# ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | آبان 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، ادغام دو شرکت مک‌آفی اینترپرایز و فایرآی رسماً آغاز شد و در آینده‌ای نزدیک این دو غول دنیای امنیت سایبری تحت عنوان یک شرکت واحد، قدرتمندتر از قبل به ده‌ها هزار مشتری خود در کشورهای مختلف خدمات‌دهی خواهند کرد. همانطور که در این ماهنامه خواهید خواند، این نقل‌وانتقال عظیم در حالی صورت می‌گیرد که اجرای مستمر حملات مخرب، پیچیده و گسترده، کسب‌وکار تبهکاران سایبری را پررونق‌تر از همیشه کرده است.

از دیگر رخدادهای مهم یک ماه اخیر که در این ماهنامه به آن پرداخته شده می‌توان به بدافزار جدیدی تحت عنوان FoggyWeb که توسط مایکروسافت کشف شده، اشاره کرد. بدافزار مذکور توسط گروه هکری Nobelium برای استقرار و اجرای کدهای بدافزاری و سرقت اطلاعات حساس از سرورهای Active Directory Federation Services مورد استفاده قرار گرفته است.

در ماه‌های اخیر، موارد متعددی از سوءاستفاده مهاجمان از آسیب‌پذیری محصولات مختلف وی‌ام‌ور با هدف رخنه به شبکه سازمان‌ها گزارش شده است. یکی از جدیدترین نمونه از این حملات سوءاستفاده از یک ضعف‌امنیتی "حیاتی" در محصول vCenter Server می‌باشد. راهنمای فنی جهت برطرف نمودن آسیب‌پذیری مذکور در این ماهنامه به تفصیل مورد بررسی قرار گرفته است.

شرکت مایکروسافت همچنین در اواخر این ماه در خصوص دو ضعف‌امنیتی در PowerShell 7 که منجر به عبور از سد کنترل‌های امنیتی Windows و افشای اطلاعات اصالت‌سنجی می‌شود، هشدار داد. جزئیات مربوط به نسخه‌های به‌روز شده، نسخه‌هایی از PowerShell که تحت تاثیر آسیب‌پذیری‌های فوق بوده‌اند و نحوه به‌روزرسانی در این ماهنامه قابل مطالعه است.

بررسی‌های اخیر محققان شرکت کوالیس و سایت VirusTotal بر روی نمونه‌ها و حملات بزرگ باج‌افزاری سال‌های اخیر نشان می‌دهد که مهاجمان علاوه بر بهره‌جویی از ضعف‌های امنیتی شناخته شده و جدید، در بیشتر موارد از برخی آسیب‌پذیری‌های قدیمی برای توزیع باج‌افزار سوءاستفاده می‌کنند. مشروح گزارش‌های فوق در این ماهنامه قابل مطالعه است.

در این ماهنامه به روش کار نمونه دیگری از باج‌افزارهای گروه Nobelium به نام Tomiris پرداخته شده که با بهره‌گیری از تکنیک موسوم به زنجیره تأمین پس از هک شرکت سولارویندز اقدام به تزریق کد آلوده به یکی از فایل‌های نرم‌افزار SolarWinds Orion و تبدیل آن به یک درب‌پشتی کردند. علاوه بر باج‌افزار مذکور، در این ماهنامه عملکرد نسخ جدید باج‌افزار مخرب دیگری مورد بررسی قرار گرفته که از ماژول‌های سفارشی و برنامه‌ریزی شده برای آلوده‌سازی سیستم‌های تحت Linux استفاده می‌کنند.

در ماهی که گذشت محققان شرکت امنیتی سوفوس در گزارشی به بررسی فهرستی از رایج‌ترین اشتباهات امنیتی موجود که هنگام بررسی و خنثی‌سازی حملات سایبری در طیف وسیعی از سازمان‌ها با آنها مواجه شده‌اند، پرداخته‌اند. برگردان مشروح گزارش سوفوس در این ماهنامه قابل مطالعه است.

در اولین ماه از پاییز ۱۴۰۰، مایکروسافت، سیسکو، مک‌آفی، وی‌ام‌ور، اوراکل، ادوبی، گوگل، اپل، موزیلا، آپاچی و جونیپر نت‌ورکز 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

# FoggyWeb بدافزار جدید

## گروه Nobelium


مایکروسافت (Microsoft Corp) بدافزار جدیدی را کشف کرده که توسط گروه هکری Nobelium برای استقرار و اجرای کدهای بدافزاری و سرقت اطلاعات حساس از سرورهای Active Directory Federation Services - به اختصار ADFS - مورد استفاده قرار گرفته است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، جزییات این بدافزار مورد بررسی قرار گرفته است.

Nobelium، گروهی است که برخی منابع آن را منتسب به سازمان اطلاعات خارجی غیرنظامی فدراسیون روسیه (Russian Foreign Intelligence Service - به اختصار SVR) می‌دانند. از Nobelium با نام‌های APT29، The Dukes یا Cozy Bear نیز یاد می‌شود. این مهاجمان سال گذشته در جریان حملاتی از نوع زنجیره تامین (Supply Chain Attack) از طریق یکی از نرم‌افزارهای ساخت شرکت سولاروینذز (SolarWinds, LLC) موفق به رخنه به هزاران شرکت و سازمان شدند.

حملات زنجیره تامین حملات سایبری هستند که با هدف قرار دادن عناصر با امنیت کمتر در شبکه، به کل سازمان آسیب می‌رسانند. در واقع در این حملات، مهاجمان با بهره‌جویی از اجزای آسیب‌پذیر یک نرم‌افزار معتبر در زنجیره تامین یک سازمان به آن رخنه و یا آن را دچار اختلال می‌کنند.

در جریان حمله فوق، مهاجمان پس از هک شرکت سولاروینذز اقدام به تزریق کد آلوده به یکی از فایل‌های نرم‌افزار SolarWinds Orion با نام SolarWinds.Orion.Core.BusinessLayer.dll و تبدیل آن به یک درب‌پشتی (Backdoor) کردند. فایل مذکور نیز از طریق قابلیت به‌روزرسانی خودکار این نرم‌افزار به شبکه مشتریان سولاروینذز راه یافته بود. در عمل موجب شد که شبکه مشتریان این نرم‌افزار در هر نقطه از جهان به تسخیر آنها در بیاید.

در اردیبهشت ماه، دولت ایالات متحده به طور رسمی سازمان اطلاعات خارجی غیرنظامی فدراسیون روسیه را متهم به "کمپین جاسوسی سایبری گسترده" در این کشور نمود.

