گزارش سالانه‌ی بررسی نقش مرورگر در کاهش یا افزایش حملات سایبری

APK | Engineering and Technical Company
Amn Pardazan Kavir

مرورگر به شاخص‌ترین واسط کاری در سازمان‌های امروزی تبدیل شده است. در نتیجه به کانون چشم‌انداز تهدید گسترده‌ای مبدل گشته که داده‌ها، دستگاه‌ها و برنامه‌های کاربردی را در معرض خطر قرار می‌دهد.
این حملات، از استفاده از مرورگر برای دسترسی مخرب به برنامه‌های SaaS تا سرقت داده‌های حساسی که روی آن ذخیره شده است یا سوء استفاده از آن جهت به خطر انداختن نقطه پایانی که روی آن اجرا می‌شود را دربر می‌گیرند. اما تیم‌های امنیتی تا به اینجا آن‌ها را ترکیبی از خطرات نقاط پایانی پراکنده، هویت و SaaS در نظر گرفته‌اند. در نتیجه، تا کنون تلاشی برای تحلیل و درک این حملات سایبری انجام نشده، یک اکوسیستم تهدید مبتنی بر مرورگر، در حال تکاملی که حجم و پیچیدگی‌اش به‌سرعت درحال افزایش است.
تیم LayerX پژوهشی گسترده انجام داده است تا اولین گزارش سالانه‌ی امنیت مرورگر را تهیه کند که قابلیت دید جامع و بینشی تفصیلی از چگونگی فعالیت‌های مرورگری مهاجمان ارائه میکند.

نکات مهم بدست آمده درباره مرورگرها

۱. بیش از نیمی از مروگرها در محیط سازمانی به غلط پیکربندی شده‌اند. درحالی که تهدید مرورگر پیکربندی‌شده تقریباً غیرممکن است، سرقت داده از مرورگرهایی که به اشتباه پیکربندی شده‌اند مانند گرفتن شکلات از یک نوزاد است. رایج‌ترین پیکربندی‌های نادرست شامل استفاده‌ی نادرست از پروفایل‌های مرورگر شخصی روی دستگاه‌های کاری (۲۹%)، روتین Patching ضعیف (۵۰%) و استفاده از پروفایل‌های مرورگر سازمانی روی دستگاه‌های مدیریت‌نشده است.
۲. از هر ۱۰ برنامه کاربردی SaaS سه مورد Shadow SaaS غیرسازمانی هستند و هیچ راهکار شناسایی/امنیت SaaS نمی‌تواند خطرات آن را مرتفع کند. Shadow Saas و مهم‌تر از آن، هویت‌های Shadow، منبع اصلی از دست دادن داده در سازمان هستند. درحال‌حاضر هیچ ابزار امنیت داده‌ای (چه یک DLP مرسوم باشد چه DSPM) به آنچه کارمندان روی برنامه‌های کاربردی شخصی خود انجام می‌دهند دسترسی یا کنترل ندارد.
۳. مهاجمان از تکنیک‌های حمله‌ی مخفی استفاده می‌کنند که نه امنیت ایمیل و نه ابزارهای امنیت شبکه نمی‌توانند آن‌ها را شناسایی کنند. تکنیک‌های حمله‌ی پیشرفته از طریق مرورگر، همچون استفاده از برنامه‌های کاربردی SaaS جهت توزیع بدافزار یا سوءاستفاده از سایت‌های معروف برای فیشینگ، به تهدیدی رایج تبدیل شده‌اند.
۴. ابزارهای امنیتی رایج بیش از نیمی از مسیرهای حمله را در Zero Hour شناسایی نمی‌کنند که باعث می‌شود حملات مرورگری هدفمند، یکی از دلایل اصلی نقض‌های امنیتی در سازمان‌ها باشند.
۵. اغلب خطرات مرورگری می‌توانند منجر به جعل هویت شوند. رمز عبورهای ضعیف، پیکربندی نادرست و مسائل امنیت SaaS همگی حول محور هویت دیجیتال هستند. این یافته‌ی ناامیدکننده یک دغدغه‌ی اصلی را مطرح می‌کند - اینکه هویت دیجیتال همچنان پاشنه‌ی آشیل سازمان‌ها است.
یافته‌های این گزارش به‌وضوح نشان می‌دهد که مرورگرها اصلی‌ترین نقطه کور امینت سایبری هستند و حفاظت دربرابر خطراتی که مرورگرها برای محیط IT سازمانی ایجاد می‌کنند فراتر از توانایی تیم امنیتی است. ضعف‌های امنیتیِ نادیده گرفته‌شده که بسیار رایج هستند، در ترکیب با فعالیت‌های گسترده‌ی مهاجمان که این ضعف‌ها را هدف قرار می‌دهند، چالشی ایجاد می‌کند که ذینفعان امنیتی باید در برنامه‌ریزی و اجرای معماری امنیت سایبری خود در نظر داشته باشند.

فهرست مطالب

مقدمه

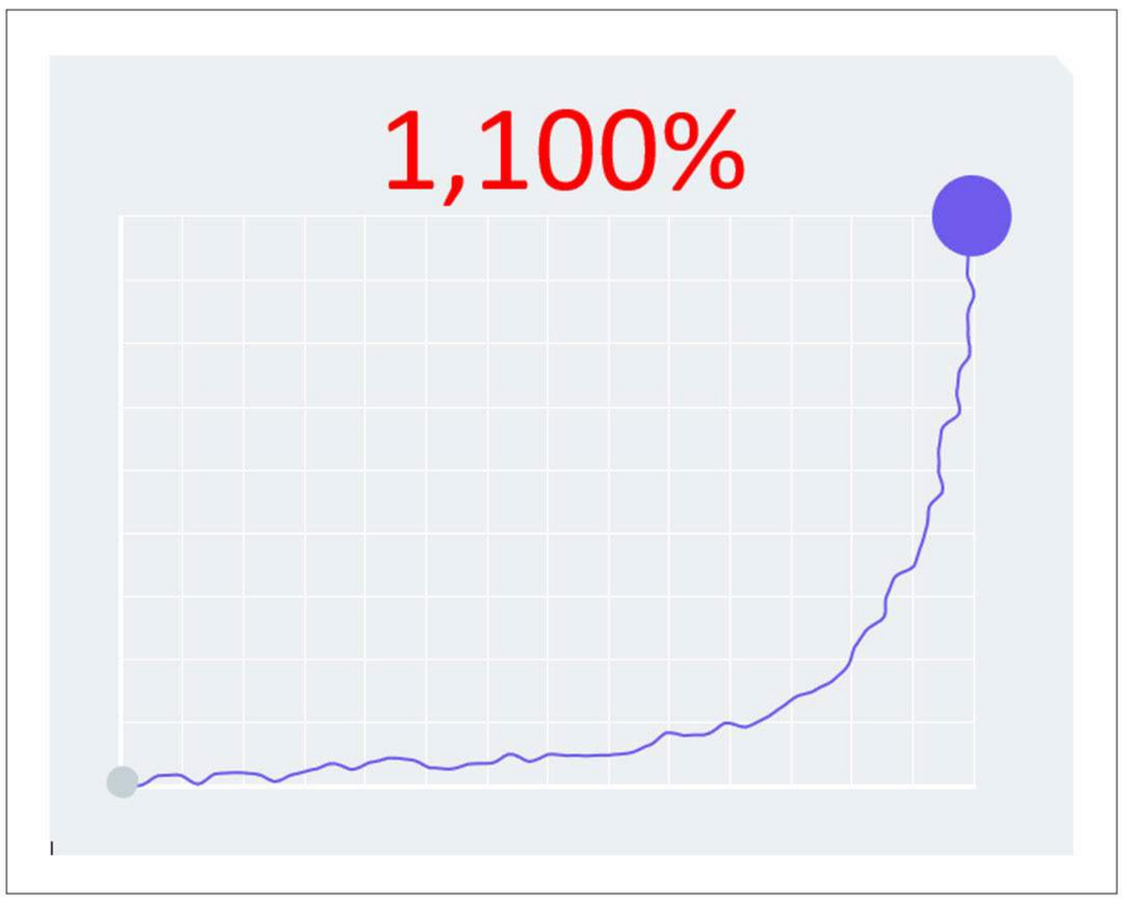
با تغییر مرورگرها، تهدیدهای مرتبط با مرورگر نیز تغییر کرده است.
عبارت «هیچ‌چیز بجز تغییر دائمی نیست» مهم‌ترین شاخصه‌ی امنیت سایبری را بیان می‌کند. یک استراتژی دفاعی مطمئن با تصدیق اینکه چشم‌انداز تهدید همواره درحال تغییر است آغاز می‌شود. چشم‌انداز تهدید مدام تکامل می‌یابد، به پیشرفت‌های دفاع موجود پاسخ می‌دهد و مدام مسیرهای حمله‌ی جدید و آسیب‌رسان ایجاد می‌کند.
گزارشی که در ادامه خواهید خواند اولین گزارشی است که به روبه‌رشدترین منبع تهدیدات در محیط سازمانی امروز، یعنی مرورگر می‌پردازد. مرورگر، خواه سطح حمله‌ای مستقل باشد و خواه مسیری برای دسترسی مخرب، در هسته‌ی حملات متعددی که امروزه سازمان‌ها را هدف می‌گیرند قرار دارد.
این موضوع نباید مایه‌ی تعجب باشد. این حقیقتی واضح است که اکنون مرورگر، رابط کاری کلیدی در محیط سازمانی مدرن است. با این حال، ما بر این باوریم که رهبران امنیتی هنوز هنگام طرح‌ریزی دفاع محیط خود، تمامی پیامدهای این حقیقت را تصدیق نمی‌کنند. آمارها و شکل‌های این گزارش حاکی از حقیقتی نگران‌کننده هستند. حقیقتی که ما را بر آن می‌دارد که صادقانه به این فکر کنیم که باید معماری پشته‌های امنیتی خود و تحلیل ریسک و اولویت بندی‌های بنیادین آن را مجدداً ارزیابی کنیم.
به‌علاوه، پرسشی ضروری‌تر پیش می‌آید. آیا ابزارهای امنیتی که تاکنون به کار رفته‌اند نیروی کافی برای مقاومت دربرابر چشم‌انداز تهدید مرورگر را برای محیط ما فراهم می‌کنند؟ اگر نه، باید به دنبال چه نوع حفاظتی باشیم؟
از این رو، ارزش حقیقی این گزارش به اعداد و ارقام ضمیمه شده یا آمارهای نقل‌شده نیست. بلکه ارزش آن به توانایی سوق دادن ما به‌سمتی است که از خودمان بپرسیم محیط‌مان دربرابر جهانی که این گزارش توصیف می‌کند، چگونه عمل می‌کنند. طبیعتاً پاسخها ممکن است بسیار متفاوت باشند. با وجود این تفاوت‌ها، نقشی که مرورگرها در سازمان‌های امروزی ایفا می‌کنند و همچنین حجم خطرات سایبری که در معرض آن قرار دارند، به‌شدت در حال تغییر است. ما باید این تغییر را تصدیق کرده و با آن سازگار شویم تا بتوانیم محیط‌های امنی برقرار کنیم.

