خبرنامه الکترونیکی ۶۴

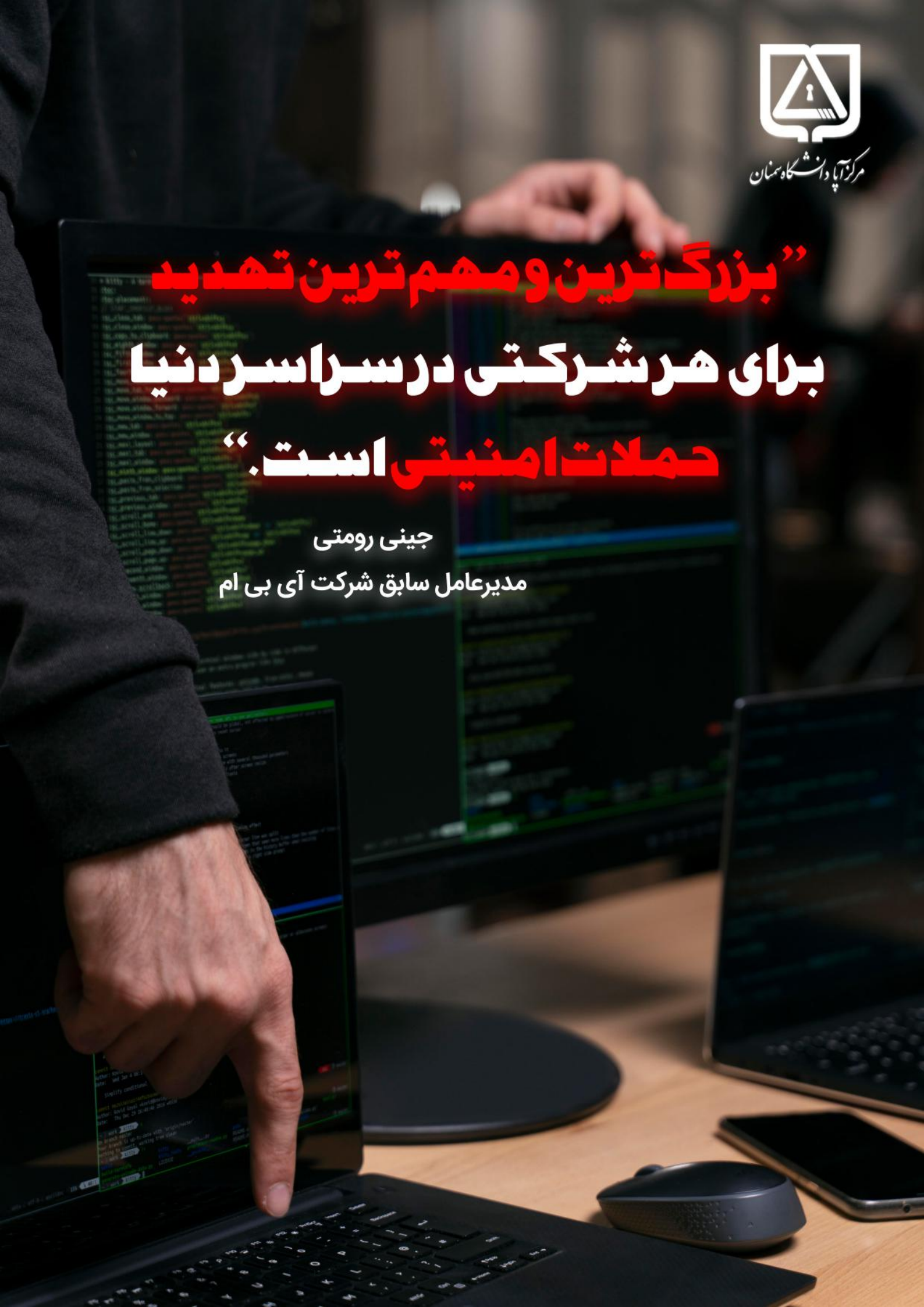
مرکز تخصصی آپا دانشگاه سمنان

شماره شصت و چهارم، سال ششم، مهر ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

مایکروسافت در حال ارائه پشتیبانی از Passkeys در ویندوز 11 است

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert


مرکز آپا دانشگاه سمنان
”بزرگ‌ترین و مهم‌ترین تهدید
برای هر شرکتی در سراسر دنیا
حملات امنیتی است.“
جینی رومتی
مدیرعامل سابق شرکت آی بی ام

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

خبر

مجرمان سایبری گواهی‌های فیشینگ و EV را برای ارائه Payloadهای باج‌افزار ترکیب می‌کنند