شرکت امنیت سایبری ولکسیتی (Volexity Inc.) نیز ۴ خرداد ۱۴۰۰ در مقاله‌ای که مشروح آن در لینک زیر قابل مطالعه است، بر اساس کارزارهای فیشینگ شناسایی شده و شباهت آن‌ها به تاکتیک‌های مشاهده شده در رویدادهای سال ۲۰۱۸، گروه APT29 را مسئول حملات فوق دانست.

https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

به نقل از این شرکت، این گروه، سازمان‌های دولتی و غیردولتی، موسسات تحقیقاتی و آژانس‌های بین المللی مستقر در ایالات متحده و اروپا را هدف قرار داده است.

براساس گزارشی که مایکروسافت در ۵ مهر ماه منتشر کرده، بدافزار گروه Nobelium، که FoggyWeb لقب گرفته است، یک درب پشتی بسیار هدفمند است که از پروتکل Security Assertion Markup Language - به اختصار SAML - سوءاستفاده می‌کند.

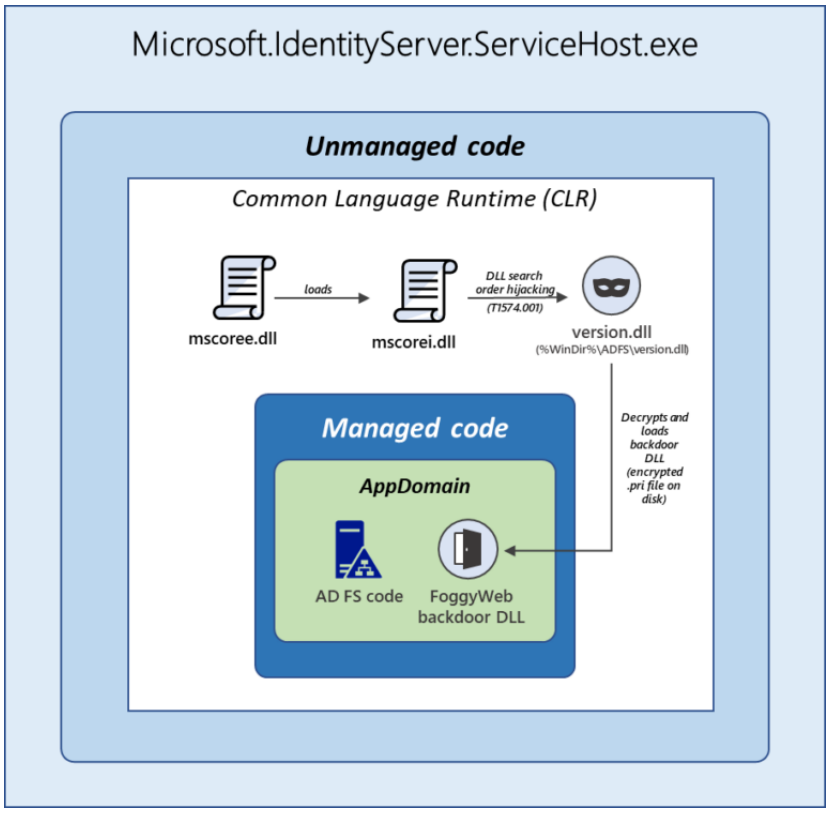
Nobelium از تاکتیک‌های مختلفی برای سرقت اطلاعات اصالت‌سنجی با هدف دستیابی به سطح دسترسی Administrator در سرورهای ADFS استفاده می‌کند. هنگامی که Nobelium اطلاعات اصالت‌سنجی را بدست آورد و موفق به هک سرور شد، مهاجمان برای ماندگارکردن خود و نفوذ بیشتر از بدافزارها و ابزارهای پیچیده استفاده می‌کنند.

Nobelium از درب‌پشتی FoggyWeb جهت استخراج از راه دور پیکربندی پایگاه‌داده سرورهای هک شده ADFS، گواهینامه رمزگشایی شده Token-signing و گواهینامه Token-decryption و همچنین دانلود و اجرای کدهای بیشتر استفاده می‌کند. همچنین می‌تواند اجزا و کدهای مخرب دیگر را از سرور کنترل و فرمان‌دهی (C2) دریافت کرده و آنها را در سرور هک شده اجرا کند.

پس از هک سرور ADFS، Nobelium با استفاده از حق دسترسی Administrator، دو فایل زیر را در سیستم دانلود می‌کند.

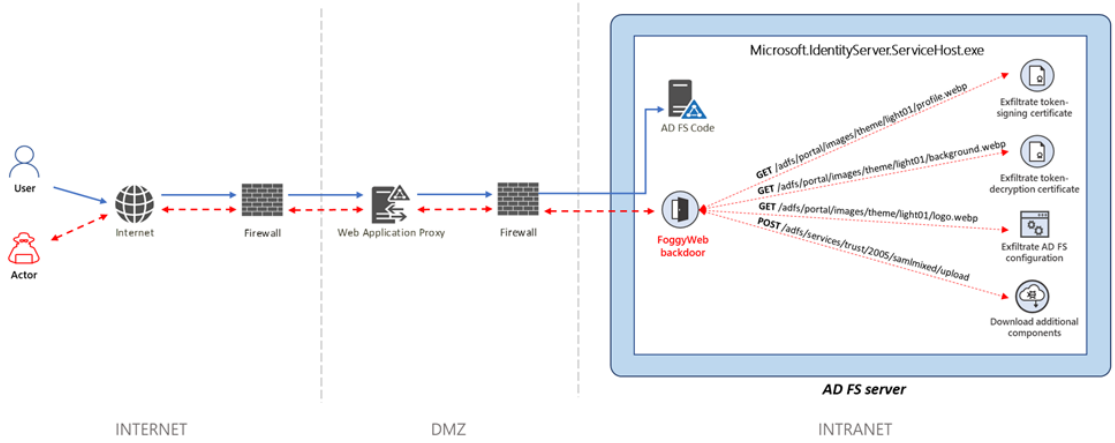
- %WinDir%\ADFS\version.dll
- %WinDir%\SystemResources\Windows.Data.TimeZones\pris\Windows.Data.TimeZones.zh-PH.pri

FoggyWeb در فایل رمزگذاری شده Windows.Data.TimeZones.zh-PH.pri ذخیره شده است، در حالی که فایل مخرب version.dll را می‌توان به عنوان اجراکننده (Loader) آن درنظر گرفت.




این درب‌پشتی اقدام به راه‌اندازی HTTP Listeners می‌کند تا نشانی‌های URL تعریف شده توسط مهاجم را که از ساختار URL معتبر ADFS تقلید می‌کنند، پیکربندی نموده و تمام درخواست‌های HTTP GET/POST را که از اینترنت/اینترانت به سرور ADFS ارسال می‌شود، رصد کند و درخواست‌های HTTP که مطابق با الگوهای URL سفارشی شده توسط مهاجم است، رهگیری نماید.

