژگی‌های فونت CSS در Chrome. بهره‌برداری موفق از این نقص می‌تواند منجر به کرش مرورگر، اختلال در رندر، تخریب داده‌ها یا رفتارهای پیش‌بینی‌نشده دیگر شود.

در پیام ثبت تغییرات (commit) اشاره شده که وصله CVE-2026-2441 مشکل فوری را برطرف می‌کند، اما همچنان «کارهای باقی‌مانده» تحت باگ ۴۸۳۹۳۶۰۷۸ در حال پیگیری است؛ موضوعی که نشان می‌دهد این اصلاح ممکن است موقتی باشد یا مسائل مرتبط دیگری هنوز نیازمند رسیدگی باشند.

این وصله در چندین کامیت به‌صورت «cherry-pick» (بازانتقال به نسخه پایدار) اعمال شده است؛ نشانه‌ای از اهمیت بالای آن و ضرورت انتشار در نسخه پایدار، احتمالاً به دلیل بهره‌برداری فعال از آسیب‌پذیری در دنیای واقعی.

با وجود تأیید سوءاستفاده از این نقص روز-صفر، گوگل جزئیات بیشتری درباره حملات منتشر نکرده است. گوگل اعلام کرده است که دسترسی به جزئیات باگ و لینک‌های مرتبط ممکن است تا زمانی که اکثریت کاربران به‌روزرسانی را دریافت کنند، محدود باقی بماند. همچنین اگر این نقص در یک کتابخانه شخص ثالث وجود داشته باشد که پروژه‌های دیگر نیز به آن وابسته‌اند و هنوز اصلاح نشده، محدودیت‌ها حفظ خواهد شد.

گوگل این آسیب‌پذیری را برای کاربران کانال پایدار دسکتاپ Google Chrome برطرف کرده و نسخه‌های جدید برای ویندوز، macOS (۷۶/۱۴۵.۰.۷۶۳۲.۷۵) و لینوکس (۱۴۴.۰.۷۵۵۹.۷۵) طی روزها یا هفته‌های آینده به‌صورت تدریجی منتشر می‌شوند.

کاربرانی که تمایلی به به‌روزرسانی دستی ندارند، می‌توانند اجازه دهند Chrome به‌صورت خودکار بررسی و پس از اجرای مجدد مرورگر، وصله را نصب کند.

این نخستین آسیب‌پذیری روز-صفر Chrome در سال ۲۰۲۶ است که بهره‌برداری فعال از آن تأیید و وصله شده است. سال گذشته نیز گوگل در مجموع هشت آسیب‌پذیری روز-صفر مورد سوءاستفاده در دنیای واقعی را برطرف کرد که بسیاری از آن‌ها توسط گروه تحلیل تهدید این شرکت، Google Threat Analysis Group (TAG)، گزارش شده بودند؛ گروهی که به رصد و شناسایی روز-صفرهای مورد استفاده در حملات جاسوس‌افزاری علیه اهداف پر ریسک شهرت دارد.

[۳] هدف‌گیری حساب‌های Microsoft Entra در حملات وی‌فیشینگ با کد دستگاه

عاملان تهدید، سازمان‌های فناوری، تولید و مالی را در کمپین‌هایی هدف قرار می‌دهند که ترکیبی از فیشینگ با کد دستگاه و وی‌فیشینگ (vishing) بوده و جریان احراز هویت دستگاه OAuth 2.0 را سوءاستفاده می‌کنند تا حساب‌های Microsoft Entra را به خطر بیندازند.

برخلاف حملات قبلی که از برنامه‌های مخرب OAuth برای نفوذ به حساب‌ها استفاده می‌کردند، این کمپین‌ها از شناسه‌های کلاینت OAuth قانونی مایکروسافت و جریان احراز هویت دستگاه استفاده می‌کنند تا قربانیان را به احراز هویت فریب دهند.

این روش به مهاجمان توکن‌های احراز هویت معتبر می‌دهد که بدون نیاز به سایت‌های فیشینگ معمول یا سرقت رمز عبور و کدهای چندمرحله‌ای، امکان دسترسی به حساب قربانی را فراهم می‌کند.

منابع گزارش می‌دهند گروه ShinyHunters پشت حملات وی‌فیشینگ با کد دستگاه است، موضوعی که عاملان تهدید بعداً تأیید کردند. این گروه قبلاً برای نفوذ به حساب‌های SSO Okta و Microsoft Entra و سرقت داده‌ها شناخته شده‌اند. مایکروسافت در حال حاضر اطلاعاتی برای ارائه ندارد.