تهدیدهای امنیتی مرورگر در سال ۲۰۲۲

در این گزارش، آمارها از تحلیل‌های ما درمورد ۵۰۰ کاربر تصادفی LayerX به دست آمده‌اند. هر آمار دیگری که در گزارش ذکر شده است بر اساس گستره‌ی وسیعی از گزارش‌های امنیت سایبری در دسترس عموم است.
تیم‌های امنیت سایبری به‌طور مداوم درحال رسیدگی به مجموعه‌ی پیچیده‌ای از تهدیدهای امنیتی هستند. موارد زیر، ۹ مورد از برجسته‌ترین تهدیدهای امنیت مرورگر در سال ۲۰۲۲ بوده‌اند.
۱. حملات فیشینگ از طریق دامین‌های مشهور
۲. توزیع بدافزار از طریق سیستم‌های اشتراک‌گذاری فایل
۳. نشت داده از طریق پروفایل‌های شخصی مرورگر
۴. مرورگرهای قدیمی
۵. رمز عبورهای آسیب‌پذیر
۶. دستگاه‌های مدیریت‌نشده
۷. افزونه‌های پرخطر
۸. Shadow SaaS
۹. دور زدن MFA در حملات AiTM

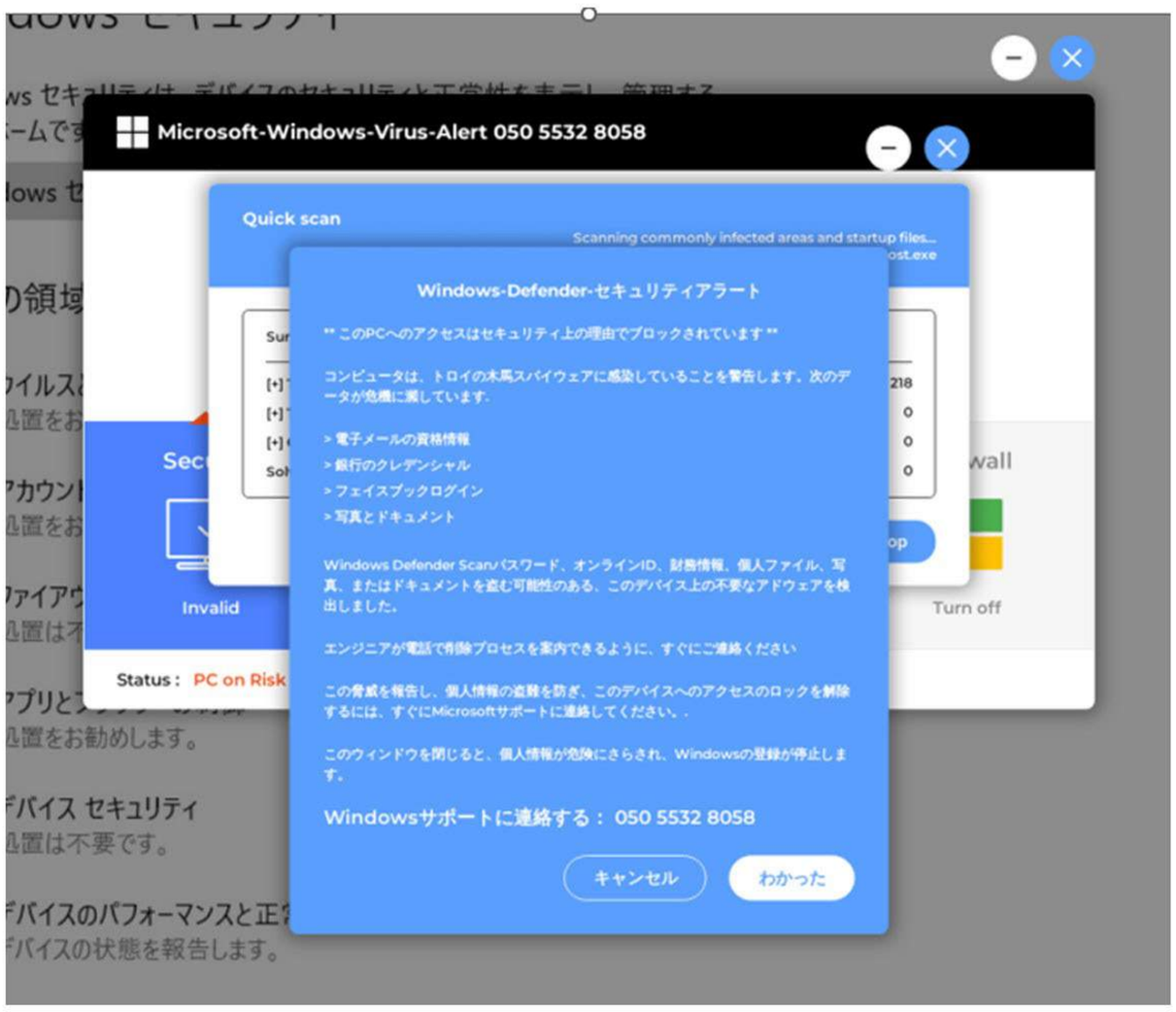
۱- حملات فیشینگ از طریق دامین‌های مشهور

حملات فیشینگ باعث می‌شوند وبسایت‌ها به‌صورت منابعی معتبر ظاهر شوند، درحالی که در واقع حاوی بدافزار یا سایر انواع کدهای مخرب هستند؛ و بدین صورت وبسایت‌ها به سلاح تبدیل می‌شوند. بسیاری از شرکت‌های ارائه‌دهنده‌ی امنیت به‌منظور تعدیل خطرات فیشینگ، وبسایت‌ها را با تعیین میزان امنیت URL فیلتر می‌کنند. این بررسی امنیت وبسایت بر اساس شهرت دامین است که بر اساس معیارهای متفاوتی همچون سن، تاریخچه‌ی URL، شهرت IP، محبوبیت وبسایت و غیره محاسبه می‌شود. اگر یک وبسایت شهرتی معتبر داشته باشد در این بررسی تأیید می‌شود.
اخیراً شواهد فزاینده‌ای مبنی بردور زدن این سازوکارهای امنیتی توسط کمپین‌های فیشینگ از طریق سرقت شهرت مشاهده شده است. این‌ها حملاتی هستند که ارائه‌دهندگان فیلترینگ URL را با میزبانی فیشینگ روی دامین‌های معتبر و قابل اطمینان، مانند GitHub، AWS، Microsoft، Google و غیره، گمراه می‌کنند. شهرت و اعتبار این دامین‌ها باعث می‌شود حملات موفقیت‌آمیز باشند و به سادگی فیلترهای Reputation را دور بزنند.
بر اساس پژوهشی که توسط واحد ۴۲ شرکت Palo Alto Networks انجام شد، از ژوئن ۲۰۲۱ تا ژوئن ۲۰۲۲، تعداد URLهای فیشنگی که روی پلتفرم‌های SaaS معتبر قرار گرفتند بیش از ۱۱۰۰% افزایش داشته است.