هکرهای منتسب به روسیه از اردیبهشت ماه، در حال استفاده از درب پشتی FoggyWeb هستند.




این شرکت به سازمان‌هایی که مورد نفوذ قرار گرفته‌اند یا آلوده شده‌اند، انجام اقدامات زیر را توصیه می‌کند:

- زیرساخت‌های شبکه‌ای چه در محل سازمان چه در بسترهای رایانش ابری، از لحاظ پیکربندی، تنظیمات مختص هر کاربر و هر برنامه، قواعد Forwarding و سایر تغییراتی که ممکن است مهاجمان برای حفظ دسترسی خود انجام داده باشند، ارزیابی و بررسی شوند.
- هر گونه دسترسی کاربر و برنامه‌های کاربردی حذف شود و پیکربندی‌ها برای هر یک بررسی شده و مجدداً رمزهای عبور جدید و پیچیده تنظیم و اعمال شود.
- همانطور که در توصیه‌نامه امنیتی زیر اشاره شده از یک ماژول امنیتی سخت‌افزاری (Hardware Security Module - به اختصار HSM) جهت جلوگیری از افشا و استخراج اطلاعات توسط تهدیداتی همچون FoggyWeb استفاده شود.

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

محققان شرکت مایکروسافت در ماه‌های گذشته نیز به بدافزارهای زیر که توسط گروه Nobelium مورد استفاده قرار گرفتند، اشاره کردند:

- BoomBox
- EnvyScout
- Shellcode
- VaporRage
- NativeZone
- GoldMax
- Sibot
- GoldFinder

مشروح گزارش این شرکت در خصوص تهدیدات مذکور در لینک‌های زیر قابل مطالعه است:

- https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/
- https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

گزارش مایکروسافت در خصوص درب‌پشتی FoggyWeb نیز در لینک زیر قابل دریافت است:

https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

# FontOnLake؛

## تهدیدی علیه سیستم‌های تحت Linux


اخیراً شرکت ای‌ست (.ESET, LLC) در گزارشی به تحلیل خانواده‌ای بدافزاری پرداخته که از ماژول‌های سفارشی و برنامه‌ریزی شده برای آلوده‌سازی سیستم‌های تحت Linux استفاده می‌کنند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده جزییات این بدافزار بررسی شده است.

شرکت ای‌ست بدافزار فوق را FontOnLake نامگذاری کرده است. ماژول‌های موجود در این بدافزار که دائما در حال تکامل هستند، دسترسی از راه دور را برای مهاجمان فراهم می‌کنند، اطلاعات اصالت‌سنجی قربانیان را جمع‌آوری نموده و به عنوان یک سرور پروکسی عمل می‌کنند.

این خانواده بدافزاری برای سرقت اطلاعات اصالت‌سنجی (همچون رمزهای عبور SSH) یا انجام سایر فعالیت‌های مخرب از برنامه‌های کاربردی به ظاهر معتبر برای دانلود درب‌پشتی (Backdoor) و روتکیت (Rootkit) استفاده می‌کند. بدافزار مذکور از فرامینی همچون kill، cat و sshd که معمولاً در سیستم‌های تحت Linux استفاده می‌شوند به عنوان سازوکاری جهت ماندگاری در سیستم استفاده می‌کند.

محققان ای‌ست در سال گذشته چندین نمونه از این بدافزار را که در سایت VirusTotal آپلود شده بود، شناسایی کردند. اولین فایل از این نمونه بدافزاری در ماه می ۲۰۲۰ در VirusTotal آپلود شده است.

FontOnLake که به صورت پیچیده و حرفه‌ای طراحی شده، علاوه بر بکارگیری درگاه‌های غیر استاندارد، برای هر یک از حملات هدفمند خود از سرورهای کنترل و فرمان‌دهی (C2) منحصر به فردی استفاده می‌کند تا شناسایی نشود.

با اینکه محققان ای‌ست اعلام نموده‌اند که FontOnLake در قالب تروجان (Trojan) در برنامه‌های کاربردی به ظاهر معتبر منتشر می‌شود، اما نمی‌دانند چگونه این مهاجمان قربانیان را برای دانلود برنامه‌های فوق ترغیب می‌کنند. از جمله فرامین مبتنی بر Linux که مهاجمان با تغییر آن‌ها FontOnLake را منتشر می‌کنند، می‌توان به موارد زیر اشاره کرد:

- cat: که برای چاپ محتوای یک فایل استفاده می‌شود.
- kill: فهرست تمام پروسه‌های در حال اجرا را نمایش می‌دهد.
- sftp: ابزار امن FTP است.
- sshd: پروسه سرور OpenSSH

این‌ها فرامین استاندارد Linux هستند که از ابتدای راه‌اندازی و اجرای سیستم می‌توان از آن‌ها استفاده کرد.

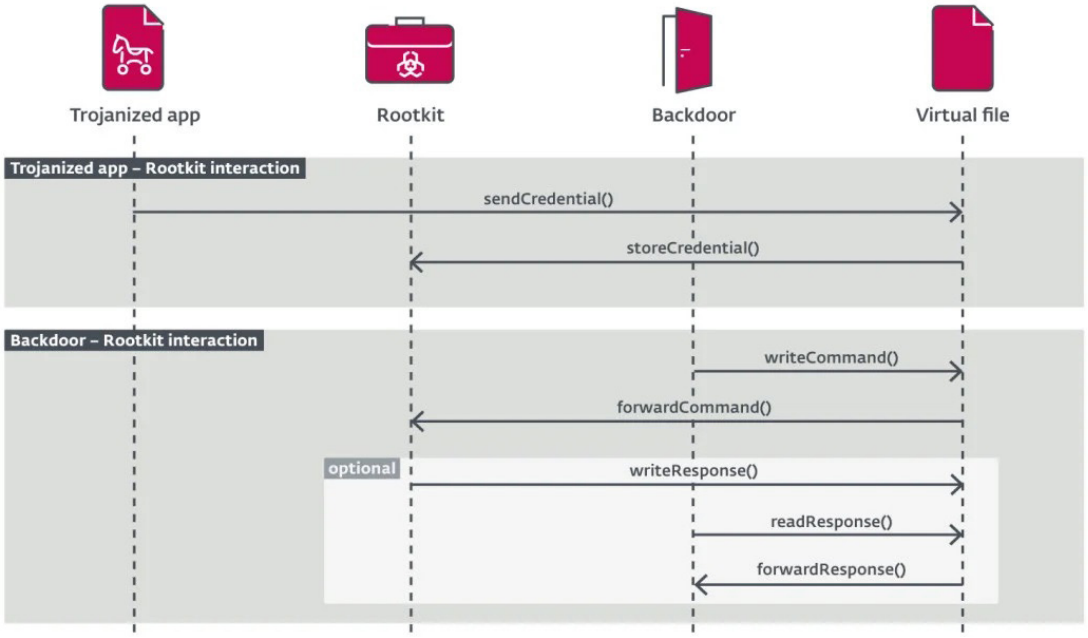
> “All the trojanized files are standard Linux utilities and serve as a persistence method because they are commonly executed on system start-up,” Vladislav Hrčka, malware analyst and reverse engineer at ESET,

محققان بر این باورند که برنامه‌های کاربردی حاوی تروجان به احتمال زیاد کد منبع (Source Code) را تغییر داده‌اند که این امر نشان‌گر این است که مهاجم آنها را کامپایل نموده و جایگزین کد اصلی کرده است.