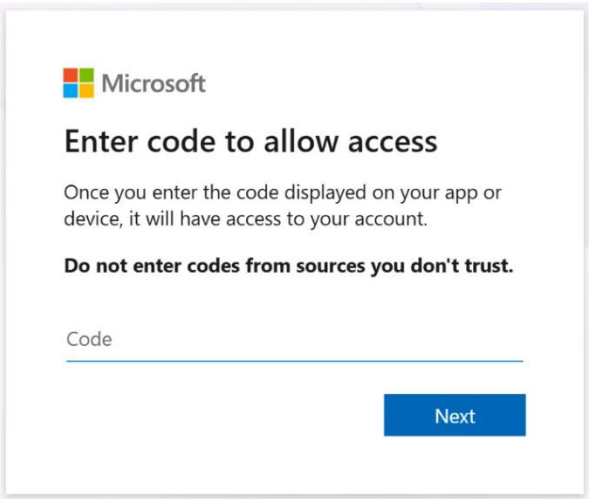
حملات مهندسی اجتماعی با کد دستگاه

BleepingComputer از منابع متعدد مطلع شده است که عاملان تهدید، حملات وی‌فیشینگ را آغاز کرده‌اند که بدون نیاز به زیرساخت تحت کنترل مهاجم، با استفاده از فرم‌های ورود قانونی مایکروسافت و جریان احراز هویت کد دستگاه، به حساب‌های سازمانی نفوذ می‌کنند.

در این حمله، جریان قانونی OAuth 2.0 Device Authorization سوءاستفاده شده تا توکن‌های احراز هویت Microsoft Entra قربانی به‌دست آید و مهاجمان به منابع و برنامه‌های متصل SSO مانند Microsoft 365، Salesforce، Google Workspace، Dropbox، Slack و دیگران دسترسی پیدا کنند.

این جریان برای دستگاه‌های با ورودی محدود مانند IoT، چاپگرها و تلویزیون‌ها طراحی شده و مشابه ورود به سرویس‌های پخش مانند Netflix است، جایی که کاربر با وارد کردن کد کوتاه روی یک دستگاه دیگر، ورود را تکمیل می‌کند.

مهاجمان با استفاده از client_id یک اپلیکیشن OAuth قانونی، کدهای device_code و user_code تولید کرده و کارمند هدف را به وارد کردن آن‌ها در صفحه microsoft.com/devicelogin ترغیب می‌کنند.



Microsoft's device authentication form

زمانی که فرد هدف کد را وارد می‌کند، از او خواسته می‌شود مانند ورود عادی، نام کاربری و رمز عبور خود را وارد کرده و مراحل احراز هویت چندمرحله‌ای (MFA) را تکمیل کند. پس از احراز هویت، مایکروسافت نام برنامه OAuth تأییدشده را نمایش می‌دهد. با این حال، از آنجا که مهاجمان می‌توانند از برنامه‌های قانونی حتی برنامه‌های خود مایکروسافت استفاده کنند، این موضوع به فرایند احراز هویت ظاهر معتبرتر و قابل‌اعتمادتری می‌دهد.

پس از اتصال اپلیکیشن OAuth به حساب، مهاجمان می‌توانند از device_code برای به‌دست آوردن توکن تازه‌سازی (refresh token) قربانی هدف استفاده کنند و سپس آن را به توکن‌های دسترسی تبدیل کنند.

این توکن‌های دسترسی به مهاجمان امکان می‌دهند بدون انجام مجدد احراز هویت چندمرحله‌ای (MFA) به سرویس‌های مایکروسافت کارمند دسترسی پیدا کنند، زیرا MFA در ورود اولیه انجام شده است.

مهاجمان اکنون می‌توانند به‌عنوان کاربر وارد Microsoft Entra شوند و به برنامه‌های SaaS متصل با SSO در سازمان قربانی دسترسی پیدا کنند، که امکان سرقت داده‌های سازمانی برای باج‌گیری را فراهم می‌کند.

KnowBe4 Threat Labs نیز یک کمپین اخیر را شناسایی کرده که از ایمیل‌ها و وب‌سایت‌های فیشینگ سنتی برای حملات device code استفاده می‌کند. این کمپین که ابتدا در دسامبر ۲۰۲۵ شناسایی شد، عمدتاً بر فریب‌های مهندسی اجتماعی مانند هشدارهای جعلی تنظیم پرداخت، اعلان‌های اشتراک‌گذاری اسناد و پیام‌های صوتی دروغین تکیه دارد.

KnowBe4 توصیه می‌کند دارندگان حساب Microsoft 365 دامنه‌ها و آدرس‌های فرستنده مخرب را مسدود کرده، مجوزهای مشکوک اپلیکیشن‌های OAuth را بررسی و لغو کنند و لاگ‌های ورود Azure AD مربوط به احراز هویت با کد دستگاه را مرور نمایند.