افزایش ۱۱۰۰درصدی URLهای فیشینگ

تصویـر زیـر نمونـه‌ای از یـک وبسـایت فیشـینگ اسـت کـه روی یـک دامیـن تحـت مالکیـت مایکروسـافت، یعنی bmtdfbwddf.blob.core.windows.net قرار گرفته است:

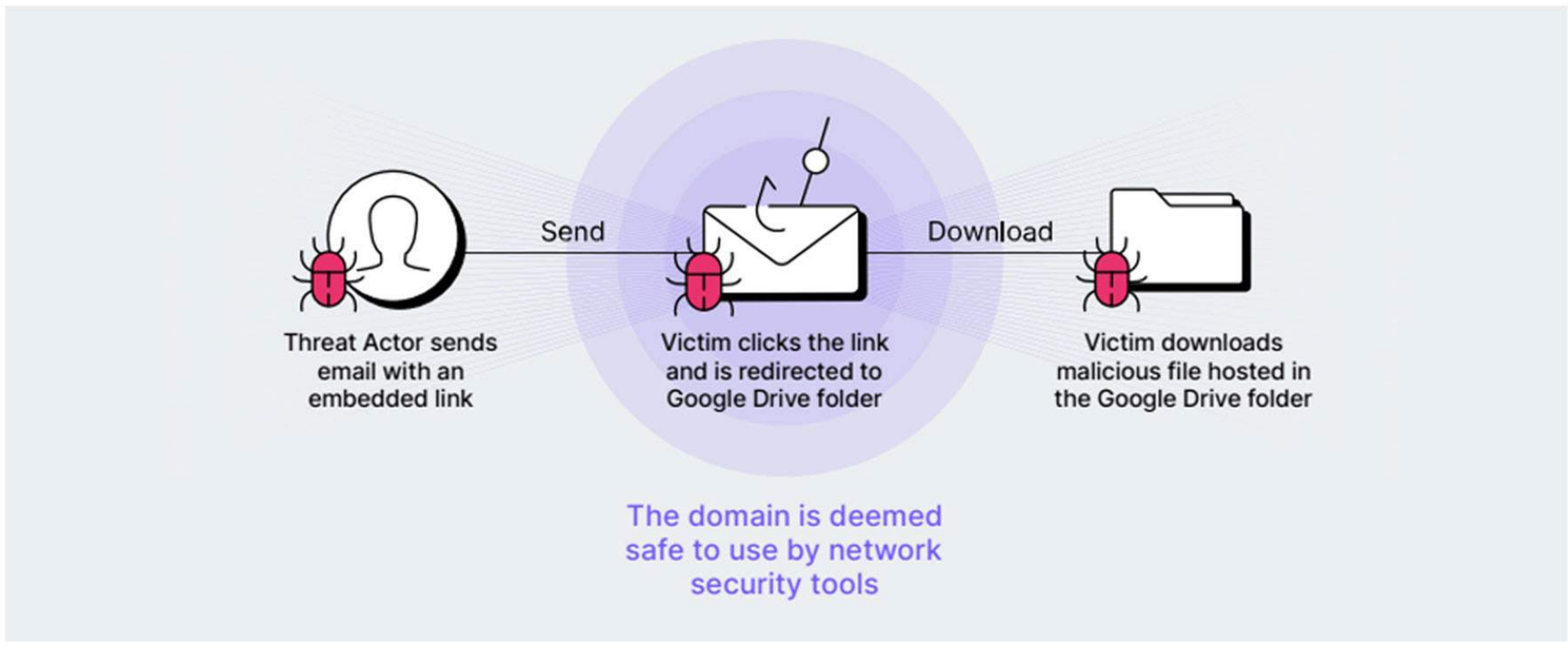


در آزمایـش اجـرا شـده، توانایـی مرورگرهـای تجـاری و ابزارهـای امنیـت شـبکه در شناسـایی سـایت‌های 1-Day Phishing (کـه پیـش از ایـن توسـط دسـت کـم یـک ارائه‌کننـده‌ی امنیـت شناسـایی شـده بودنـد) که روی دامین‌های مشهور قرار گرفته بودند، آزموده شد. ما دریافتیم که:

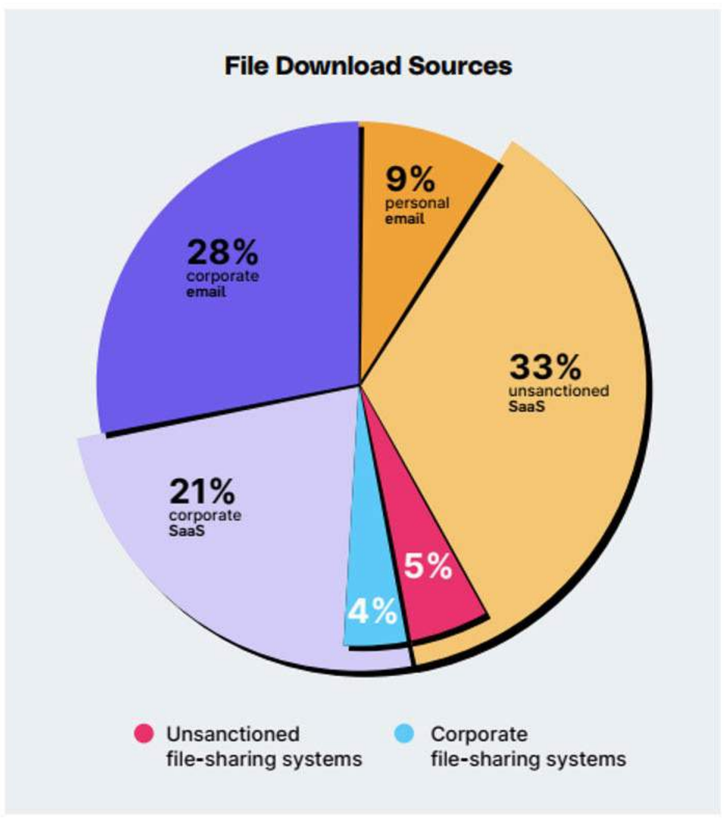
- نرخ شکار مرورگری که بهترین عملکرد را داشت ۳۶% بود که یعنی حدود دو سوم حملات از آن رد شدند.
- نـرخ شـکار راهـکار امنیـت شـبکه‌ای کـه بهتریـن عملکـرد را داشـت ۴۸% بـود کـه یعنـی بیـش از نیمـی از حملات از آن رد شدند.

۲.توزیع بدافزار از طریق سیستم‌های اشتراک‌گذاری فایل

پلتفرم‌های اشتراگذاری فایل P۲P (Peer-to-peer) می‌توانند برای توزیع بدافزار به کار روند. در این نوع حملات، عاملان تهدید محتوای مخرب را روی سایت‌های اشتراک‌گذاری فایل مورد اعتماد قرار می‌دهند تا به دستگاه‌های کاربران دسترسی پیدا کرده و بدافزار پخش کنند.
برای مثال، هکرهای چینی لینک‌های کارگذاری‌شده‌ای به فولدرهای Google Drive و Dropbox فرستادند که حاوی بدافزار بودند. این سایت‌ها شهرت خوبی دارند که باعث شد برای دورزدن سازوکارهای امنیتی مناسب باشند. این امر کار ابزارهای امنیت شبکه را به‌شدت سخت می‌کند، چراکه ممکن است نتوانند فایل‌های مخرب را شناسایی کنند چون روی وبسایت‌های اشتراک‌گذاری فایل معتبری ذخیره شده‌اند.