مهاجمان از این برنامه‌های کاربردی به ظاهر معتبر، علاوه بر انتقال بدافزار برای انتشار سایر کدهای بدافزاری، سرقت اطلاعات یا اجرای اقدامات مخرب دیگر استفاده می‌کنند.

محققان سه درب‌پشتی را نیز که به زبان C++ نوشته شده و توسط FontOnLake بکارگرفته شده، کشف کردند که برای مهاجمان دسترسی از راه دور به سیستم‌ها را فراهم می‌کنند. هر سه این درب‌های پشتی، اطلاعات اصالت‌سنجی سرقت شده sshd و تاریخچه دستورات bash را جمع‌آوری نموده و به سرور کنترل و فرمان‌دهی منتقل می‌کنند. آنها همچنین فعال بودن بدافزار را در دوره‌های زمانی نامشخص از طریق برقراری اتصال با سرورهای مذکور بررسی می‌کنند.

ای‌ست در گزارش فنی خود خاطرنشان می‌کند که ماژول FontOnLake برای مخفی نمودن خود همیشه از یک روتکیت استفاده می‌کند که این روتکیت مسئول به‌روزرسانی و انتقال درب‌های پشتی نیز می‌باشد.




همه نمونه‌های روتکیت که محققان ای‌ست در تحقیق خود شناسایی کردند دو نسخه زیر را در Kernel سیستم‌عامل Linux مورد هدف قرار می‌دهند.

kernel version 3.10.0-229.el7.X86_64
kernel version 2.6.32-696.el6.x86_64

دو نسخه کشف شده بر اساس یک پروژه روتکیت منبع باز هشت ساله به نام Suterusu است که جزییات آن در نشانی زیر قابل دریافت است.

https://github.com/mncoppola/suterusu

با بکارگیری روتکیت‌های مذکور قابلیت‌های زیر برای تبهکاران سایبری فراهم می‌شود:

- مخفی کردن پروسه
- مخفی کردن فایل
- مخفی کردن خود روتکیت
- مخفی کردن ارتباطات شبکه
- منتقل نمودن اطلاعات اصالت‌سنجی سرقت شده به درب‌پشتی مربوطه
- انجام Port Forwarding
- دریافت بسته‌هایی که به طور خاص روتکیت را به دانلود و اجرای درب‌پشتی دیگری هدایت می‌کنند.

ارتباط بین برنامه‌کاربردی حاوی تروجان و روتکیت از طریق فایل مجازی است که روتکیت ایجاد می‌کند. مهاجم می‌تواند داده‌های این فایل را بخواند یا در آن بنویسد و آن‌ها را از طریق درب‌پشتی منتقل کند.

محققان ای‌ست پس از بررسی نمونه‌های موجود در سایت VirusTotal گزارش نمودند که نویسندگان FontOnLake افرادی مجرب و ماهر هستند زیرا سرورهای کنترل و فرمان‌دهی را پس از اطمینان از دانلود غیرفعال می‌کنند.

آن‌ها در ادامه اشاره کردند که FontOnLake ممکن است همان بدافزاری باشد که قبلاً توسط محققان شرکت تنسنت (Tencent, Ltd.) تحلیل شده است و آنها را مرتبط با تهدیدات مستمر و پیشرفته (Advanced Persistent Threat - به اختصار APT) می‌دانستند. گزارش شرکت تنسنت در نشانی زیر قابل دریافت است.

https://security.tencent.com/index.php/blog/msg/180

در اواخر ماه آگوست، شرکت امنیت سایبری آواست (Avast Software s.r.o) نیز در توییتی اعلام کرد که بدافزاری جدید مبتنی بر Linux را که از Suterusu استفاده می‌کند، کشف کرده است. شرکت مذکور بدافزار فوق را HCRootkit نامید و همانند محققان ای‌ست اعلام نموده که این بدافزار نیز از طریق یک درب‌پشتی که به زبان C++ نوشته و در قالب برنامه‌های کاربردی به ظاهر معتبر منتقل و منتشر می‌شود.

محققان لیس‌ورک (Lacework, Inc.) نیز HCRootkit را تحلیل کردند و جزئیات آن را در نشانی زیر به اشتراک گذاشتند. نتایج گزارش منتشر شده نشان می‌دهد که بدافزار فوق مشابه FontOnLake است.

https://www.lacework.com/blog/hcrootkit-sutersu-linux-rootkit-analysis/

مشروح گزارش ای‌ست در نشانی زیر قابل مطالعه است:

https://www.welivesecurity.com/2021/10/07/fontonlake-previously-unknown-malware-family-targeting-linux/

# هشدار مایکروسافت

## در خصوص وجود دو آسیب‌پذیری در PowerShell

شرکت مایکروسافت (Microsoft Corp) به راهبران امنیتی توصیه نموده تا در اسرع وقت نسبت به وصله دو ضعف‌امنیتی در PowerShell 7 اقدام کنند. این آسیب‌پذیری‌ها به مهاجمان اجازه می‌دهند تا از سد کنترل‌های امنیتی Windows Defender Application Control - به اختصار WDAC - عبور کرده و به اطلاعات اصالت‌سنجی دسترسی پیدا کنند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده جزییات این دو آسیب‌پذیری مورد بررسی قرار گرفته است.

PowerShell یک بستر (Platform) و یکی از ابزارهای خودکارسازی وظایف و مدیریت پیکربندی است که توسط شرکت مایکروسافت برای سیستم‌عامل Windows ارائه شده است. این ابزار جهت کاهش حجم کاری مدیران و کاربران ایجاد شده تا قابلیت خودکارسازی تنظیمات سیستم‌عامل، وظایف و پردازش‌های ساده Windows را فراهم کند.

PowerShell متشکل از یک پوسته خط فرمان و یک زبان برنامه نویسی Scripting بوده و بیش از ۱۳۰ خط فرمان استاندارد برای توابع مختلف دارد. در ابتدا فقط یکی از مولفه‌های Windows بود که به Windows PowerShell معروف و بر روی Net Framework. ساخته شده بود. در ۱۸ آگوست ۲۰۱۶، با معرفی PowerShell Core به صورت منبع‌باز و چندبستری بر روی Net Core. ساخته شد.