به مدیران سیستم نیز توصیه می‌شود جریان Device Code را زمانی که لازم نیست غیرفعال کنند و سیاست‌های دسترسی شرطی (Conditional Access) را اعمال نمایند.

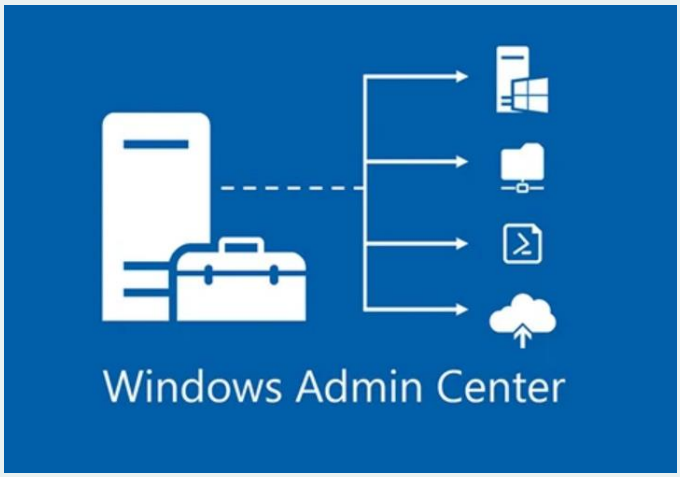
حملات فیشینگ با کد دستگاه روش جدیدی نیست و پیش‌تر چندین عامل تهدید از این روش برای نفوذ به حساب‌ها استفاده کرده‌اند.

در فوریه ۲۰۲۵، مرکز اطلاعات تهدید مایکروسافت هشدار داد که هکرهای روسی حساب‌های Microsoft 365 را با استفاده از فیشینگ کد دستگاه هدف قرار می‌دهند.

در دسامبر، ProofPoint حملات مشابهی را گزارش کرد که از کیت فیشینگ مشابهی که توسط KnowBe4 شناسایی شده بود، برای نفوذ به حساب‌های مایکروسافت استفاده می‌کردند.

[۴] افشای آسیب‌پذیری بحرانی Windows Admin Center توسط مایکروسافت

شرکت مایکروسافت یک آسیب‌پذیری افزایش سطح دسترسی را در Windows Admin Center (WAC) افشا کرده است؛ پلتفرم مبتنی بر مرورگری که به‌طور گسترده توسط مدیران IT و تیم‌های زیرساخت برای مدیریت کلاینت‌ها و سرورهای ویندوز، کلاسترها، میزبان‌های Hyper-V و ماشین‌های مجازی، همچنین سیستم‌های عضو Active Directory استفاده می‌شود.



این نقص امنیتی با انتشار نسخه ۲۵۱۱ از Windows Admin Center در اوایل دسامبر ۲۰۲۵ برطرف شد، اما اکنون به‌صورت عمومی اعلام شده است. تأخیر در افشا احتمالاً به ماهیت آسیب‌پذیری، شدت آن و حساسیت عملیاتی WAC به‌عنوان یک ابزار مدیریت متمرکز مربوط می‌شود.

درباره CVE-2026-26119

آسیب‌پذیری CVE-2026-26119 ناشی از احراز هویت نامناسب بوده و در ژوئیه ۲۰۲۵ توسط Adrea Pierini، مشاور امنیتی شرکت Semperis، کشف شده است.

جزئیات فنی هنوز منتشر نشده است اما امتیاز CVSS نشان می‌دهد که این نقص می‌تواند از راه دور، با تلاش کم، بدون نیاز به تعامل کاربر و با حداقل سطح دسترسی (داشتن اعتبارنامه معتبر سطح پایین) مورد سوءاستفاده قرار گیرد.

به گفته مایکروسافت، بهره‌برداری موفق از این آسیب‌پذیری می‌تواند به مهاجم سطح دسترسی کاربری را بدهد که برنامه آسیب‌پذیر را اجرا می‌کند. Pierini نیز اشاره کرده که «در شرایط خاص، این مشکل می‌تواند از یک کاربر عادی به سازش کامل دامنه منجر شود.»

مایکروسافت احتمال سوءاستفاده از این نقص را «بیشتر» ارزیابی کرده، زیرا امکان توسعه کد بهره‌برداری قابل‌اعتماد وجود دارد و آسیب‌پذیری‌های مشابه پیش‌تر در حملات واقعی هدف قرار گرفته‌اند. این شرکت توصیه کرده سازمان‌هایی که این به‌روزرسانی را مرتبط با محیط خود می‌دانند، آن را با اولویت بالا اعمال کنند. سازمان‌هایی که هنوز به نسخه اصلاح‌شده ارتقا نداده‌اند، باید هرچه سریع‌تر این کار را انجام دهند تا پیش از توسعه اکسپلویت توسط مهاجمان، در برابر سوءاستفاده احتمالی ایمن شوند.