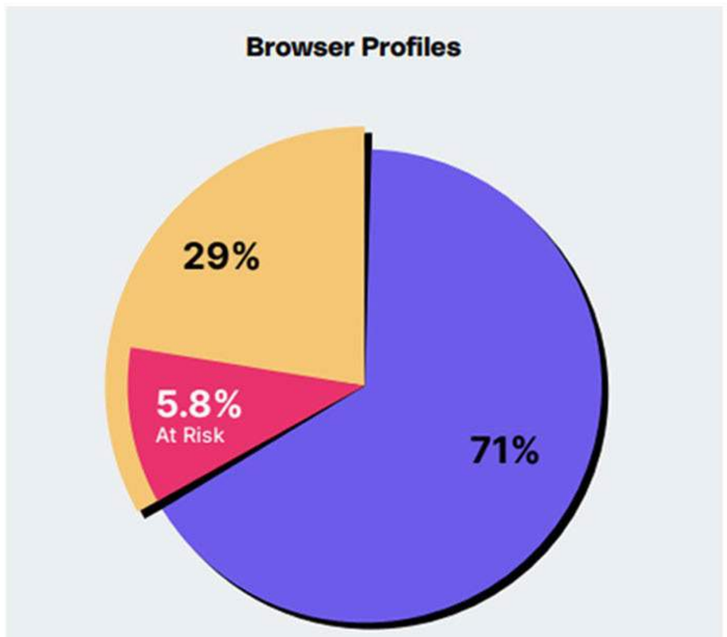
در واقع، فایل‌های بدافزار می‌توانند از طریق سیستم‌های اشتراک‌گذاری فایل مجاز و غیرمجاز توزیع شوند. این یعنی بدافزارها می‌توانند روی برنامه‌های پرکاربردی معتبری مانند Google Drive یا Microsoft OneDrive که موردتأیید IT هستند، قرار گیرند. ما با تحلیل فایل‌های دانلودشده‌ی کاربران تصادفی دریافتیم که حدود ۹% از فایل‌ها، از سیستم‌های اشتراک‌گذاری فایل دانلود شده‌اند. این دانلودها به نسبت تقریباً برابری از سیستم‌های اشتراک‌گذاری شرکتی (۵%) و غیرمجاز (۴%) بودند.



۳. نشت داده از طریق پروفایل‌های شخصی مرورگر

استفاده از پروفایل شخصی در محیط کاری می‌تواند به چندین ریسک امنیتی بیانجامد:

- مرورگر Chrome رمز عبورها را از وبسایت‌ها و برنامه‌های کاربردی همگام‌سازی می‌کند که می‌تواند تصادفاً باعث شود رمز عبورهای حساس شرکتی در دستگاه‌های شخصی همگام‌سازی شوند.
- آپلود فایل در Cloud شخصی و سیستم‌های اشتراک‌گذاری فایل، خطر جدی از دست دادن داده را ایجاد می‌کند چراکه می‌تواند داده‌های حساس شرکتی را در معرض خطر قرار دهد.
- استفاده از برنامه‌های کاربردی شرکتی با پروفایل‌های شخصی می‌تواند منجر به نشت داده‌های شرکتی شود چرا که خطر اشتراک‌گذاری اتفاقی یا عمدی داده در خارج از شرکت را افزایش می‌دهد.

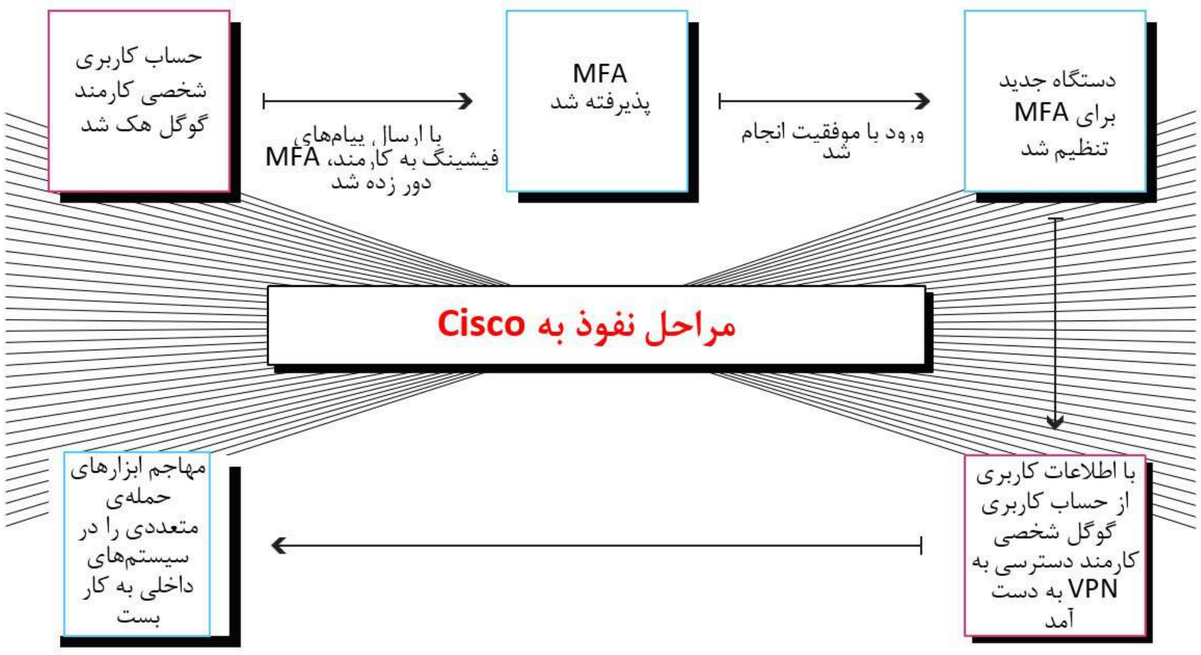


تحلیلی که روی ۵۰۰ مرورگر تصادفی انجام شد نشان داد که:

- ۲۹ % از مرورگرها به پروفایل‌های شخصی متصل هستند.
- ۵.۸ % از هویت‌های مرتبط به پروفایل مرورگرهای بررسی شده در معرض نقض امنیتی داده قرار گرفته بودند که باعث می‌شود اطلاعات اعتباری مربوط به این هویت‌ها، در معرض خطر قرار گیرند.

مثال: حمله سایبری Cisco

- اطلاعات اعتباری یکی از کارکنان Cisco با دسترسی مهاجمان به حساب کاربری گوگل شخصی او، مورد تهدید واقع شد.
- این کارمند همگام‌سازی رمز عبورها را فعال کرده و اطلاعات اعتباری Cisco خود را روی مرورگر Google Chrome شخصی خود ذخیره کرده بود.
- سپس مهاجمان به این کارمند پیام‌های فیشینگ ارسال کردند تا از کنترل امنیتی MFA عبور کنند.
- پس از دور زدن سازوکارهای MFA، مهاجمان با اطلاعات اعتباری اضافه‌ای که در پروفایل مرورگر شخصی کارمند یافته بودند، به VPN شرکت Cisco متصل شدند.
- در نهایت، آن‌ها به سیستم داخلی شرکت دسترسی پیدا کردند.



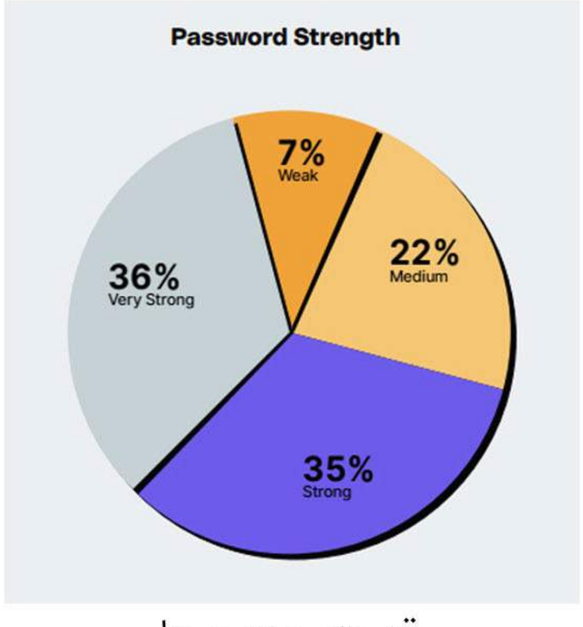
۴. مرورگرهای قدیمی

آپدیت‌های جدید مرورگرها حاوی Patchها یا راه حل‌های امنیتی ضروری هستند که معمولاً به آسیب‌پذیری‌ها و CVEهایی که اخیراً شناسایی شده‌اند، مربوط هستند. زمانی که CVE مهمی در محیط شناسایی شود، Chrome نسخه‌ی جدیدی با آپدیت امنیتی مربوطه منتشر می‌کند.
زمان Patching مهم است. با اینکه ایجاد آسیب‌پذیری‌های بحرانی Zero-day در Chromium برای مهاجمان تا میلیون‌ها دلار هزینه دارد، زمانی که 1-days شوند هزینه‌ی بهره‌برداری از آن‌ها به طرز چشمگیری کاهش می‌یابد. با گذشت چند ماه، شرح فنی آسیب‌پذیری فاش و استفاده از آن به کالایی ارزان برای استفاده‌ی مهاجمان سایبری تبدیل می‌شود. مروگرهای Patch نشده نسبت به این حملات آسیب‌پذیر هستند. از این رو هرچه سریع‌تر مرورگر به‌روزرسانی شود خطر کمتری متوجه آن است.
ما داده‌های ۵۰۰ مرورگر را تحلیل کردیم و دریافتیم که تعداد زیادی از مرورگرهای کاربران منسوخ و نسبت به CVEهای شناخته‌شده آسیب‌پذیر هستند.