در ماه‌های اکتبر و سپتامبر نیز نسخه‌های PowerShell 7.0.8 و PowerShell 7.1.5 به منظور رفع ضعف‌امنیتی موجود در PowerShell 7 و PowerShell 7.1 ارائه شده بود.

WDAC جهت محافظت از سیستم‌های Windows در برابر نرم‌افزارهای مخرب و تضمین اجرای برنامه‌های معتبر و راه‌اندازهای امن طراحی شده است و اجرای بدافزارها و نرم افزارهای ناخواسته را مسدود می‌کند.

هنگامی که لایه امنیتی مبتنی بر نرم‌افزار WDAC در Windows فعال است، PowerShell به طور خودکار به وضعیت Constrained Language Mode سوییچ می‌کند و تنها موجب دسترسی به مجموعه محدودی از Windows API می‌شود.

مهاجمان با سوءاستفاده از ضعف‌امنیتی موجود در WDAC که از نوع "عبور از سد کنترل‌های امنیتی" (Security Feature Bypass) بوده و دارای شناسه CVE-2020-0951 می‌باشد، فهرست مجاز WDAC را دور زده و فرامین PowerShell را که در حالت عادی بواسطه فعال بودن WDAC مسدود می‌شوند، اجرا می‌کنند.

شرکت مایکروسافت در گزارش خود به نشانی زیر اعلام نموده که مهاجم جهت سوءاستفاده از این آسیب‌پذیری، به سطح دسترسی ممتاز (Administrator) در سیستم محلی که PowerShell در آن اجرا می‌شود، نیاز دارد. مهاجم پس از دستیابی به سطح دسترسی بالا، به PowerShell متصل شده و فرامینی را جهت "اجرای کد ناخواسته" (Arbitrary Code Execution) ارسال می‌کند.

https://github.com/PowerShell/Announcements/issues/27

آسیب‌پذیری دوم، که دارای شناسه CVE-2021-41355 می‌باشد، ضعف امنیتی از نوع "افشای اطلاعات" (Information Disclosure) در .NET Core. است که سوءاستفاده از آن، اطلاعات اصالت‌سنجی را به صورت کاملاً واضح در سیستم‌هایی که سیستم‌عاملی غیر از Windows در آن‌ها در حال اجراست، فاش می‌کند.

مایکروسافت در گزارش دیگری به نشانی زیر، عنوان نموده که ضعف‌امنیتی مذکور از طریق System.DirectoryServices.Protocols.LdapConnection منجر به افشای اطلاعات اصالت‌سنجی به صورت کاملاً واضح در سیستم‌های فاقد سیستم‌عامل Windows می‌شود.

https://github.com/PowerShell/Announcements/issues/26

آسیب‌پذیری CVE-2020-0951 در هر دو نسخه PowerShell 7 و PowerShell 7.1 وجود دارد، در حالی که فقط کاربران Pow-erShell 7.1 از ضعف‌امنیتی با شناسه CVE-2021-41355 تأثیر می‌پذیرند.

به منظور شناسایی نسخه‌ای از PowerShell که در سیستم در حال اجرا است و تعیین اینکه سیستم در برابر کدام یک از دو ضعف امنیتی فوق آسیب‌پذیر می‌باشد، راهبران می‌توانند فرمان pwsh -v را در Command Prompt اجرا کنند.

مایکروسافت در ادامه عنوان می‌کند که در حال حاضر هیچ‌گونه اقدام کاهشی جهت مسدودسازی سوءاستفاده از ضعف‌های امنیتی مذکور وجود ندارد و به راهبران امنیتی توصیه می‌کند تا در اسرع وقت نسخه‌های به‌روز شده PowerShell 7.0.8 و PowerShell 7.1.5 را جهت محافظت سیستم‌ها در برابر حملات احتمالی نصب کنند.

مایکروسافت در ادامه به راهبران امنیتی توصیه نموده که به‌روزرسانی نسخه‌ای از PowerShell 7 را که تحت تاثیر ضعف‌های امنیتی مذکور نبوده است، در دستور کار خود قرار دهند. جزئیات مربوط به نسخه‌های به‌روز شده و نسخه‌هایی از PowerShell که تحت تاثیر آسیب‌پذیری‌های فوق بوده‌اند در نشانی‌های زیر قابل دریافت است.

https://github.com/PowerShell/Announcements/issues/27

https://github.com/PowerShell/Announcements/issues/26

در ماه جولای نیز این شرکت در مورد آسیب‌پذیری دیگری از نوع "اجرای کد از راه دور" (Remote Code Execution) با شناسه CVE-2021-26701 در PowerShell 7 هشدار داده بود.

این شرکت اعلام نموده که با انتشار به‌روزرسانی‌های بعدی از طریق سرویس Microsoft Update Service، به‌روزرسانی PowerShell برای مشتریان Windows 10 و Windows Server آسان‌تر می‌شود.

# رویدادها و وقایع امنیتی

# کلاهبرداری گردانندگان REvil
## از شرکای خود


برخی گزارش‌ها حکایت از آن دارد که گردانندگان باج‌افزار REvil اقدام به در کنترل گرفتن مذاکرات مطالبه باج با قربانیان نموده و از پرداخت سهم باج دریافتی به شرکای خود اجتناب می‌کنند.

گروه باج‌افزاری REvil که در نیمه اول سال ۲۰۱۹ ظاهر شد، با نام‌های Sodin و Sodinokibi نیز شناخته می‌شود. تصور می‌شود که این گروه جانشین گروه باج‌افزاری GandCrab است که البته اکنون دست از فعالیت کشیده است. REvil نام باج‌افزاری است که در قالب خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) به سایر مهاجمان فروخته می‌شود و توانسته طرفداران زیادی را در بازارهای زیرزمینی تبهکاران سایبری به خود جلب کند.

در خدمات 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 از قربانی به نویسنده باج‌افزار و مبلغ بیشتر (معمولاً ۸۰-۷۰ درصد) به متقاضی سرویس می‌رسد.

گردانندگان باج‌افزار REvil با استفاده از یک کلید اصلی (Master Private Key)، تمام فایل‌های رمزگذاری شده توسط مشترکان RaaS را رمزگشایی نموده و شرکای خود را از این معامله خارج کرده و کل باج را سرقت می‌کنند.

این کلاهبرداری چندی پیش در تالارهای گفتگوی زیرزمینی، بین مشترکان RaaS مورد بحث و بررسی قرار گرفته و اخیراً توسط محققان امنیتی و توسعه‌دهندگان بدافزار نیز تأیید شده است.