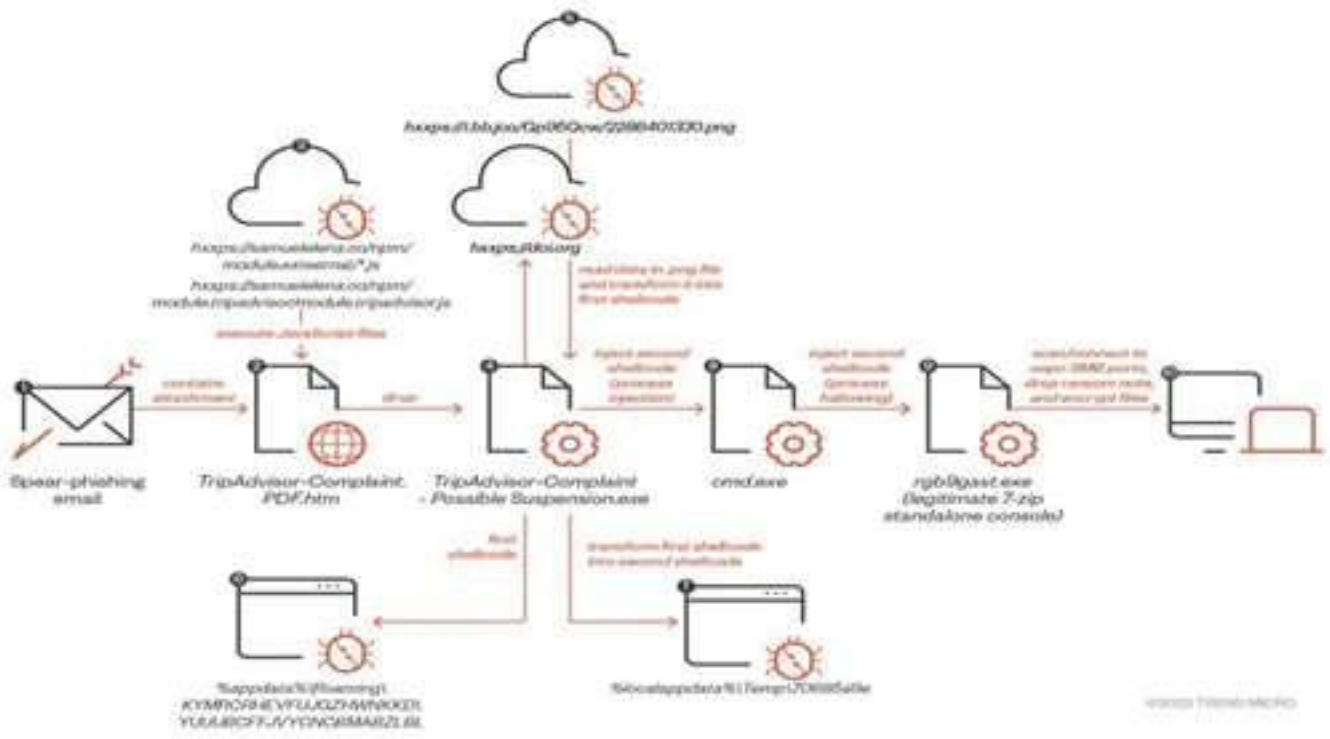
مشاهده شده است که عوامل تهدید RedLine و Vidar[1] به باج افزار روی آورده اند. در این کمپین‌ها، از فیشینگ برای توزیع محموله‌های اولیه استفاده می‌شود. این محموله‌ها با گواهی‌های سطح Extended Validation[2] امضا شده اند.

محققان Trend Micro در تحلیل جدیدی که این هفته منتشر شد، گفتند: «این نشان می‌دهد که تهدیدکنندگان با چند منظوره کردن تکنیک‌های خود عملیات را ساده می‌کنند».

در حادثه‌ای که توسط این شرکت امنیت سایبری مورد بررسی قرار گرفت، گفته می‌شود که قربانی ناشناس ابتدا یک بدافزار دزد اطلاعات را با گواهی امضای کد EV دریافت کرده است و به دنبال آن باج افزاری را با استفاده از همان تکنیک تحویل، دریافت کرده است. درگذشته، آلودگی‌های QakBot از نمونه‌های امضاشده با گواهی‌های امضای کد معتبر برای دور زدن حفاظت‌های امنیتی استفاده می‌کردند.

حملات با ایمیل‌های فیشینگ شروع می‌شوند که از فریب‌های رایج استفاده می‌کنند. آنها فایل‌های پیوست مخربی را با ظاهر تصاویر PDF یا JPG نشان می‌دهند اما درواقع فایل‌های اجرایی هستند که پس از اجرا، حمله را آغاز می‌کنند.

درحالی‌که این کمپین، بدافزار دزدی را در ماه ژوئیه به قربانی مذکور ارسال کرده بود، یک پیلود باج افزار در اوایل آگوست پس از آنکه قربانی یک پیام ایمیل حاوی یک پیوست شکایت جعلی تریپ ادوایزر (" TripAdvisor-Complaint.pdf.html") دریافت کرد، به سیستم او راه پیدا کرد. سپس این پیلود گام‌هایی را آغاز کرد که به استقرار باج افزار منتهی شد.



1- دو بدافزار سرقت اطلاعات

2- EV

محققان می‌گویند: «در این مرحله، برخلاف نمونه‌های دزد اطلاعاتی که ما بررسی کردیم، فایل‌هایی که برای رها کردن payload باج‌افزار استفاده می‌شوند، گواهی‌های EV نداشتند. با این حال، این دو از عامل تهدید یکسانی سرچشمه می‌گیرند و با استفاده از روش تحویل یکسانی پخش می‌شوند؛ بنابراین می‌توانیم تقسیم کار را بین ارائه‌دهنده payload و اپراتورها فرض کنیم.»