نسخه‌های مرورگر Chrome میان ۵۰۰ کاربر، دسامبر ۲۰۲۲

۵. رمز عبورهای آسیب‌پذیر

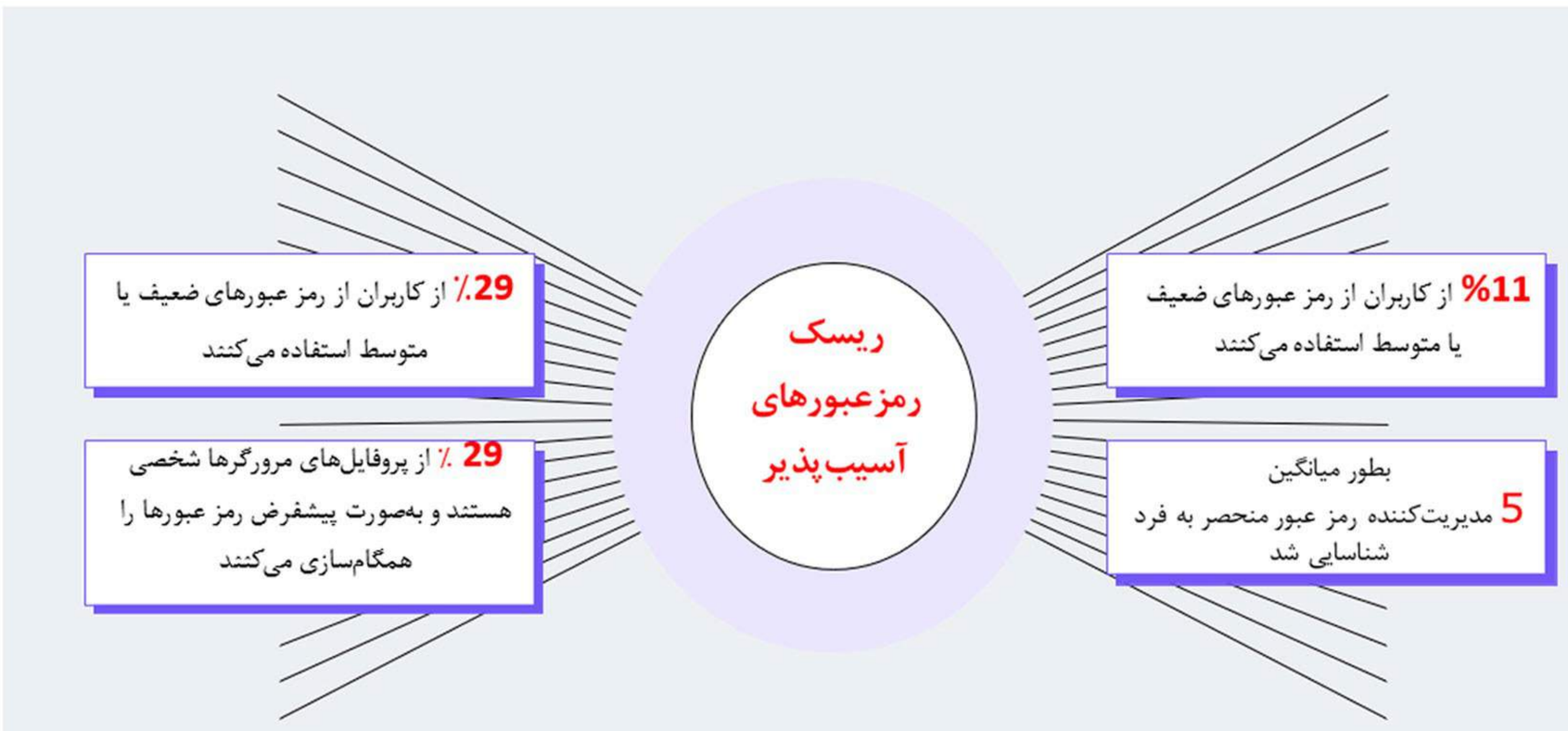
رمز عبورهای ضعیف و رمز عبورهای تکراری همچنان از عوامل اصلی نقض امنیتی داده‌ها هستند. حدود ۷۰% از نقض‌های امنیتی موفق شامل استفاده از اطلاعات اعتباری گم‌شده یا دزدیده‌شده، حملات Brute Force یا استفاده از رمز عبورهای تکراری روی وبسایت‌های متفاوت هستند.
به‌علاوه، استفاده‌ی گسترده از پروفایل‌های شخصی Chrome منجر به همگام‌سازی رمز عبور روی دستگاه‌ها می‌شود. این امر سطح حمله‌ی بالقوه و خطر دسترسی عاملان مخرب به رمز عبورها را افزایش می‌دهد. خطر امنیتی مهم دیگری که شرکت‌ها در خصوص رمز عبور با آن مواجه هستند، از سوی سیستم‌های مدیریت رمز عبور غیرمجاز ایجاد می‌شود که رمز عبور کارکنان را بدون نظارت یا تأیید IT کنترل می‌کند و ممکن است توسط هکرها نقض شود. سپس ممکن است رمز عبورها به اشخاص ثالث فروخته شوند.



قدرت رمزعبورها

تحلیلی انجام شده بر روی ۵۰۰ مرورگر تصادفی نشان داد که:

- ۲۹ % از کاربران از رمز عبورهای ضعیف یا متوسط استفاده می‌کنند.
- ۱۱ % از کاربران مرتباً از رمز عبورهای تکراری استفاده می‌کنند.
- ۲۹ % از پروفایل‌های مرورگرها شخصی هستند و به‌صورت پیشفرض رمز عبورها را همگام‌سازی می‌کنند.
- میانگین ۵ مدیریت‌کننده‌ی رمز عبور منحصربه‌فرد شناسایی شد.



۶. دستگاه‌های مدیریت‌نشده

درحالی که دورکاری در سرتاسر جهان گسترش یافته است، کارکنان از دسکتاپ‌ها، لپ‌تاپ‌ها، سرورها، تبلت‌ها و موبایل‌های شخصی برای کار استفاده می‌کنند. این دستگاه‌های غیرمجاز از طریق منابع سازمانی مانند شبکه‌های داخلی شرکت، برنامه‌های کاربردی SaaS، فایل‌های حساس و نرم‌افزارها به داده‌های حساس شرکتی متصل می‌شوند.
این دستگاه‌های مدیریت‌نشده تحت نظارت یا مورد شناسایی دپارتمان IT نیستند و در نتیجه فاقد حفاظت امنیتی مناسبی هستند که دستگاه‌های مدیریت‌شده دارند. این باعث می‌شود این دستگاه‌ها Gateway آسانی برای حملات سایبری به شبکه‌ی سازمانی باشند. یک دستگاه مدیریت نشده‌ی درمعرض خطر می‌تواند منجر به دسترسی مکرر به برنامه‌های کاربردی SaaS و حملات جعل هویت جدی شود.
Forrester در یک نظرسنجی دریافت که ۶۹% از پاسخ‌دهندگان مدعی شدند نیمی از دستگاه‌ها یا حتی بیشتر، مدیریت‌شده نبوده‌اند.

معیار	دستگاه‌های مدیریت‌شده	دستگاه‌های مدیریت‌نشده
ابزارهای امنیت شرکتی (EDR، امنیت شبکه)	✔	✘
قابلیت دید و مدیریت دستگاه TI	✔	✘
سیاست‌های DLP	✔	✘
سیستم عامل و مرورگر به‌روزرسانی‌شده	✔	✘
دسترسی مجاز به داده‌های شرکت	✔	✘
ورودهای SSO	✔	✔

دستگاه‌های مدیریت‌نشده خطر امنیتی برای سازمان‌ها ایجاد می‌کنند.