گروه REvil که توسط مهاجمان باتجربه در تالارهای گفتگوی زیرزمینی تبلیغ می‌شد، گروهی با درآمدی بسیار بالا است که فقط اقدام به جذب هکرهای مجرب شبکه می‌نمودند. اگرچه گروه REvil در ابتدا به عنوان تبهکاران سایبری "صادق" آغاز به کار نمودند، به زودی به کلاهبرداری از سهم ۷۰ درصدی باج پرداختی به شرکای خود روی آورد.

به نقل از مدیر تیم تحقیقات اینتل (Intel Corporation)، حداقل از سال ۲۰۲۰، مهاجمان مختلف در بازارهای زیرزمینی ادعا کرده‌اند که گردانندگان RaaS مذاکرات خود را با قربانیان در اتاق‌های گفتگوی خصوصی بدون آنکه شرکای آنها مطلع باشند، انجام می‌دهند. این شایعه پس از تعطیلی ناگهانی DarkSide و Avaddon و انتشار کلیدهای رمزگشای این دو باج‌افزار بیشتر شد.

وی در ادامه عنوان می‌کند که گردانندگان REvil نیز مشابه شرکای آنها برای مذاکره و مطالبه باج از قربانی، از اتاق‌های گفتگوی خصوصی استفاده می‌کنند. در این حال وقتی مذاکرات به نقطه حساسی می‌رسد، گردانندگان REvil با ادعای اینکه قربانی بدون پرداخت باج در حال خروج از مذاکرات است، مسئولیت و ادامه مذاکرات را بر عهده می‌گیرد. گردانندگان REvil مذاکرات خود را با قربانی ادامه داده و باج را بصورت کامل بدون پرداخت سهم شرکای خود دریافت می‌کنند.

اخیراً، این ادعاها اهمیت بیشتری پیدا کرده است زیرا یک مهندس معکوس بدافزار زیرزمینی، شواهدی از رمزگشایی دوگانه REvil (Double-dipping practices) در فایل‌های قربانیان ارائه کرده است. این افشاگری پس از آن صورت می‌گیرد که شرکت امنیت سایبری بیت‌دیفندر (Bitdefender) اقدام به انتشار یک ابزار رمزگشای اصلی برای قربانیان REvil نمود.

در یکی از تالارهای گفتگو که در تصویر نشان داده شده نویسنده متن ادعا نموده که مشترکان RaaS، تنها کسانی نیستند که می‌توانند سیستم‌هایی را که با نمونه باج‌افزار REvil رمزگذاری کرده‌اند، رمزگشایی کنند. گردانندگان REvil نیز یک کلید اصلی دارند که از آنها برای بازیابی فایل‌های رمزگذاری شده استفاده می‌کنند.


کلید عمومی (Public Key) در تصویر بالا به صورت زیر ارائه شده است:

```
FF5EEDCAEDEE6250D488F0F04EFA4C957B557BDBDC0BBCA2BA1BB7A64D043A3D
```

بازیابی فایل‌های رمزگذاری شده از طریق کلید اصلی که فقط در اختیار گردانندگان REvil است یا کلید کارزار (campaign key) که مشترکان RaaS آن را در اختیار دارند، امکان‌پذیر است.

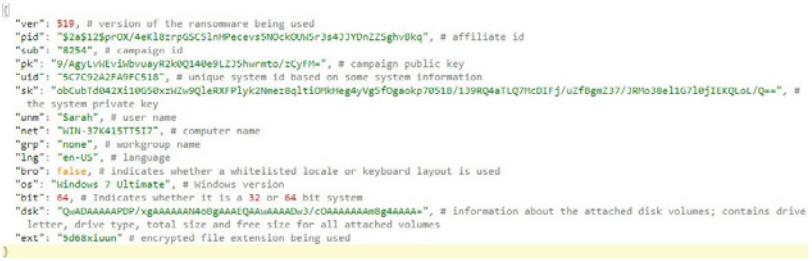
۱۱ تیر ماه، برخی مشتریان شرکت کاسیا (Kaseya, Ltd) که از محصول Kaseya VSA استفاده می‌کردند هدف باج‌افزار REvil قرار گرفتند. VSA از جمله محصولات این شرکت جهت مدیریت از راه دوره شبکه‌ها و نقاط پایانی است. یکی از کاربردهای اصلی VSA فراهم کردن بستری برای مدیریت نقاط پایانی مشتریان شرکت‌های ارائه‌دهنده خدمات پشتیبانی ( Managed Service Provider - به اختصار MSP ) است.

هنگامی که مهاجمان REvil برای مدت محدودی فعالیت خود را متوقف کرده بودند، کاسیا به طرز مرموزی یک رمزگشای اصلی برای حمله خود دریافت کرد که به شرکت‌های ارائه‌دهنده خدمات پشتیبانی و مشتریان آنها اجازه می‌داد فایل‌ها را به صورت رایگان بازیابی و رمزگشایی کنند.

شرکت ضدویروس بیت‌دیفندر نیز چندی پیش ابزار رایگانی منتشر کرد که امکان رمزگشایی فایل‌های رمزگذاری شده را برای قربانیان باج‌افزار REvil، بدون نیاز به پرداخت مبلغ اخاذی شده فراهم می‌کند. بیت‌دیفندر اعلام نمود که این ابزار رمزگشا را با همکاری یک نهاد قانونی ایجاد و منتشر کرده است. به نقل از بیت‌دیفندر، قربانیانی که REvil قبل از ۲۲ تیر آنها را مورد حمله قرار داده و فایل‌های آنها را رمزگذاری نموده است، می‌توانند جهت رمزگذاری فایل‌هایشان از این رمزگشا استفاده کنند.

بیت‌دیفندر درآن زمان عنوان نمود که نمی‌تواند جزئیات مربوط به نحوه دستیابی به کلید رمزگشایی اصلی یا نهاد قانونی مذکور را به اشتراک بگذارد. به نظر می‌رسد کلیدی که بیت‌دیفندر در ابزار رمزگشای خود از آن استفاده کرده، همان کلید اصلی باشد و احتمالاً همان چیزی است که به قربانیان Kaseya کمک می‌کند تا فایل‌ها را به صورت رایگان بازیابی کنند. احتمال دارد که دریافت کلید رمزگشایی REvil برای مشتریان کاسیا نیز به تحقیقات نهاد قانونی مذکور مرتبط باشد.

مهاجمان باج‌افزاری برای دسترسی به پرتال پرداخت REvil، به بخشی از اطلاعات موجود در اطلاعیه باج‌گیری (Ransom note) نیاز دارند. این رشته از کاراکترهای ظاهراً بی‌معنی شامل داده‌های مختلفی همچون نوع سیستم، حمله، نسخه بدافزار مورد استفاده و کلید خصوصی است.