در عین حال، IBM X-Force کمپین‌های فیشینگ جدیدی را کشف کرده است که نسخه بهبودیافته‌ای از یک بارگذار بدافزار به نام DBatLoader را منتشر می‌کند که همین امسال به‌عنوان مجرایی برای توزیع FormBook و Remcos RAR استفاده می‌شد.

قابلیت‌های جدید DBatLoader دور زدن UAC، ماندگاری و تزریق فرایند را تسهیل می‌کند که نشان می‌دهد عاملان تهدید به طور فعال مشغول نگهداری آن هستند تا با استفاده از آن برنامه‌های مخربی که می‌توانند اطلاعات حساس را جمع‌آوری کرده و کنترل از راه دور سیستم‌ها را فعال کنند، ارسال کنند. مجموعه‌ای از حملات اخیر که از اواخر ژوئن شناسایی‌شده‌اند، به‌گونه‌ای طراحی‌شده‌اند که بدافزارهایی مانند Agent Tesla و Warzone RAT. A را نیز ارائه دهند. اکثر پیام‌های ایمیل انگلیسی زبان‌ها را هدف گرفته اند، اگرچه ایمیل‌هایی به زبان‌های اسپانیایی و ترکی نیز مشاهده شده‌اند. در چندین کمپین مشاهده شده، عوامل تهدید کنترل کافی بر زیرساخت ایمیل برای فعال کردن ایمیل‌های مخرب برای عبور از روش‌های احراز هویت ایمیلDKIM SPF, و DMARC اعمال کردند.

مجرمان سایبری گواهی‌های فیشینگ و EV را برای ارائه Payloadهای باج‌افزار ترکیب می‌کنند

آسیب‌پذیری بحرانی در GitLab

به‌روزرسانی‌های امنیتی GitLab، برای رسیدگی به یک آسیب‌پذیری بحرانی منتشر شده است که به مهاجمان اجازه می‌دهد خطوط لوله را مانند سایر کاربران از طریق سیاست‌های اسکن امنیتی برنامه‌ریزی شده اجرا کنند.

جزئیات آسیب‌پذیری

GitLab یک پلت‌فرم مدیریت پروژه و ردیابی نرم‌افزار منبع باز مبتنی بر وب است که نسخه رایگان و تجاری آن را ارائه می‌دهد.

این آسیب‌پذیری با عنوان CVE-2023-4998 و امتیاز 9.6 ارزیابی شده است.

جعل هویت کاربران بدون مجوز آنها، برای اجرای وظایف خط لوله، می‌تواند منجر به دسترسی مهاجمان به اطلاعات حساس یا بهره‌برداری از مجوزهای کاربران جعل شده برای اجرای کد، تغییر داده‌ها یا راه‌اندازی رویدادهای خاص در سیستم GitLab شود.

با توجه به اینکه GitLab برای مدیریت کد استفاده می شود، این آسیب‌پذیری می‌تواند منجر به آسیب رساندن به نشت داده‌ها، حملات زنجیره تامین و سایر سناریوهای پرخطر شود.

اکسپلویت موفقیت‌آمیز از آسیب‌پذیری CVE-2023-5009 می‌تواند به یک مهاجم اجازه دهد به اطلاعات حساس دسترسی داشته باشد یا از مجوزهای بالاتر کاربر جعل شده برای تغییر کد منبع یا اجرای کد بر روی سیستم استفاده کند.