[۵] مایکروسافت: نقص باعث خلاصه‌سازی ایمیل‌های محرمانه توسط Copilot

شرکت مایکروسافت اعلام کرده که یک نقص در Microsoft 365 Copilot از اواخر ژانویه باعث شده این دستیار هوش مصنوعی ایمیل‌های محرمانه را خلاصه‌سازی کند و سیاست‌های پیشگیری از دست رفتن داده (DLP) که سازمان‌ها برای حفاظت از اطلاعات حساس استفاده می‌کنند را دور بزند.

بر اساس هشدار سرویس مشاهده‌شده توسط BleepingComputer، این نقص (با شناسه CW1226324 و اولین‌بار در ۲۱ ژانویه شناسایی شده) ویژگی چت در تب Work از Copilot را تحت تأثیر قرار می‌دهد و به‌طور نادرست ایمیل‌های موجود در پوشه‌های Sent Items و Drafts کاربران، از جمله پیام‌هایی با برچسب محرمانگی که برای محدود کردن دسترسی ابزارهای خودکار طراحی شده‌اند، می‌خواند و خلاصه می‌کند.

Copilot Chat، نسخه چت Microsoft 365 Copilot، چتی هوشمند با قابلیت درک محتواست که به کاربران امکان تعامل با عامل‌های هوش مصنوعی را می‌دهد. مایکروسافت این قابلیت را از سپتامبر ۲۰۲۵ برای کاربران تجاری Microsoft 365 در Word، Excel، PowerPoint، Outlook و OneNote منتشر کرده است.

شرکت مایکروسافت تایید کرده که «ایمیل‌های کاربران با برچسب محرمانه به‌طور نادرست توسط چت Microsoft 365 Copilot پردازش می‌شوند».

مایکروسافت افزود: «چت تب Work در Copilot حتی ایمیل‌هایی که برچسب حساسیت دارند و سیاست DLP برای آن‌ها تنظیم شده را خلاصه می‌کند».

این شرکت اعلام کرده که یک خطای کدنویسی نامشخص دلیل مشکل است و از اوایل فوریه، به‌روزرسانی برای رفع آن آغاز شده است. تا روز چهارشنبه، مایکروسافت همچنان روند استقرار وصله را نظارت می‌کند و با بخشی از کاربران آسیب‌دیده تماس می‌گیرد تا صحت عملکرد اصلاحیه را بررسی کند.

مایکروسافت توضیح داد: «یک مشکل کد اجازه می‌دهد موارد موجود در پوشه‌های Sent Items و Draft توسط Copilot پردازش شوند، حتی اگر برچسب محرمانه روی آن‌ها تنظیم شده باشد».

شرکت هنوز جدول زمانی نهایی برای رفع کامل مشکل ارائه نکرده و تعداد کاربران یا سازمان‌های آسیب‌دیده را مشخص نکرده است و گفته تنها دامنه تأثیر ممکن است با ادامه تحقیقات تغییر کند.

این حادثه به‌عنوان یک هشدار سرویس (advisory) برچسب‌گذاری شده که معمولاً برای مشکلات محدود یا با اثر محدود استفاده می‌شود.

به‌روزرسانی ۱۹ فوریه: مایکروسافت اعلام کرد که مشکل باعث نمی‌شد کسی به اطلاعاتی دسترسی پیدا کند که قبلاً مجاز نبود، اما این رفتار با تجربه مورد انتظار Copilot مطابقت نداشت و یک به‌روزرسانی پیکربندی برای مشتریان سازمانی در سراسر جهان اعمال شده است.

به‌روزرسانی ۲۰ فوریه: مایکروسافت گزارش داده که علت ریشه‌ای مشکل برطرف شده و وصله هدفمند برای جلوگیری از تأثیر بیشتر در اکثریت محیط‌های آسیب‌دیده اعمال شده است. روند استقرار تنها برای بخش کوچکی از محیط‌های پیچیده باقی مانده و پس از دریافت اصلاحیه، ایمیل‌های جدید تحت تأثیر قرار نخواهند گرفت.

