U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Privacy, Access, Civil Liberties, and Transparency
Washington, DC 20528

20 جون، 2024

همکار گرامی،

ممکن است خبر داشته باشید که، از 23 جنوری 2024 تا 26 جنوری 2024، ابزار ارزیابی امنیت کیمیایی (CSAT) متعلق به آژانس امنیت سایبری و امنیت زیرساخت (CISA)، مورد هدف یک نفوذ امنیت سایبری توسط یک عامل مخرب قرار گرفت، که به دسترسی غیرمجاز به ارسالی‌های ارائه شده به «برنامه تضمین پرسنل» و حساب های «کاربرانی که مجاز به دسترسی به معلومات آسیب پذیری کیمیایی-تروریسم» (CVI)، منجر شد.

در حالی که تحقیقات CISA هیچ مدرکی در مورد اخراج این داده‌ها پیدا نکرد، ما به تمامی افرادی که معلومات شناسایی شخصی (PII) آن‌ها جهت بررسی به برنامه استانداردهای ضدتروریسم تاسیسات کیمیایی CISA (CFATS) ارسال شده یا دارای حساب کاربری CVI Authorized User بودند، به دلیل احتیاط زیاد، اطلاع می‌دهیم که ممکن است این معلومات به‌طور نامناسبی مورد دسترسی قرار گرفته باشد. من نگرانی و ناامیدی شما را درک می کنم و اینجا هستم تا معلوماتی در مورد این تلاش برای نفوذ سایبری را در اختیار شما قرار دهم.

شما این اطلاع را دریافت می‌کنید زیرا (1) یک تاسیسات کیمیایی که در آن به ساحات ممنوعه و/یا دارایی‌های مهم دسترسی داشتید، ممکن است معلومات شناسایی شخصی شما (PII) را برای بررسی تحت «برنامه اطمینان از پرسونل» ارائه کرده باشد، یا (2) شما یا یک تاسیسات کیمیایی PII محدود و جزئیات تماس تجاری را برای ایجاد یک حساب کاربر مجاز CVI بین جون 2007 تا جولای 2023 ارسال کرده باشید. ما همچنین با تاسیسات کیمیایی که شما به آن وابسته هستید تماس گرفته ایم تا در مورد جنبه های فنی نفوذ صحبت کنیم.

معلوماتی که احتمالا تحت تاثیر قرار گرفته اند

برنامه اطمینان از پرسونل. برنامه اطمینان از پرسونل CFATS به مراکز تحت نظارت CFATS امکان مطابقت با استاندارد عملکرد مبتنی بر خطر 12(iv) (RBPS) — اطمینان از پرسونل را فراهم کرد. 12(iv) RBPS[1] پرسنل تأسیسات و بازدیدکنندگان بدون اسکورت را که به ساحات و دارایی‌های مهم در مراکز کیمیایی پرخطر دسترسی داشتند یا به دنبال دسترسی بودند را موظف کرد که از نظر داشتن روابط احتمالی با تروریزم بررسی شوند. این شامل ارسال PII از طریق CSAT برای بررسی مستقیم یا بررسی مجدد در برنامه‌های دیگر وزارت امنیت داخلی به منظور بررسی افراد در برابر دیتابیس یا پایگاه داده شناسایی تروریست‌ها بود[2].

PII که از طریق برنامه اطمینان از پرسونل ارسال شد، شامل نام فرد، تاریخ تولد، شهروندیت یا جنسیت بود. PII اضافی نیز ارائه شد، در صورت موجود بودن یا در صورت نیاز برای افراد غیر آمریکایی، شامل:

- نام‌های مستعار
- مفل تولد
- تابعیت
- شماره پاسپورت
- شماره جبران
- شماره A
- شماره شناسایی ورود جهانی
- شماره شناسایی TWIC

حساب‌های کاربری CSAT. در کل، دو نوع حساب کاربری برای مراکزی که معلومات خود را برای CSAT ارسال می‌کنند، وجود دارد: کاربران CSAT که نظرسنجی‌های تاپ سکرین (Top-Screen)، ارزیابی‌های آسیب‌پذیری امنیتی و برنامه‌های امنیتی سایت/محل (شامل کاربران مجاز CVI) را ارسال میکنند یا در توسعه آن دخیل هستند و کاربران

[1] 6 C.F.R. 27.230(a)(12)(iv).