محصولات تحت تأثیر

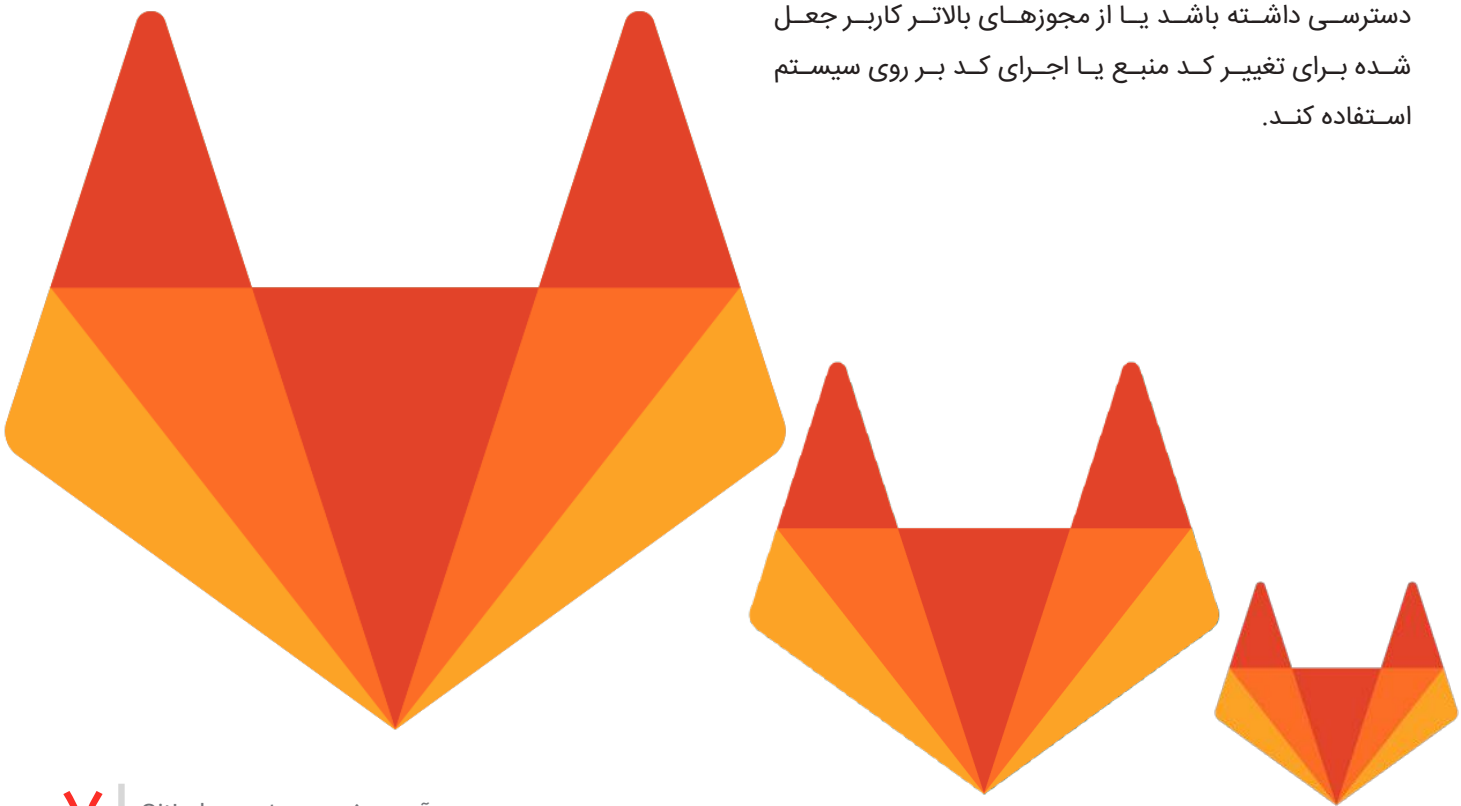
این آسیب‌پذیری در GitLab نسخه‌های 13,12 تا 16,2,7 و 16,3 تا 16,3,4 تاثیرگذار بوده است.

توصیه‌های امنیتی

به کاربران توصیه شده است، برای محافظت در برابر خطرات احتمالی، به‌روزرسانی‌های امنیتی را اعمال کنند. نسخه‌های 16,3,4 و 16,2,7 آسیب‌پذیری CVE-2023-5009 را برطرف کرده‌اند.

از کاربران نسخه‌های قبل از 16,2 که رفع مشکل امنیتی را دریافت نکرده‌اند، خواسته شده است انتقال مستقیم و سیاست‌های امنیتی را فعال نکنند. انتقال مستقیم، قابلیتی است که امکان مهاجرت گروه ها و پروژه ها را با انتقال مستقیم فراهم می کند. در حالی که سیاست‌های امنیتی، از اسکن‌هایی که بر اساس زمان‌بندی یا در خط لوله پروژه اجرا می‌شوند، پشتیبانی می‌کنند.

در صورت فعال بودن هر دو ویژگی، نمونه آسیب‌پذیر خواهد بود.



یک Backdoor پیشرفته به نام Dead glyph با تاکتیک‌های مختلف بدافزاری

محققان امنیت سایبری بدافزاری به نام Deadglyph کشف کردند که در حملات سایبری جاسوسی یک گروه تهاجمی به نام Stealth Falcon مورد استفاده قرار گرفته است.

معماری Deadglyph به‌عنوان یک معماری غیرمعمول شناخته شده است چراکه شامل یک فایل باینری native x64 و یک فایل .NET می‌باشد، این ترکیب غیرمعمول است زیرا معمولاً تنها از یک زبان برنامه‌نویسی برای پیاده‌سازی نرم‌افزارهای مخرب استفاده می‌شود. این تفاوت ممکن است به معنای توسعه جداگانه این دو مؤلفه باشد و در عین حال از ویژگی‌های منحصر بفرد زبان‌های برنامه‌نویسی متفاوتی که بکار گرفته شده، بهره می‌برد.

همچنین، این امکان وجود دارد که استفاده از زبان‌های برنامه‌نویسی مختلف یک تاکتیک عمدی است تا تحلیل را مشکل‌تر کند و اجازه ندهد به سادگی به آن دست پیدا کرد. بر خلاف دیگر بدافزارهای backdoor سنتی، دستورات به‌صورت ماژول‌های اضافی از یک سرور تحت کنترل دریافت می‌شوند که به این برنامه امکان ایجاد پردازه‌های جدید، خواندن فایل‌ها و جمع‌آوری اطلاعات از سیستم‌های تخریب شده را می‌دهد.

Stealth Falcon[1] در ابتدا توسط Citizen Lab در سال 2016 فاش شد و با حملات جاسوسی هدفمندی در خاورمیانه شناخته شد. این حملات با استفاده از لینک‌های مخصوص که به اسناد حاوی ماکرو متصل بودند و به‌منظور اجرای دستورات دلخواه صورت می‌گیرند.

تحقیقات بعدی توسط رویترز در سال 2019 عملیات پروژه راون را فاش کرد که اعضای آن شامل گروهی از مهاجمان سابق ایالات متحده بود که توسط شرکت امنیتی به نام DarkMatter جهت جاسوسی استخدام شده بودند.