[۶] تبدیل اعتبارنامه‌های سرقت‌شده به هویت‌های واقعی توسط بدافزارهای Infostealer

بدافزارهای مدرن Infostealer سرقت اعتبارنامه‌ها را فراتر از نام‌های کاربری و گذرواژه‌ها گسترش داده‌اند. در یک سال گذشته، کمپین‌ها با سرعت بیشتری اجرا شده و کاربران را بدون تمایز بین کارکنان سازمانی و افراد با دستگاه‌های شخصی هدف قرار داده‌اند.

بدافزارهای مدرن Infostealer سرقت اعتبارنامه‌ها را فراتر از نام‌های کاربری و گذرواژه‌ها گسترش داده‌اند. در یک سال گذشته، کمپین‌ها با سرعت بیشتری اجرا شده و کاربران را بدون تمایز بین کارکنان سازمانی و افراد با دستگاه‌های شخصی هدف قرار داده‌اند.
این بدافزارها معمولاً هم‌زمان با جمع‌آوری اعتبارنامه‌ها، داده‌های نشست و فعالیت کاربران را نیز برداشت می‌کنند. مجموعه داده‌های به‌دست‌آمده توسط کارگزاران دسترسی اولیه تجمیع و فروخته شده و سپس در حملات دیگر علیه محیط‌های شخصی و سازمانی مجدداً استفاده می‌شوند.

برای درک بهتر دامنه و پیامدهای این فعالیت، محققان Specops بیش از ۹۰,۰۰۰ دیتادمپ Infostealer را تحلیل کردند که بیش از ۸۰۰ میلیون رکورد داده جمع‌آوری‌شده در طول عفونت‌های فعال را شامل می‌شد.

این مجموعه داده‌ها شامل اعتبارنامه‌ها، کوکی‌های مرورگر، تاریخچه مرور و فایل‌های سطح سیستم ذخیره‌شده محلی روی دستگاه‌های آلوده بود.

نتیجه بررسی تصویر روشنی از نحوه استفاده مهاجمان از داده‌های فنی برای مرتبط کردن آن‌ها با کاربران واقعی، سازمان‌ها و الگوهای رفتاری ارائه می‌دهد و نشان می‌دهد که یک آلودگی حتی پس از نفوذ اولیه نیز ارزشمند باقی می‌ماند. زمانی که اعتبارنامه‌های سرقت‌شده به داده‌های هویتی تبدیل می‌شوند

بزرگ‌ترین ریسک این است که داده‌های Infostealer به‌راحتی چندین حساب و رفتار را به یک فرد واقعی مرتبط می‌کنند. این دیتادمپ‌ها معمولاً نام‌های کاربری تکراری در سرویس‌های مختلف، نام کاربری ویندوز، فایل‌های ذخیره‌شده در پوشه‌های کاربر، داده‌های نشست فعال و سوابق دقیق فعالیت در محیط‌های گوناگون را افشا می‌کنند.

ترکیب این نشانه‌ها به مهاجمان اجازه می‌دهد از یک اعتبارنامه به‌خطرافتاده به شناسایی فرد، محل کار او و حتی نقش احتمالی‌اش در سازمان برسند.

این همگرایی، مرز میان هویت شخصی و حرفه‌ای را که بسیاری از مدل‌های امنیتی بر اساس آن طراحی شده‌اند، از بین می‌برد. در نتیجه، نفوذی که ممکن است از یک دستگاه شخصی آغاز شود، می‌تواند به‌سرعت به ریسک سطح سازمانی تبدیل شود.

راهکار Specops Password Policy با اسکن مداوم Active Directory در برابر پایگاه داده‌ای شامل بیش از ۵.۴ میلیارد اعتبارنامه افشاشده، به سازمان‌ها کمک می‌کند این زنجیره را قطع کنند؛ رویکردی که فراتر از بررسی گذرواژه تنها در زمان ایجاد یا بازنشانی عمل می‌کند.

اعتبارنامه‌هایی که پیش‌تر افشا شده‌اند، حتی اگر از نظر فنی با سیاست‌های رمز عبور سازمان مطابقت داشته باشند، مسدود می‌شوند و امکان تنظیم یا استفاده مجدد از آن‌ها وجود نخواهد داشت؛ اقدامی که ریسک استفاده مجدد از گذرواژه‌های به‌خطرافتاده در حساب‌های شخصی و سازمانی را کاهش می‌دهد.

محل جمع‌آوری داده‌ها توسط Infostealer و سوءاستفاده از آن‌ها

دیتاست جمع‌آوری‌شده شامل اعتبارنامه‌ها و داده‌های نشست مرتبط با طیف وسیعی از سرویس‌ها بود که نشان می‌دهد چگونه داده‌های Infostealer هم هویت و هم دسترسی را افشا می‌کنند.