اخیراً گروه‌های باج‌افزاری جدیدتر از شخصی ماهر به منظور کنترل کامل فعالیت‌های گردانندگان باج‌افزاری و عملیات رمزگشایی سیستم‌های قفل شده استفاده می‌کنند.

مدیر ارشد فناوری امسی‌سافت (Emsisoft, Ltd) خاطرنشان می‌کند که به نقل از گردانندگان REvil، کلید اصلی نوعی تضمین در برابر شرکای آنان است و آنها نیاز به توضیح ندارند و حق مذاکرات با قربانی را در هر مرحله‌ای برای خود محفوظ نگه می‌دارند.

مدیر ارشد فناوری امسی‌سافت در ادامه خاطرنشان می‌کند که شایعه شده بود که گروه باج‌افزار DarkSide نیز حملات خود را به این شیوه اجرا می‌کنند.

# ادغام McAfee Enterprise و FireEye؛
## آغاز فصلی جدید در دنیای امنیت سایبری


ادغام دو شرکت McAfee Enterprise و FireEye رسما آغاز شده و در آینده‌ای نزدیک این دو غول دنیای امنیت سایبری تحت عنوان یک شرکت واحد، قدرتمندتر از قبل به ده‌ها هزار مشتری خود در کشورهای مختلف خدمات‌دهی خواهند کرد.

در ماه مارس شرکت McAfee خدمات و محصولات سازمانی خود را به مبلغ ۴ میلیارد دلار به Symphony Technology Group - به اختصار STG - واگذار کرد که منجر به ظهور شرکت جدید McAfee Enterprise شد.

در ماه ژوئیه نیز، FireEye از فروش محصولات این شرکت به STG به قیمت ۱.۲ میلیارد دلار خبر داد.

اکنون با ادغام محصولات McAfee Enterprise و FireEye و تشکیل شرکتی با بیش از ۵ هزار کارمند باید شاهد آغاز فصلی جدید در دنیای امنیت سایبری باشیم.

این نقل‌وانتقال عظیم در حالی صورت می‌گیرد که اجرای مستمر حملات مخرب، پیچیده و گسترده، کسب‌وکار تبهکاران سایبری را پررونق‌تر از همیشه کرده است. اخاذی‌های چندمیلیون دلاری از شرکت‌ها و سازمان‌های مطرح توسط گردانندگان باج‌افزار و اجرای حملات فوق‌حرفه‌ای نظیر آن چه که در حمله زنجیره تأمین (Supply Chain) به SolarWinds و در پی آن تسخیر هزاران مشتری این شرکت شاهد بودیم نمونه‌هایی کوچک از این اتفاقات است.

راهکارهای شرکت McAfee Enterprise موسوم به "از دستگاه تا ابر" (Device-to-Cloud) و ترکیب آنها با محصولات قدرتمند و اختصاصی FireEye فرصتی طلایی برای مقابله با نفوذگران و مهاجمانی است که چند سال اخیر همواره از ارائه‌دهندگان راهکارهای امنیتی یک قدم جلوتر بوده‌اند.

نگاهی به محصولات دو شرکت McAfee Enterprise و FireEye نشان می‌دهد که محصولات متنوع آنها در نقش مکمل یکدیگر موجب ظهور نسل جدیدی از راهکارها در حوزه‌های مختلف از جمله امنیت سرورها و نقاط پایانی، امنیت بسترهای رایانش ابری، جلوگیری از نشت داده‌ها (DLP) و مدیریت عملیات‌های امنیتی خواهد شد.

پیش‌بینی می‌شود سود سالیانه شرکت جدید ۲ میلیارد دلار باشد.

همراه با تکمیل مراحل ادغام دو شرکت و تحولات آتی، اطلاع رسانی در این زمینه ادامه خواهد داشت.

# تعطیلی مجدد

## باج‌افزار REvil


در پی حملات موسوم به Hijacking در درگاه پرداخت Tor و سایت نشت‌داده‌های باج‌افزار REvil، فعالیت این باج‌افزار برای بار دیگر متوقف شده است.

گروه باج‌افزاری REvil که در نیمه اول سال ۲۰۱۹ ظاهر شد، با نام‌های Sodin و Sodinokibi نیز شناخته می‌شود. تصور می‌شود که این گروه جانشین گروه باج‌افزاری GandCrab است که البته اکنون دست از فعالیت کشیده است. REvil نام باج‌افزاری است که در قالب خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) به سایر مهاجمان فروخته می‌شود و توانسته طرفداران زیادی را در بازارهای زیرزمینی تبهکاران سایبری به خود جلب کند.

در خدمات 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 از قربانی به نویسنده باج‌افزار و بخشی دیگر به متقاضی سرویس می‌رسد.

از زمان راه‌اندازی REvil در سال ۲۰۱۹، این باج‌افزار حملات متعددی را علیه شرکت‌های معروفی انجام داده است.

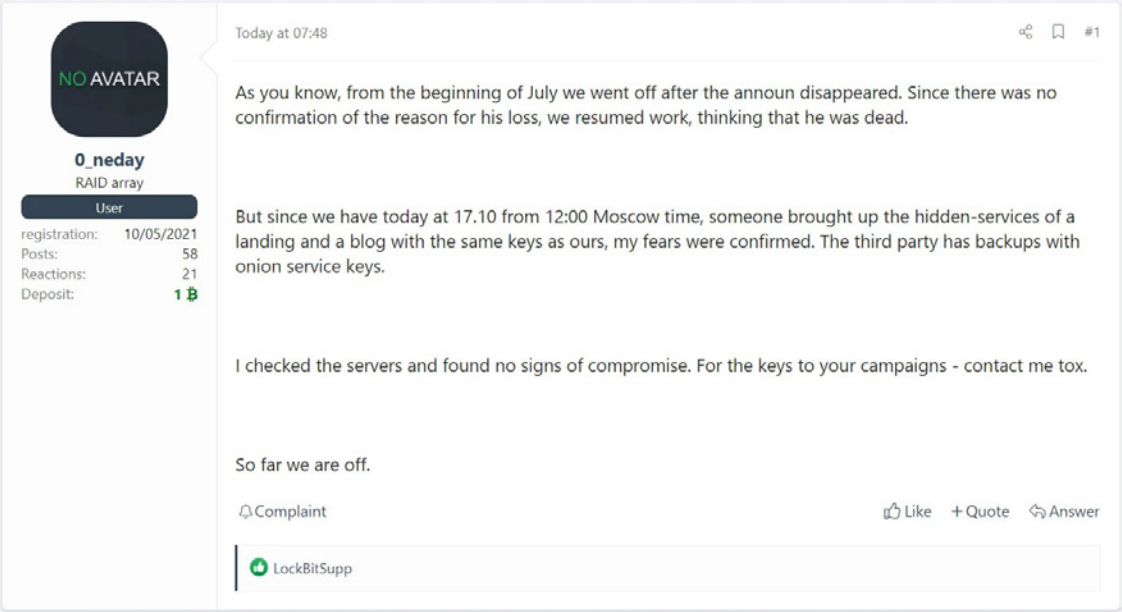
پس از آن در ۲۲ تیر ۱۴۰۰، گردانندگان REvil به طرز مرموزی سایت‌های پرداخت باج را غیرفعال و به طور موقت زیرساخت‌های مخرب خود را از کار انداختند. برخی منابع احتمال می‌دادند که این اتفاقات در نتیجه مذاکرات کاخ سفید با مسکو در مورد لزوم توقف حملات باج‌افزاری مهاجمان روسی به سازمان‌ها و زیرساخت‌های آمریکا رخ داده و فشار دولت روسیه عامل اصلی تعطیلی REvil بوده است.