احتمالا Stealth Falcon و اعضای دخیل در پروژه راون به دلیل مشابهت در تاکتیک‌ها و هدف‌گیری‌ها یک گروه هستند. این گروه همچنین از آسیب‌پذیری‌های روز

صفر ویندوز مانند CVE-2018-8611 و CVE-2019-0797 استفاده کرده‌اند. در آوریل 2020 اعلام شد که این گروه جاسوسی بیشترین تعداد آسیب‌پذیری‌های روز صفر را نسبت به هر گروه دیگری از سال 2016 تا 2019 استفاده کرده است.

در همان زمان، ESET جزئیات استفاده از یک backdoor به نام Win32/StealthFalcon را نیز توضیح داد که از سرویس انتقال پس‌زمینه ویندوز[2] جهت ارتباط و به آوردن کنترل کامل سیستم قربانی استفاده کرده است. روش دقیقی که برای ارسال این برنامه استفاده می‌شود در حال حاضر ناشناخته است، اما جزء اولیه که اجرای

1- FruityArmor
2- BITS

آن را فعال می‌کند یک بارگذار شل‌کد است که شل‌کد را از رجیستری ویندوز استخراج و بارگذاری می‌کند که به‌عنوان ماژول x64 و یک اجراکننده شناخته می‌شود. سپس اجراکننده با بارگذاری یک مولفه .NET به نام Orchestrator ادامه می‌دهد تا با سرور کنترل ارتباط برقرار کند. دستوراتی که از سرور دریافت می‌شود به‌صورت ماژول‌های اجرایی به انجام می‌رسند و می‌توانند در یکی از سه دسته تسک‌های Orchestrator ، اجراکننده و آپلود انجام شوند.

بعضی از وظایف اجراکننده شامل ایجاد فرآیند، دسترسی به فایل و جمع‌آوری اطلاعات متا دستگاه است. ماژول تایمر جهت پرس و جوی دوره‌ای سرور C2 به همراه ماژول شبکه استفاده می‌شود که از طریق درخواست‌های POST HTTPS ارتباط C2 را پیاده‌سازی می‌کند.

تسک‌های آپلود، همان‌طور که از نامش پیداست، به backdoor این امکان را خواهد داد تا خروجی دستورات و خطاها را بارگذاری کنند.

Deadglyph از مکانیزم‌های ضد-تشخیصی متعددی بهره می‌برد، از جمله نظارت مداوم بر فرآیندهای سیستم و پیاده‌سازی الگوهای شبکه تصادفی. علاوه بر این، این بدافزار توانایی حذف خود را دارد تا احتمال تشخیص آن در موارد خاصی را به حداقل برسد.

توصیه‌های امنیتی

1. به‌روزرسانی نرم‌افزارها: اطمینان حاصل کنید که سیستم‌عامل و نرم‌افزارهای شما به‌روز هستند. به‌روزرسانی‌ها اغلب اقدامات امنیتی را ارائه می‌دهند که می‌توانند از آسیب‌پذیری‌ها جلوگیری کنند.
2. آنتی‌ویروس: نصب یک برنامه آنتی‌ویروس با قابلیت به‌روزرسانی خودکار می‌تواند به شما کمک کند تا بدافزارها را تشخیص داده و از ورود آنها به سیستم جلوگیری کنید.
3. هویت و دسترسی محدود: دسترسی به سیستم و داده‌های حساس را به کاربران معتبر محدود کنید.
4. آموزش کارکنان: کارکنان را در مورد تهدیدات امنیتی و نحوه رفتار در مقابل ایمیل‌ها و پیام‌های مشکوک آموزش دهید. حملات پیشرفته معمولاً از راه‌های مهندسی اجتماعی برای نفوذ استفاده می‌کنند.
5. مانیتورینگ فعال: نظارت مستمر بر فعالیت‌های سیستمی و شبکه، می‌تواند به میزان قابل توجهی ازورود مهاجمان و بدافزارها به سیستم جلوگیری کند.
6. استفاده از فایروال: نصب یک فایروال سخت‌افزاری یا نرم‌افزاری می‌تواند از ورود ناخواسته به سیستم جلوگیری کند و ترافیک مشکوک را مسدود سازد.
7. پشتیبانی و بازیابی داده: سیستم منظم پشتیبان‌گیری از داده‌های مهم خود ایجاد کنید و برای دسترسی و بازیابی داده‌ها، تدابیر امنیتی را به کار گیرید. این موضوع می‌تواند در مواجهه با حملات رمزگذاری‌شده یا حذف داده‌ها مفید باشد.
8. بررسی مرتب ایمیل‌ها: ایمیل‌ها و پیوست‌های مشکوک را به دقت بررسی کنید و هیچگاه پیوست‌های منابع نامعتبر را دانلود نکنید.
9. استفاده از شبکه VPN: در صورت امکان، از یک شبکه مجزا استفاده کنید تا اطلاعات شما از دسترسی غیرمجاز محافظت شود.
10. حفاظت از اطلاعات و ورودی‌های رجیستری: به‌دقت کنترل کنید که چه اطلاعاتی به رجیستری وارد می‌شود و از داده‌ها و اطلاعات مهم حفاظت کنید.