سرویس‌های حرفه‌ای و سازمانی

LinkedIn، GitHub، Microsoft Teams، Outlook و دامنه‌های سازمانی به‌طور مکرر در دیتاست دیده شدند. تنها LinkedIn تقریباً ۹۰۰,۰۰۰ رکورد ارائه داد که مسیر مستقیمی از داده‌های سرقت‌شده به نام واقعی، عنوان شغلی و وابستگی سازمانی کاربر ایجاد می‌کند. برای عاملان تهدید، این اطلاعات امکان فیشینگ هدفمند، مهندسی اجتماعی و اولویت‌بندی دسترسی به محیط‌های سازمانی را فراهم می‌کند، به‌ویژه در جایی که گذرواژه‌ها دوباره استفاده می‌شوند.

هویت شخصی و شبکه‌های اجتماعی

پلتفرم‌هایی مانند YouTube و Facebook نیز در حجم بالا ظاهر شدند. این سرویس‌ها معمولاً شامل نام واقعی، عکس و ارتباطات اجتماعی هستند که شناسایی کاربران آسیب‌دیده و اتصال آن‌ها به سایر حساب‌ها را آسان می‌کند و بهره‌برداری هدفمند را ساده‌تر می‌سازد.

سرویس‌های حساس و پرریسک

دیتاست همچنین اعتبارنامه‌ها و کوکی‌های مرتبط با سرویس‌های حساس، از جمله دامنه‌های دولتی و مالیاتی مانند IRS و Canada Revenue Agency و همچنین پلتفرم‌های محتوای بزرگسالان را شامل می‌شد. دسترسی به این سرویس‌ها ریسک‌هایی فراتر از تصاحب حساب سنتی ایجاد می‌کند. در حوادث گذشته، عاملان تهدید از داده‌های پلتفرم‌های بزرگسالان برای باج‌گیری استفاده کرده‌اند و وقتی این داده‌ها به هویت واقعی و محل کار فرد مرتبط شود، تأثیر آن به سرعت افزایش می‌یابد.

آگاهی امنیتی اما همچنان آسیب‌پذیر

دامنه‌هایی مانند Shodan و حتی mil.gov نیز در دیتاست ظاهر شدند، که نشان می‌دهد آگاهی فنی تضمین ایمنی نیست. اقدامات امنیتی رعایت‌شده در محیط‌های سازمانی همیشه در سیستم‌های شخصی اجرا نمی‌شوند، اما افشا در این سیستم‌ها می‌تواند همچنان ریسک سازمانی ایجاد کند.

علت مؤثر بودن Infostealer

افشای داده‌ها توسط Infostealer ناشی از یک شکست منفرد نیست، بلکه ترکیبی از رفتارهای رایج تکرارشونده در مقیاس بزرگ است: نصب نرم‌افزار از منابع غیرقانونی، استفاده دوباره از گذرواژه‌ها در حساب‌های شخصی و سازمانی و ذخیره‌سازی اعتبارنامه‌ها در مرورگر برای راحتی.

اعتبارنامه‌ها و داده‌های پرداخت ذخیره‌شده در مرورگر، به‌ویژه برای مهاجمان ارزشمند هستند. زمانی که Infostealer سیستمی را آلوده می‌کند، این ذخیره‌ها دسترسی فوری به اطلاعات با ارزش را فراهم می‌کنند و تأثیر یک عفونت را به‌طور قابل‌توجهی افزایش می‌دهند.

کاهش تأثیر پس از سرقت اعتبارنامه

زمانی که داده‌های Infostealer جمع‌آوری و منتشر شد، پیشگیری تنها چالش نیست؛ سؤال اصلی این است که مدافعان چقدر سریع می‌توانند آن‌ها را قبل از استفاده مجدد برای حرکت جانبی، تصاحب حساب یا اجرای باج‌افزار خنثی کنند.

با توجه به اینکه دیتادمپ‌های Infostealer اغلب هفته‌ها یا ماه‌ها قبل از شناسایی در گردش هستند، کاهش تأثیر مؤثر باید فرض کند که برخی اعتبارنامه‌ها پیش‌تر افشا شده‌اند. استفاده دوباره از گذرواژه‌ها یکی از مطمئن‌ترین روش‌ها برای عملیاتی کردن داده‌های Infostealer است. اعتبارنامه‌های جمع‌آوری‌شده از دستگاه‌های شخصی به‌طور معمول علیه محیط‌های سازمانی، سرویس‌های ابری و سیستم‌های دسترسی از راه دور آزمایش

می‌شوند و اغلب موفقیت‌آمیز هستند، حتی زمانی که این گذرواژه‌ها از نظر پیچیدگی استاندارد رعایت شده باشند.