۷. افزونه‌های پرخطر

افزونه‌های مرورگرها مسیر حمله‌ی مطلوبی هستند، چراکه وقتی روی مرورگر نصب شوند می‌توانند سطوح دسترسی بیش از حدی اعطا کنند. در مطالعه‌ای که اخیراً روی افزونه‌های Chrome با دست کم ۱۰۰۰ دانلود انجام شد، محققان Incogni دریافتند که حدود نیمی (۴۸.۶%) از آن‌ها به‌طور بالقوه خطر امنیتی یا حریم خصوصی جدی ایجاد می‌کنند. این افزونه‌ها سطوح دسترسی‌ای کسب می‌کنند که آن‌ها را قادر به جمع‌آوری اطلاعات قابل شناسایی شخصی (PII)، پخش کردن آگهی‌افزار و بدافزار، و دسترسی به رمز عبورها و داده‌های مالی می‌سازد.
از میان افزونه‌های خطرناک بالقوه، تعداد اندکی از آن‌ها آشکارا مخرب هستند. افزونه‌های مخرب می‌توانند به روش‌های گوناگونی نصب شوند و معمولاً مخفی هستند تا کاربران را فریب دهند.

مثال: Vipersoft

- Vipersoft از طریق بازی‌های کرک شده و فایل‌های exe. قابل دانلود، بدافزار پخش می‌کند.
- سپس بدافزار افزونه‌ی مخربی به نام Venomsoft روی مرورگرهای مبتنی بر Chrome نصب می‌کند.
- این افزونه رمز عبورها و رمزارزهای کاربر را سرقت می‌کند.
- افزونه تلاش می‌کند خود را به‌عنوان افزونه‌ی شناخته‌شده و رایجی مانند Google Sheet نشان دهد.

میزان خطر: حیاتی

تحلیلی انجام شده روی ۵۰۰ مرورگر تصادفی، چندین مثال از افزونه‌های مشکل‌ساز را آشکار کرد.

8

افزونه از Chrome Store حذف شدند

افزونه‌های حذف شده از Chrome Store استانداردهای حریم خصوصی یا امنیتی گوگل را نقض می‌کردند.

3

افزونه مخرب

٪38

از افزونه‌ها Permissionهای بیش از حد می‌دهند.

11

افزونه‌ی غیر سازگار

افزونه‌هایی که با سیاست‌های امنیتی یا حریم خصوصی شرکت سازگاری ندارند.

66

افزونه‌ی کم‌شهرت

۸. Shadow SaaS

Shadow SaaS به استفاده از برنامه‌های کاربردی Software as a Service تأییدنشده در سازمان گفته می‌شود. این برنامه‌های کاربردی ممکن است توسط کارکنان برای امور مربوط به کار استفاده شوند اما رسماً توسط دپارتمان IT شرکت تأیید یا تصدیق نشده‌اند.
Shadow SaaS چندین خطر امنیتی دارد. اول، این برنامه‌ها الزامات امنیتی برنامه‌های مورد تأیید IT را ندارند. این امر می‌تواند خطر از دست دادن داده‌ها یا آلوده شدن به بدافزار را افزایش دهد. به‌علاوه، برنامه‌های Shadow SaaS در سیستم‌های امنیتی و مدیریتی شرکت ادغام نشده‌اند که باعث می‌شود مانیتور کردن استفاده از آن‌ها دشوار باشد. در نهایت، استفاده از برنامه‌های Shadow SaaS توانایی شرکت برای پیروی از دستورالعمل‌های داده و حریم خصوصی را کاهش می‌دهد. آپلود کردن داده‌های حساس شرکت روی برنامه‌های تأییدنشده دستورالعمل‌ها را نقض می‌کند، ممکن است اطلاعات شخصی را در معرض خطر قرار دهد و می‌تواند به جریمه شدن و رویه‌های قانونی بیانجامد.

٪31

از برنامه‌های مورداستفاده‌ی کارکنان به هویت‌های غیرسازمانی متصل هستند

٪67

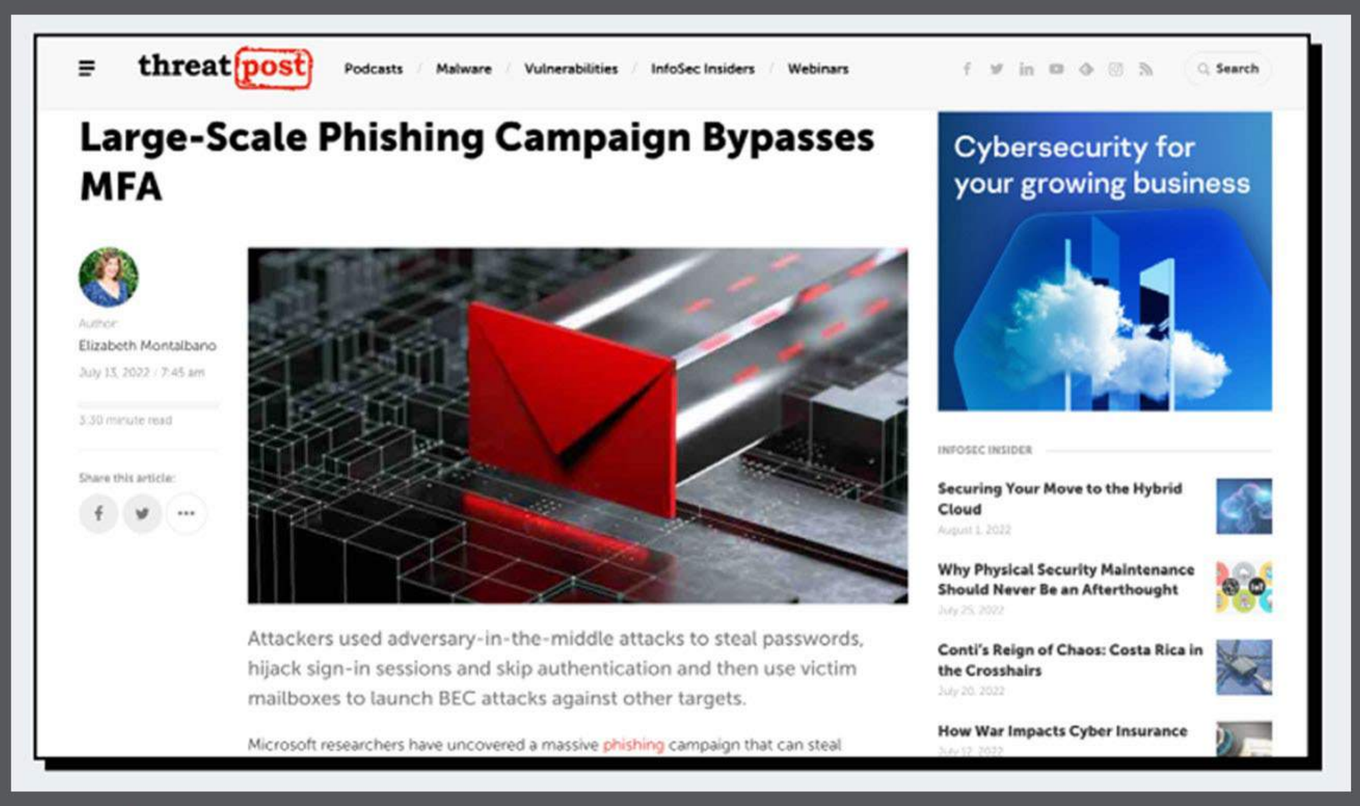
از کاربران ابزارهای مشارکت خود را وارد سازمان‌هایشان کرده‌اند