همچنین، به یاد داشته باشید هیچ سیستمی به‌طور کامل از تهدیدات امنیتی محافظت نمی‌کند، بنابراین ترکیب تدابیر متعدد و ایجاد یک فرهنگ امنیتی در سازمان شما حائز اهمیت است. همچنین توسعه‌دهندگان امنیتی و محققان امنیتی باید کماکان در حال بررسی تهدیدات امنیتی جدید باشند تا بتوانند در اسرع وقت، تهدیدات را شناسایی و از بروز آن‌ها جلوگیری کنند.

حمله بدافزار HiddenGh0st RAT به MS-SQL و MySQL

بدافزار کنترل از راه دور Gh0st RAT، یک نرم‌افزار مخرب معروف است که به‌طور گسترده توسط مهاجمان مورد استفاده قرار می‌گیرد و کد آن به‌صورت عمومی در دسترس می‌باشد.

محققان به تازگی نسخه‌ای از Gh0st RAT را کشف کرده‌اند که به منظور حمله به سرورهای MS-SQL، از یک rootkit مخفی استفاده می‌کند. این rootkit مخفی کار بدافزار را پنهان و از حذف آن جلوگیری خواهد کرد. Rootkit بدافزاری است که فعالیت خود را در سیستم‌عامل کامپیوتر یا دستگاه دیگری مخفی می‌کند تا توانایی کنترل از راه دور آن را به‌دست آورد. این نوع بدافزار به‌طور معمول توسط نفوذکنندگان یا مهاجمان به منظور انجام فعالیت‌های مخرب یا سرقت اطلاعات حساس استفاده می‌شود.

HiddenGh0st نوعی از Gh0st RAT است که توانایی سرقت اطلاعات QQ Messenger را دارد و از سال 2022 کشف شده است.

پژوهشگران امنیت سایبری به‌تازگی گزارش داده‌اند که بدافزار HiddenGh0st به‌صورت فعال به سمت سرورهای MS-SQL و MySQLای که تنظیمات نامناسبی داشتند، حمله می‌کند. این تنظیمات شامل عدم مراقبت یا عدم مدیریت سرورهای MS-SQL و MySQL است که

در ادامه به برخی از این موارد اشاره می‌شود:

1. عدم به‌روزرسانی نرم‌افزارها: عدم به‌روزرسانی سیستم‌عامل، پایگاه‌داده‌ها و نرم‌افزارهای مرتبط با سرورها می‌تواند به آسیب‌پذیری‌های امنیتی منجر شود.
2. استفاده از رمزهای عبور ضعیف: استفاده از رمزهای عبور ضعیف یا پیش‌فرض برای دسترسی به سرورها، که به‌راحتی توسط حملاتی مانند Hid-denGh0st قابل تخمین هستند.
3. اجازه دسترسی به افراد غیرمجاز: تعیین دسترسی‌های نامناسب برای کاربران یا سیستم‌های خارجی به سرورها، ممکن است به دسترسی غیرمجاز مهاجم منجر شود.
4. عدم نظارت مداوم: عدم نظارت و ممانعت از فعالیت‌های غیرمعمول یا حملات به سرورها، می‌تواند امنیت سیستم را تخریب کند.
5. ترکیب کردن سرورهای آسیب‌پذیر در شبکه: اگر سرورهای آسیب‌پذیر در شبکه‌ای با سرورهای حیاتی ترکیب شوند، امکان شناسایی حملات و محافظت از سرورهای حیاتی کاهش می‌یابد.

HiddenGh0st از رمزنگاری، رمزگشایی و اجرای فایل PE خود در حافظه استفاده می‌کند تا از این طریق شناسایی نشود.

داده‌های جمع‌آوری‌شده عبارتند از:

- اطلاعات نسخه ویندوز
- سرعت پردازنده (CPU)
- تعداد واحدهای پردازشی مرکزی (CPUs)
- آدرس IP عمومی
- آدرس IP خصوصی
- نام میزبان سیستم آلوده
- تعداد دوربین‌های وب
- زمان تاخیر اتصال به اینترنت
- سرعت رابط شبکه
- ظرفیت حافظه
- ظرفیت دیسک محلی
- لیست محصولات امنیتی نصب‌شده
- شماره ورود به QQ Messenger
- وضعیت اتصال به اینترنت (LAN، MODEM، PROXY)

توصیه‌های امنیتی

برای جلوگیری از تهدیدات بدافزار Gh0st RAT و HiddenGh0st و دیگر تهدیدات امنیتی مشابه، کاربران باید توصیه‌های امنیتی زیر را در نظر داشته باشند:

1. به‌روزرسانی نرم‌افزارها: اطمینان حاصل کنید که سیستم‌عامل و تمام نرم‌افزارهای شما به‌روز باشند. به‌روزرسانی‌های امنیتی را فوراً اعمال کنید.
2. نصب آنتی‌ویروس: نصب یک آنتی‌ویروس معتبر و به‌روز و اسکن منظم فایل‌ها و برنامه‌های دانلود شده را توصیه می‌کنیم.
3. فعال‌سازی دیواره آتش (Firewall): از یک دیواره آتش استفاده کنید تا ترافیک شبکه را کنترل کنید و دسترسی به سیستم شما را محدود کنید.
4. مدیریت دسترسی‌ها: دسترسی به پوشه‌ها و فایل‌های حساس را محدود کنید و فقط به افرادی که لازم است، دسترسی دهید.
6. مدیریت سرویس‌ها: سرویس‌ها و برنامه‌های غیرضروری را غیرفعال کنید و فقط سرویس‌های مورد نیاز را اجرا کنید.