قطع استفاده دوباره از گذرواژه‌ها، ارزش عملیاتی دیتاست‌های Infostealer را کاهش می‌دهد و زمان بهره‌برداری را کوتاه می‌کند. همراه با سیاست‌های گذرواژه قوی‌تر که از عبارات عبور طولانی و اجرای مداوم پشتیبانی می‌کنند، این کنترل‌ها امنیت گذرواژه را از یک پیکربندی ایستا به یک اقدام فعال برای محدودسازی تهدید تبدیل می‌کنند.

از آنجایی که افشای هویت روزبه‌روز خارج از محدوده سازمان آغاز می‌شود، کاهش استفاده مجدد و تأثیرات بعدی اعتبارنامه‌های سرقت‌شده یکی از مؤثرترین روش‌ها برای شکست زنجیره‌های حمله مبتنی بر Infostealer است.

[۷] آشکارسازی کلیدها در JavaScript از طریق ۵ میلیون اپلیکیشن

آشکارسازی کلیدهای API لو رفته چیز جدیدی نیست، اما مقیاس مشکل در کدهای فرانت‌اند تا پیش از این largely ناشناخته بود. تیم تحقیقاتی Intruder یک روش جدید برای شناسایی کلیدها ایجاد کرده و ۵ میلیون اپلیکیشن را برای یافتن کلیدهای مخفی در بسته‌های JavaScript اسکن کرد. نتایج نشان‌دهنده شکاف بزرگی در نحوه ایمن‌سازی برنامه‌های تک‌صفحه‌ای (SPA) توسط صنعت بود.

۴۲,۰۰۰ کلید در معرض دید

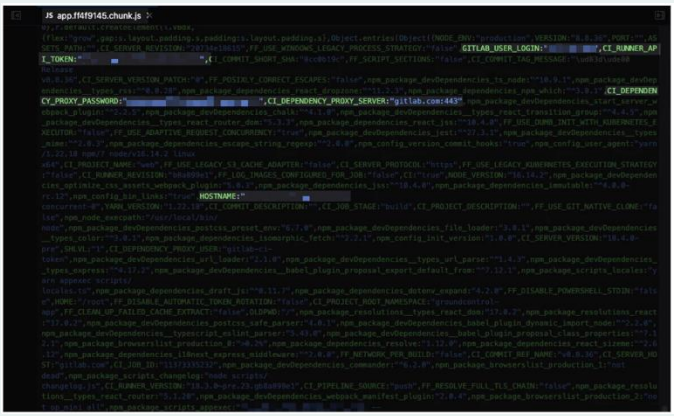
اعمال روش شناسایی جدید در مقیاس بزرگ نتایج شگفت‌انگیزی داشت. فایل خروجی تنها بیش از ۱۰۰ مگابایت متن ساده بود و بیش از ۴۲,۰۰۰ توکن افشا شده در ۳۳۴ نوع راز مختلف را شامل می‌شد.

این‌ها صرفاً کلیدهای آزمایشی کم‌ارزش یا توکن‌های از کار افتاده نبودند. ما اعتبارنامه‌های فعال و حیاتی را در کد تولیدی یافتیم که عملاً کنترل‌های امنیتی که بیشتر سازمان‌ها به آن‌ها متکی هستند را دور می‌زدند. در ادامه، تقسیم‌بندی مهم‌ترین ریسک‌های کشف‌شده ارائه شده است.

توکن‌های مخزن کد

مهم‌ترین افشاها شامل توکن‌های مربوط به پلتفرم‌های مخزن کد مانند GitHub و GitLab بود. در مجموع ۶۸۸ توکن یافت شد که بسیاری از آن‌ها هنوز فعال بودند و دسترسی کامل به مخازن را فراهم می‌کردند.

در یک مورد، یک توکن دسترسی شخصی GitLab مستقیماً در یک فایل JavaScript جاسازی شده بود. این توکن امکان دسترسی به تمام مخازن خصوصی سازمان، از جمله کلیدهای خطوط لوله CI/CD برای سرویس‌های بعدی مانند AWS و SSH را داشت.



کلیدهای API مدیریت پروژه

یک افشای مهم دیگر شامل کلید API مربوط به Linear، یک اپلیکیشن مدیریت پروژه، بود که مستقیماً در کد فرانت‌اند جاسازی شده بود.

این توکن کل نمونه Linear سازمان را افشا می‌کرد، شامل تیکت‌های داخلی، پروژه‌ها و لینک‌ها به سرویس‌ها و پروژه‌های SaaS پایین‌دست.