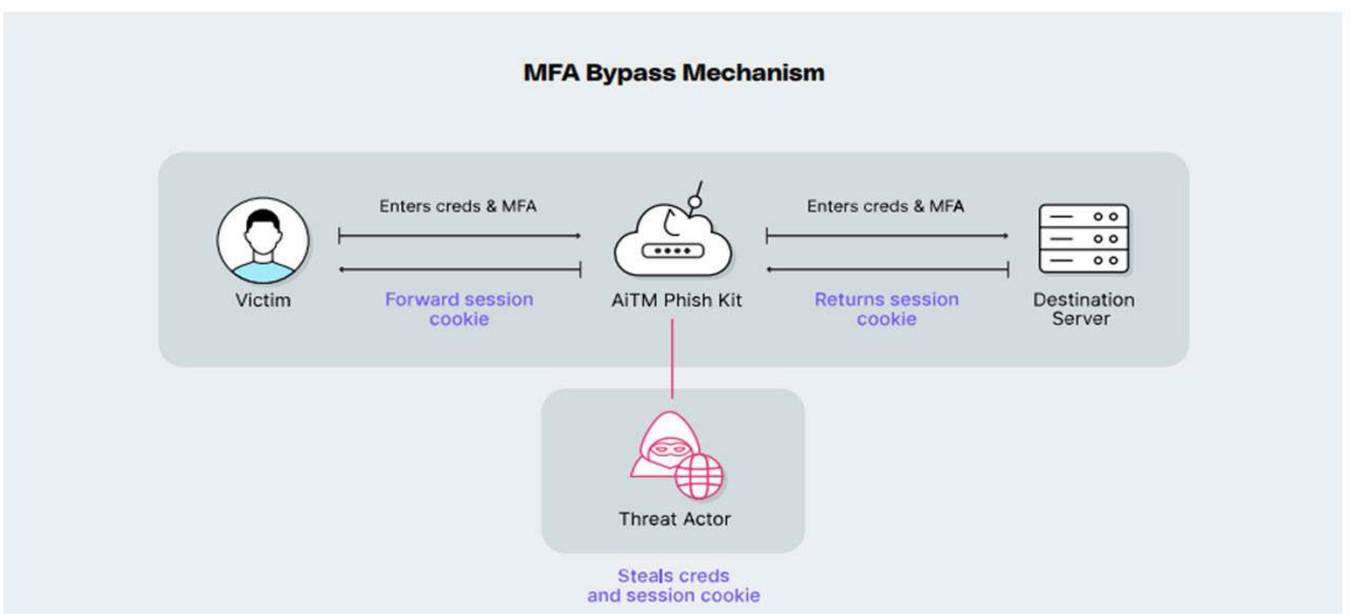
٪70

از سازمان‌ها برنامه‌های کاربردی روی Cloud اجرا می‌کنند که مورد تأیید رسمی دپارتمان‌های IT نیستند

۹. دور زدن MFA در حملات AiTM

فیشینگ اطلاعات اعتباری، مثلاً دزدیدن ورود به سیستم و رمز عبورهای کاربر یا فریب دادن آن‌ها به منظور ارائه‌ی این موارد، مدت‌هاست که توسط هکرها انجام می‌شود. با معرفی MFA (احراز هویت چندمرحله‌ای) و به‌دلیل صحت‌سنجی اضافه‌ای که کاربر باید به منظور ورود ارائه کند، این کار برای مهاجمان دشوارتر شده است.
مهاجمان برای مقابله با این مشکل از حمله‌های Real-Time علیه سیستم‌های تحت حفاظت MFA به‌صورت Adversary in the Middle (AiTM) استفاده می‌کنند. رویکرد AiTM مهاجم را در میانه‌ی فرایند احراز هویت، میان کلاینت و سرور قرار می‌دهد تا تبادل را قطع کرده و اطلاعات اعتباری را به سرقت ببرد. قطع کردن اطلاعات احراز هویت MFA به مهاجم اجازه می‌دهد MFA را دور بزند و به داده‌های حساس دسترسی پیدا کند. گزارش اخیر Okta، افزایش چشمگیر حملات دور زدن MFA طی دو سال اخیر را نشان می‌دهد.





مکانیزم دور زدن MFA

نکات برجسته‌ی سالانه‌ی امنیت مرورگر

در زیر به اخبار مهمی پرداختیم که در سال ۲۰۲۲ در دنیای امنیت مرورگر اثری به جا گذاشتند.

ژانویه: هکرها از پخش‌کننده ویدئو برای دزدیدن کارت‌های اعتباری از بیش از ۱۰۰ سایت استفاده کردند
هکرها از یک سرویس Cloud ویدئویی استفاده کردند که برای دزدیدن اطلاعات وارد شده در فرم‌های وبسایت اسکریپت‌های مخربی وارد آن می‌کرد. این اسکریپت‌ها که به Form jacker شهرت دارند، اطلاعات پرداخت حساس وارد شده در فرم‌های وبسایت‌های هک شده را سرقت می‌کنند.

فوریه: گوگل اولین هک Zero-Day مرورگر Chrome در سال ۲۰۲۲ را تأیید کرد
گوگل آپدیتی برای رسیدگی به CVE-۲۰۲۲-۰۶۰۹ منتشر کرد که یک آسیب‌پذیری use-after-free با قابلیت اجرای کدی دلخواه روی سیستم تحت‌تأثیر توصیف شده است.

مارس: حمله‌ی Browser in the Browser در محیط یافت شد
یک تکنیک فیشینگ با عنوان Browser in the Browser (BITB) پدیدار شده است که شامل شبیه‌سازی پنجره مرورگری درون مرورگر به‌منظور جعل کردن دامین قانونی است. این تکنیک به مسیر حمله‌ی خطرناکی موردپسند مجرمان سایبری تبدیل شده است.

آوریل: آپدیت اورژانسی Chrome برای رفع RCE Zero-Day
گوگل آپدیتی برای Chrome منتشر کرده است که باگ آسیب‌پذیری Zero-Day حیاتی CVE-۲۰۲۲-۱۳۶۴ را رفع می‌کند. این آسیب‌پذیری اجرای از راه دور کد را به‌دلیل ضعف اختلالی از نوع V۸ ممکن می‌سازد.

می: غول‌های تکنولوژی حمایت خود را از ورود بدون رمز عبور اعلام کردند
مایکروسافت، اپل و گوگل از برنامه‌ای برای حمایت از یک استاندارد ورود بدون رمز عبور (که با عنوان passkey شناخته می‌شوند) رونمایی کردند. این به کاربران غول‌های تکنولوژی اجازه می‌دهد بدون استفاده از رمز عبور وارد حساب کاربری خود شوند.

ژوئن: پایان Internet Explorer
برنامه کاربردی دسکتاپ Internet Explorer با رسیدن به پایان عمر خود، غیرفعال خواهد شد و Microsoft Edge مبتنی بر Chromium جایگزین آن خواهد شد.

ژوئیه: کمپین گسترده‌ی AiTM Phishing
مایکروسافت یک کمپین فیشینگ گسترده کشف کرد که بیش از ۱۰ هزار سازمان را هدف قرار داده بود. این کمپین از Adversary-in-the-middle استفاده کرده و قادر به دور زدن MFA است.

آگوست: پنجمین آسیب‌پذیری Zero-Day
در ماه آگوست پنجمین آسیب‌پذیری Zero-day در Chrome که گوگل از ابتدای سال حل کرد، ثبت شد.

سپتامبر: نقض داده‌های Uber
Uber گزارش‌های مبنی بر نقض امنیت سایبری در سراسر سازمان را تأیید کرد. این نقض امنیتی با یک کمپین مهندسی اجتماعی روی کارکنانش آغاز شده بود که در آن هکر از اطلاعات اعتباری دزدی که آنلاین یافت میشد استفاده کرده و سپس با یک MFA prompt که کارمند را بیش از یک ساعت درگیر می‌کرد تا در نهایت به آن عمل کند، دسترسی پیدا می‌کرد.

اکتبر: نوع جدیدی از حمله‌ی فیشینگ
هکرها می‌توانند از App Mode در مرورگرهای Chromium برای حملات فیشینگ مخفیانه استفاده کنند.

نوامبر: افزونه‌ی مخرب Cloud۹
افزونه‌ی مخربی به مهاجمان امکان کنترل از راه دور Google Chrome را می‌دهد.

دسامبر: نقض داده‌ای مشتریان Lastpass
Lastpass برای دومین بار در سال تأیید کرد که هکرها به سرویس ذخیره اطلاعات Cloud شخص ثالثی دسترسی پیدا کرده‌اند که دربردارنده‌ی داده‌های شخصی مشتریان بود.

پیش‌بینی‌های حوزه امنیت مرورگر در سال ۲۰۲۳

افـراد حرفـه‌ای حـوزه‌ی امنیـت در سـال ۲۰۲۳ می‌تواننـد انتظـار چـه چیـزی در حـوزه‌ی امنیـت مرورگـر داشـته باشند؟ متخصصان ما پیش‌بینی‌های خود را به اشتراک گذاشتند:
۱. SaaS یـک دغدغـه‌ی نظـارت و امنیـت خواهـد بـود. افزایـش پیوسـته‌ی اسـتفاده از برنامـه کاربـردی SaaS ادامـه خواهـد داشـت. بـا رشـد محیـط SaaS مدیریـت آن دشـوارتر خواهـد شـد و نقـاط کـور، برنامه‌هـای کاربـردی Shadow و هویت‌هـا، دسـتگاه‌ها و منابـع مدیریت‌نشـده‌ی کارکنـان بیشـتر و بیشـتر خواهنـد شـد. حفـظ نظـارت بـر برنامه‌هـای SaaS کـه مـدام در حـال افزایـش هسـتند می‌توانـد بـرای دپارتمان‌هـای IT زمان‌بر و کلافه‌کننده باشد.