مرکز آپا دانشگاه سمنان

قدرت فایروال(دیوار آتش)

به قوانین آن است نه قیمت آن!!

فایروال گران بدون قوانین خوب مانند تفنگ بی فشنگ است...

مرکز آپا دانشگاه سمنان

آموزش

مایکروسافت در حال ارائه پشتیبانی از Passkeys در ویندوز ۱۱ است

مایکروسافت به‌عنوان بخشی از به‌روزرسانی بزرگ این سیستم‌عامل دسکتاپ، به‌طور رسمی پشتیبانی از کلیدهای عبور[1] را در ویندوز 11 ارائه می‌کند که برای کاهش سطح حمله طراحی‌شده‌اند. این ویژگی به کاربران این امکان را می‌دهد که بدون نیاز به ارائه نام کاربری و رمز عبور به وب سایت‌ها و برنامه‌ها وارد شوند، در عوض به پین دستگاه یا اطلاعات بیومتریک خود برای تکمیل این مرحله تکیه کنند.

بر اساس استانداردهای FIDO، Passkeys برای اولین بار در می 2022 به‌عنوان جایگزینی برای رمزهای عبور به شیوه‌ای قوی و مقاوم در برابر فیشینگ معرفی شد. از آن زمان تاکنون اپل، گوگل و تعدادی از سرویس‌های دیگر اعتبارنامه Web Authentication[2] را تأیید کردند و در ماه‌های اخیر توسط آن ها به کار گرفته شده است. درحالی‌که این غول فناوری در ژوئن 2023 مدیریت رمز عبور را در برنامه Windows Insider اضافه کرد، این خبرنشان دهنده در دسترس بودن عمومی این ویژگی است.

دیوید وستون، معاون امنیت تجاری و سیستم عامل، گفت: «کلیدهای عبور آینده بین پلتفرمی مدیریت ورود امن هستند. یک رمز عبور یک اعتبارنامه رمزنگاری منحصربه‌فرد و غیرقابل حدس زدن ایجاد می‌کند که به‌طور ایمن در دستگاه شما ذخیره می‌شود».

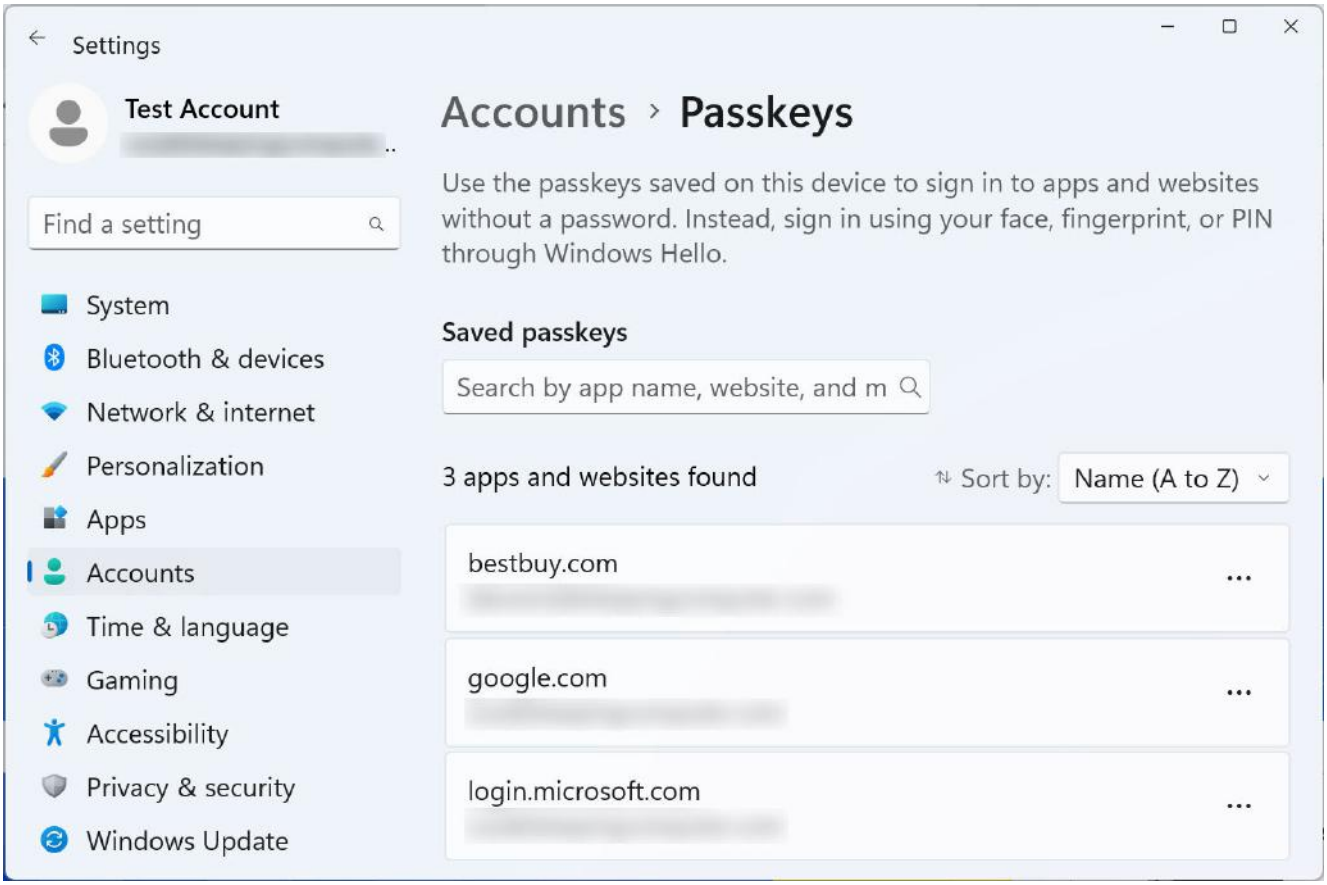
کلیدهای عبور به دستگاه‌های خاصی (مانند رایانه‌ها، تبلت‌ها یا گوشی‌های هوشمند) مرتبط می‌شوند و با ارائه دفاعی قوی در برابر حملات فیشینگ، مسدود کردن عوامل تهدید از سرقت اطلاعات اعتباری و خنثی کردن تلاش‌های دسترسی غیرمجاز، نقشی اساسی در کاهش خطر نقض داده‌ها دارند.