دیگر کلیدهای کشف‌شده

ما کلیدهای افشا شده در طیف وسیعی از سرویس‌ها را شناسایی کردیم، از جمله:

- API نرم‌افزار CAD – دسترسی به داده‌های کاربر، متادیتای پروژه و طرح‌های ساختمانی، از جمله یک بیمارستان
- پلتفرم‌های ایمیل – دسترسی به فهرست‌های ایمیل، کمپین‌ها و داده‌های مشترکین
- وبهوک‌ها برای پلتفرم‌های چت و اتوماسیون – Slack 213، 2 Microsoft Teams، Discord 1 و Zapier 98، همه فعال
- مبدل‌های PDF – دسترسی به ابزارهای تولید اسناد شخص ثالث
- پلتفرم‌های تحلیل و هوش فروش – دسترسی به داده‌های جمع‌آوری‌شده شرکت و مخاطب
- کوتاه‌کننده‌های لینک – توانایی ایجاد و شمارش لینک‌ها

روش سنتی برای شناسایی کلیدها در اپلیکیشن‌ها، جستجوی مسیرهای شناخته‌شده و استفاده از عبارت‌های منظم برای تطبیق فرمت‌های شناخته‌شده است.

این روش مفید است اما محدودیت دارد و بسیاری از نوع‌های افشا، به‌ویژه آن‌هایی که نیاز به اسپایدر کردن اپلیکیشن یا احراز هویت دارند، شناسایی نمی‌شوند. **مثال:** قالب توکن دسترسی شخصی GitLab در Nuclei.

- اسکنر URL پایه را دریافت می‌کند، مانند https://portal.intruder.io/
- درخواست HTTP GET به همان URL ارسال می‌کند
- تنها پاسخ مستقیم آن درخواست را بررسی کرده و صفحات و منابع دیگر مثل فایل‌های JavaScript را نادیده می‌گیرد
- الگوی توکن GitLab را شناسایی می‌کند و در صورت یافتن، API عمومی GitLab را بررسی می‌کند
- اگر فعال باشد، هشدار صادر می‌شود

این روش ساده اما مؤثر است، به‌ویژه وقتی قالب‌ها مسیرهای رایج برای افشا را مشخص می‌کنند. با این حال، اسکنرهای زیرساخت معمولاً مرورگر هدلس اجرا نمی‌کنند و فایل‌های JavaScript لازم برای رندر صفحه را بررسی نمی‌کنند.

نقطه کور فرآیند ساخت

ابزارهای Static Application Security Testing (SAST) کد منبع را برای شناسایی آسیب‌پذیری‌ها بررسی می‌کنند و راه اصلی شناسایی کلیدها قبل از ورود به محیط تولید هستند. آن‌ها مؤثرند اما برخی کلیدهای موجود در بسته‌های JavaScript از دید تحلیل استاتیک پنهان می‌مانند.

چالش Dynamic Application Security Testing (DAST)

ابزارهای DAST عملکرد پیچیده‌تری دارند و می‌توانند اپلیکیشن‌ها را به‌طور کامل بررسی کرده و احراز هویت را پشتیبانی کنند. با این حال:

- هزینه بالا دارند
- پیکربندی پیچیده لازم است
- معمولاً فقط برای تعداد محدودی اپلیکیشن با ارزش اجرا می‌شوند
- بسیاری از ابزارهای DAST دامنه کافی برای شناسایی همه فرمت‌های توکن را ندارند

این شکاف باعث می‌شود که بسیاری از کلیدها در کد فرانت‌اند شناسایی نشوند، حتی وقتی SAST و اسکنرهای زیرساخت به‌کار گرفته شده‌اند.

حفظ کلیدهای واقعی

کنترل‌های shift-left اهمیت دارند؛ SAST، اسکن مخزن و guardrail های IDE مشکلات واقعی را می‌گیرند و از برخی دسته‌های افشا جلوگیری می‌کنند. اما همان‌طور که این تحقیق

نشان می‌دهد، همه مسیرهای ورود یک راز به محیط تولید پوشش داده نمی‌شوند.

کلیدهایی که در مراحل ساخت و استقرار معرفی می‌شوند، می‌توانند از این کنترل‌ها عبور کرده و وارد کد فرانت‌اند شوند. با افزایش خودکارسازی و کدنویسی مبتنی بر هوش مصنوعی، این مشکل جدی‌تر خواهد شد.

به همین دلیل، اسپایدر کردن اپلیکیشن‌های تک‌صفحه‌ای (SPA) برای شناسایی کلیدها قبل از ورود به محیط تولید ضروری است. تیم Intruder ابزار شناسایی خودکار کلیدهای SPA را توسعه داده تا تیم‌ها بتوانند این موارد را به‌طور مؤثر شناسایی کنند.