[2] برای کسب معلومات بیشتر در مورد دیتابیس یا پایگاه داده شناسایی تروریست‌ها، به این صفحه انترنتی مراجعه کنید: https://www.fbi.gov/investigate/terrorism/tsc

CSAT که معلومات اطمینان از پرسونل را ارسال می‌کنند. در هر دو مورد، معلومات جمع آوری شده برای ایجاد یک حساب CSAT یکسان است: نام، عنوان، آدرس تجارت و شماره تلفن تجارت.

جزئیات نفوذ سایبری

در تاریخ 26 جنوری، CISA فعالیت‌های احتمالی مخرب[3] را که دستگاه CSAT Ivanti Connect Secure را تحت تأثیر قرار می‌داد، شناسایی کرد. سیزا به‌طور فوری سیستم را آفلاین کرد، برنامه را از بقیه شبکه جدا کرد و یک بررسی جنایی شروع کرد. این بررسی شامل کارشناسان فنی از دفتر رئیس معلومات CISA، تیم شکار تهدید امنیت سایبری ما و مرکز عملیات شبکه وزارت امنیت داخلی بود.

در طول بررسی، شناسایی کردیم که یک عامل مخرب یک وب‌شل پیشرفته را بر روی دستگاه Ivanti نصب کرده است. این نوع وب‌شل می‌تواند برای اجرای دستورات مخرب یا نوشتن فایل‌ها به سیستم بنیادی استفاده شود. تحلیل ما نشان داد که یک عامل مخرب در طول دو روز به صورت تکراری به وب‌شل دسترسی پیدا کرد.

مهم‌ترین امر این است که بررسی به پایان رسید و هیچ گونه اخراج داده از CSAT یا دسترسی مخربانه به دستگاه Ivanti شناسایی نشد. تمام معلومات موجود در CSAT با استفاده از رمزگذاری AES 256 رمزگذاری شده بود و معلومات هر برنامه دارای کنترل‌های امنیتی اضافی بودند که احتمال دسترسی افقی را محدود می‌کردند. کلیدهای رمزگذاری از نوع دسترسی‌ای که عامل تهدید به سیستم داشت، مخفی بودند.

توصیه ها برای افرادی که تحت تاثیر قرار گرفته اند

در حالی که تحقیقات هیچ مدرکی مبنی بر سرقت مدارک پیدا نکرد، به شما توصیه می‌کنیم که دستورالعمل‌های CISA را در مورد نحوه محافظت از خود در برابر حملات روش خردمند/نیرومند (Brute Force) که توسط عاملین سایبری انجام می‌شود بخوانید و دنبال کنید (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), انتخاب و محافظت از پسوردها (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), and تأیید هویت چند مرحله‌ای (https://www.cisa.gov/MFA).

CISA یک وب‌سایتی ایجاد کرده است که حاوی کاپی‌هایی از این اطلاعیه، پرسش‌های متداول، به‌روزرسانی‌های دوره‌ای و یک فرصت برای ثبت‌نام در لیست توزیع ایمیل برای دریافت به‌روزرسانی‌ها در وب‌سایت می‌باشد. در حالی که CISA در حال بررسی راه‌حل‌های احتمالی اضافی است، ما شما را تشویق می‌کنیم که در فهرست توزیع ما برای این حادثه ثبت نام کنید تا آخرین به‌روزرسانی‌ها را در www.cisa.gov/csat-notification دریافت کنید. سوالات افراد تحت تأثیر این حادثه باید به بخش امنیت کیمیایی CISA به آدرس CFATS.Notifications@cisa.dhs.gov ارسال شود.

با احترام،

James Burd

افسر حریم خصوصی

[3] برای کسب معلومات بیشتر در مورد این نوع فعالیت‌های مخرب، به این صفحه مراجعه کنید: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b