کلیدهای عبور تعدادی مزیت را ارائه می‌دهند زیرا برای هر وب‌سایت یا برنامه منحصر به فرد هستند و نیاز به تنظیم رمزهای عبور پیچیده و دردسر به خاطر سپردن آن‌ها را از بین می‌برند. آن‌ها همچنین بین دستگاه‌های موجود در یک سیستم‌عامل (یا اکوسیستم) همگام‌سازی می‌شوند و فرآیند ورود به سیستم را آسان‌تر می‌کنند.

برای جلوگیری از حملات، این شرکت امکان تولید کلیدهای عبور با استفاده از Windows Hello را فراهم

1-passkeys
2-WebAuthn

می‌کنـد و کاربـران را قـادر می‌سـازد تـا بـا چهـره، پیـن یـا اثرانگشـت خـود وارد حسـاب‌های وب سـایت یـا برنامـه وب خـود شـوند. عـلاوه بـر ایـن، مشـتریان ویـنـدوز 11 همچنیـن می‌تواننـد از دسـتگاه‌های تلفـن همـراه جفـت شـده بـا بلوتـوث بـرای تکمیـل فرآیندهـای ورود اسـتفاده کننـد.
کاربـران مـی تواننـد رمـز عبـور ذخیـره شـده خـود را بـا رفتـن بـه Start > Settings > Accounts > Passkeys مدیریـت کننـد. در کنـار ایـن اعلامیـه، مایکروسـافت اعـلام کـرد کـه Windows Hello for Business را بـه دسـتگاه‌های تحـت مدیریـت سـازمانی ویـنـدوز 11 نیـز مـی‌آورد تـا با ایجـاد امکان بـرای تیم‌هـای فنـاوری اطلاعـات بـه منظـور تعییـن خـط مشـی بـرای دسـتگاه‌های متصـل بـه Microsoft Entra ID، هویـت کاربـران را ایمـن کنـد.



مدیریت کلیدهای عبور در ویندوز 11

دیویـد وسـتون می‌گویـد: «ویـنـدوز ۱۱ بـا توانمندسـازی کاربـران بـرای جایگزینـی رمزهـای عبـور بـا کلیـد هـای عبـور، کار را بـرای هکرهایـی کـه از رمزهـای عبـور سـرقت شـده از طریـق حمـلات فیشـینگ اسـتفاده مـی کننـد، سـخت تـر می کنـد».
دو ویژگـی قابـل توجـه دیگرمرتبـط بـا کاربردهـای سـازمانی عبارت‌انـد از بهبودهایـی در فایـروال داخلـی ویـنـدوز و یـک گزینـه کنتـرل برنامـه سفارشـی جدیـد بـرای اطمینـان از اینکه فقـط برنامه‌هـای تائیـد شـده و قابل‌اعتمـاد روی دسـتگاه‌ها مجـاز هسـتند و از نقـاط پایانـی در برابـر کدهـای تقلبـی محافظـت می‌کنـد. وسـتون گفـت: «بـا کنتـرل کدهـای ناخواسـته یـا مخـرب در حـال اجـرا، کنتـرل برنامـه بخـش مهمـی از یـک اسـتراتژی امنیتـی کلـی اسـت. کنتـرل برنامـه اغلـب به‌عنـوان یکـی از مؤثرتریـن ابزارهـای دفـاع در برابـر بدافزارهـا ذکـر می‌شـود».

منابع:

https://thehackernews.com/2023/09/microsoft-is-rolling-out-support-for.html
https://www.bleepingcomputer.com/new-s/microsoft/windows-11-22h2-adds-a-built-in-passkey-manager-for-windows-hello/

تلاش ما
حفظ امنیت
شماست...