۲.حـملات هرچـه بیشـتر مبتنـی بـر SaaS و کمتـر مبتنـی بـر فایـل خواهنـد بـود. ازدیـاد اسـتفاده از برنامه‌هـای SaaS در محیـط سـازمانی بـه نوبـه‌ی خـود سـهم فایل‌هـای مرسـوم را در آن‌هـا کاهـش خواهـد داد. ایـن امـر در چشـم‌انداز تهدیـد نیـز انعـکاس می‌یابـد و حـملات بیشـتری از تکیـه بـر اجـرای فایـل بـه سـمت تمرکـز بـر دسترسـی مخـرب بـه SaaS و برنامه‌هـای کاربـردی تحـت وب حرکـت می‌کننـد. انتظـار می‌رود سهم حملات مبتنی بر وب و Cloud افزایش یابد.

۳. مرورگـر بـه سـطح حملـه‌ی اصلـی تبدیـل می‌شـود. جایـگاه منحصربه‌فـرد مرورگـر به‌عنـوان ابـزار پیـش فـرض بـرای اسـتفاده‌ی کاری و شـخصی، مهاجمـان بیشـتری را بـه سـمت تبدیـل کـردن اسـتفاده شـخصی از مرورگـر بـه مسـیر حملـه‌ای بـرای دسترسـی بـه منابـع کاری سـوق خواهـد داد. مهاجمـان تلاش خواهنـد کـرد بـا هـدف قـرار دادن مرورگرهـای شـخصی کارکنـان بـه داده‌هـای سـازمانی دسترسـی مخـرب پیـدا کننـد کـه بـه دلیـل کاربـرد دوگانـه‌ی مرورگـر اسـت. ایـن نیـز به‌نوبـه‌ی خـود تیم‌هـای امنیتـی را بـر آن مـی‌دارد کـه بـا تمام فعالیت‌های مروری به‌عنوان یک سطح حمله‌ی منفرد و یکپارچه برخورد کنند.

۴.صفحـات وب مخـرب پیچیده‌تـر خواهنـد شـد. تکامـل تکنولـوژی وب بـرای کاربـران تجربـه‌ی مـروری غنی‌تـر، پویاتـر و منعطف‌تـری بـه ارمغـان مـی‌آورد، امـا وجـه دیگـری نیـز دارد. ایـن امـر مهاجمـان را قـادر بـه پنهـان کـردن حـملات پیشـرفته در صفحـات وب می‌سـازد کـه می‌تواننـد از شناسـایی توسـط اقدامـات امنیتـی مرسـوم مصـون باشـند. ایـن پیچیدگـی رو بـه رشـد برنامه‌هـای کاربـردی تحـت وب نقـاط کـور امنیتی را افزایش خواهد داد.

توصیه‌هایی برای مدیران امنیت در سال ۲۰۲۳

مدیران امنیت آینده‌نگر باید نیاز به آگاهی امنیت مرورگر و کنترل در سازمان‌های خود را بررسی کنند. دراینجا توصیه‌هایی داریم که می‌توان بی‌درنگ به کار بست:

۱. قابلیت دید و کنترل همه‌جانبه نسبت به SaaS داشته باشید

توانایی یافتن و مانیتور کردن تمامی منابع و فعالیت‌ها بنیانی است که هر ساختار امنیتی مستحکمی باید روی آن بنا شود. ضروری است که تیم‌های امنیتی این دانش را در محیط SaaS اِعمال کنند. در حالتی عملی‌تر، پیش‌فرض هر راه‌حلی که مدعی تأمین امنیت محیط SaaS شما است، قابلیت دید بدون دردسر و جامع صرفنظر از مجاز یا غیرمجاز بودن برنامه - است.

۲. مرورگر را به اولین خط دفاعی تبدیل کنید

تنها راه مقابله با سطح حمله‌ی مرورگر که به‌سرعت درحال تکامل است، نصب قابلیت دید و حفاظت در برابر تهدید بی‌وقفه روی خود مرورگر است. مانیتورینگ، تحلیل خطر، و پاسخ فعال می‌تواند در هر رویداد مروری اِعمال شود. این اقدامات نه تنها مرورگر را به سطح حمله‌ای مدیریت شده و کنترل‌شده تبدیل می‌کند، بلکه آن را ستونی اصلی در معماری امنیتی سازمان نیز می‌کند.

۳. امنیت مبتنی بر هویت به کار ببندید

دسترسی مبتنی بر هویت به برنامه‌ها می‌تواند با استفاده از رمز عبورهای قوی و احراز هویت چندمرحله‌ای امنیت را بهبود بخشد. به‌علاوه، مدیریت هویت متمرکز و ردیابی دسترسی کاربران به سیستم‌ها و برنامه‌های کاربردی مختلف را برای سازمان‌ها آسان‌تر کرده و باعث اطمینان از دسترسی کاربران مورد تایید به داده‌های حساس می‌شود. این کار می‌تواند با ساده کردن فرایند اعطا و ابطال دسترسی به کاربران و فراهم کردن نقطه‌ی کنترلی منفرد برای مدیریت هویت کاربران، کارایی را افزایش دهد.

۴. تغییر شکل دیجیتالی را متوقف نکنید، به آن شتاب دهید

SaaS اینجاست که بماند و با رشد بیشتر، حوزه بهره‌وری را دگرگو نماید. از این تغییر استقبال کنید و در عین حال اطمینان حاصل کنید که می‌توانید امنیت آن را تضمین کنید. یکپارچگی تنها استراتژی امنیت سایبری است که منطقی به نظر می‌رسد. مکان اصلی که باید کنترل‌های امنیتی مربوط به SaaS را در آن یکپارچه سازید مرورگر است، چراکه تنها منبع دسترسی هردوی کاربران قانونی و عاملان تهدید است.

نتیجه‌گیری

این گزارش نقش کلیدی مرورگر در چشم‌انداز تهدید امروز را روشن می‌سازد. از آنجا که مرورگر به عنوان ابزار کاری و دروازه‌ی اصلی دسترسی به اینترنت به کار می‌رود، طبیعتاً به سطح حمله‌ی پرکاربردی برای خرابکاران تبدیل شده است. بااینکه هر ذینفع امنیتی احتمالاً تا حدی از این پدیده آگاه است، هدف این گزارش نشان دادن گستره‌ی حقیقی آن است که دیگر قابل نادیده گرفتن نیست.
بنابراین، کارآمدی گزارش بر اساس توانایی آن در واداشتن خوانندگان به پرسیدن پرسش‌های سازنده‌ی زیر از خودشان سنجیده می‌شود:

- من در محیط خود با کدام یک از خطرات و روندهای تشریح شده در این گزارش آشنا هستم؟
- آیا اقدامات حفاظتی لازم برای شناسایی و جلوگیری از این تهدیدات را در اختیار دارم؟
- این اقدامات حفاظتی به اندازه کافی اثرگذار هستند؟

پاسخ دادن به این پرسش‌ها نشان خواهد داد که آیا برای رسیدن به حفاظتی که محیط‌تان نیاز دارد، نیازی به به‌روزرسانی استراتژی امنیتی خود دارید یا خیر.
ادامه‌ی تکیه بر راهکارهای مبتنی بر شبکه یا پروکسی ممکن است نتواند مانع از دسترسی نیروی کار شما به صفحات وب مخرب شود. همانطور که در بالا نشان دادیم، این راهکارهای برای شناسایی حملات فیشینگ از طریق دامین‌های مشهور کافی نیستند. اما افزونه‌های مخرب و خطر بالقوه‌ی بزرگ شان چطور؟ متأسفانه، بسیاری از راهکارهای حفاظت از نقاط پایانی این موارد را پوشش نمی‌دهند. درواقع، وجه مشترک تمامی تهدیدهای تشریح شده در این گزارش پژوهشی این است که راهکارهای حفاظت مبتنی بر شبکه، نقطه پایانی یا Cloud به اندازه کافی آن‌ها را پوشش نمی‌دهند.

سخن پایانی

در راستای ایجاد بستری امن برای کاربران و جلوگیری از انتشار آلودگی در سطح شبکه و همچنین کاهش حملات از سمت کاربران شبکه پیشنهاد می‌گردد جداسازی اینترنت از اینترانت با جداسازی مرورگر در راستای پیاده‌سازی و بهبود زیرساخت سازمان‌ها قرار داده شود. شرکت امن‌پردازان کویر (APK) پیشرو در ارائه خدمات امنیت سایبری، محصول APKSWAP، سامانه دسترسی امن به اینترنت را با استفاده از فناوری جداسازی مرورگر و تکنولوژی Docker-Container ارائه نموده است. این راه‌حل نسبت به راهکارهای جداسازی فیزیکی از نظر هزینه‌های مالی، منابع انسانی، زیرساختی و همچنین توسعه‌ای مقرون به صرفه است.

جهت درخواست دمو کلیک کنید

منبع
layerxsecurity.com