اما مدتی بعد این باج‌افزار در اوایل شهریور ماه حملات خود را مجدد از سر گرفت و شرکت ضدویروس بیت‌دیفندر (Bitdefender) نیز در همان ماه ابزار رایگانی را که فایل دستورالعمل آن در نشانی زیر قابل دریافت است، منتشر کرد.

https://www.nomoreransom.org/uploads/REvil_documentation.pdf

ابزار رمزگشای مذکور، امکان رمزگشایی فایل‌های رمزگذاری شده را برای همه قربانیان REvil که فایل آنها قبل از ۲۲ تیر رمزگذاری شده بود، بدون نیاز به پرداخت مبلغ اخاذی شده فراهم می‌کرد. بیت‌دیفندر این ابزار رمزگشا را با همکاری یک نهاد قانونی ایجاد و منتشر کرده بود. این ابزار قادر بود کل کامپیوتر را به طور همزمان رمزگشایی نموده یا پوشه‌های خاصی را که مشخص شده، رمزگشایی کند.

بنا به گزارش یکی از محققان شرکت رکوردد فیوچر (Recorded Future, Inc.)، باج‌افزار REvil که در اوایل شهریور ماه حملات خود را مجدد از سر گرفته بود، در اوایل روز ۲۵ مهر ماه، سایت Tor و دامنه آن (onion domains)، توسط مهاجمانی ناشناس از طریق کلیدهای خصوصی (Private Key) این باج‌افزار مورد حمله موسوم به XSS Hijacking قرار گرفته و احتمالاً مهاجمان از سایت‌های آن نیز نسخه پشتیبان تهیه کرده‌اند.



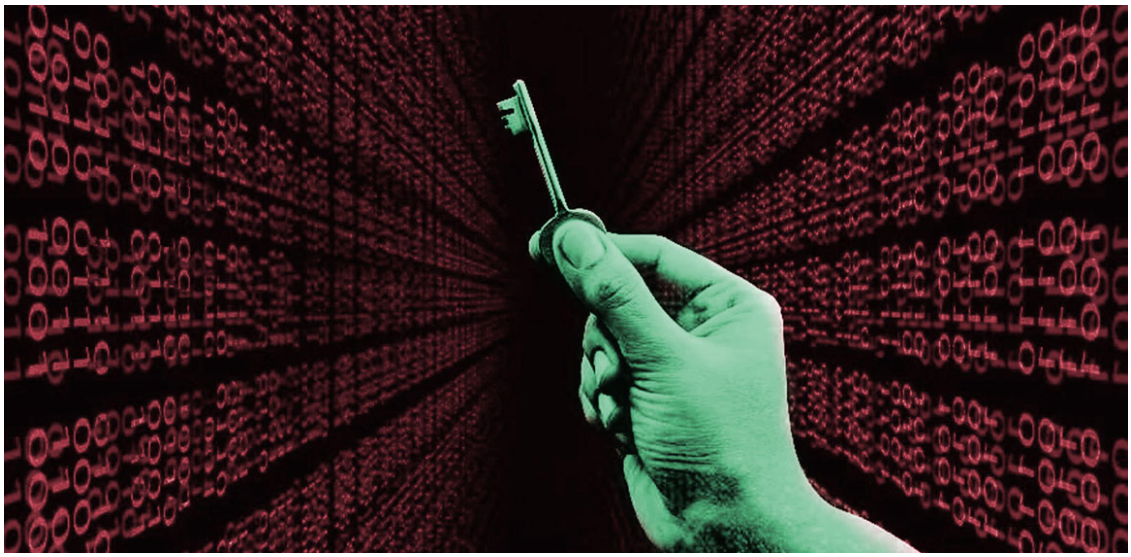

برای راه‌اندازی سرویس Tor (یک دامنه onion.) باید یک جفت کلید خصوصی و عمومی که جهت راه‌اندازی اولیه سرویس نیز استفاده می‌شود، ایجاد شود. کلید خصوصی باید مخفی بماند و فقط در اختیار کاربران قابل اعتماد با سطح دسترسی بالا قرار گیرد، زیرا هرکسی که این کلید را در اختیار داشته باشد می‌تواند از آن برای راه‌اندازی همان سرویس onion. در سرور خود استفاده کند.

از آنجا که اکنون دامنه‌ها مورد حمله Hijacking قرار گرفته‌اند، به این معنی است که مهاجمان به کلیدهای خصوصی این سرویس دسترسی دارند. البته هنوز جزییات این حمله برای کسی روشن نیست و مشخص نشده که چه کسی سرورهای این باج‌افزار را مورد حمله قرار داده است. لذا این احتمال نیز وجود دارد که مهاجمان سعی کنند کنترل حمله را مجدد به دست آورند.

پس از ازسرگیری فعالیت‌های REvil، نویسندگان این باج‌افزار برای جذب کاربران با مشکل روبرو شده‌اند، تا جایی که میزان کمیسیون‌های شرکای خود (متقاضیان خدمات RaaS) را تا ۹۰ درصد افزایش داده‌اند تا سایر تبهکاران سایبری را ترغیب به همکاری با خود کنند.

احتمال می‌رود در پی حملات موسوم به Hijacking در درگاه پرداخت Tor و سایت نشت‌داده‌های باج‌افزار REvil، فعالیت این باج‌افزار برای همیشه متوقف شده باشد. با این حال، در مورد باج‌افزارها هیچ خبر خوشی برای همیشه دوام نمی‌آورد و احتمالاً به زودی شاهد تغییر نام این باج‌افزار در قالب حملات جدیدی خواهیم بود.

# خبر خوش برای
## قربانیان باج‌افزار BlackByte

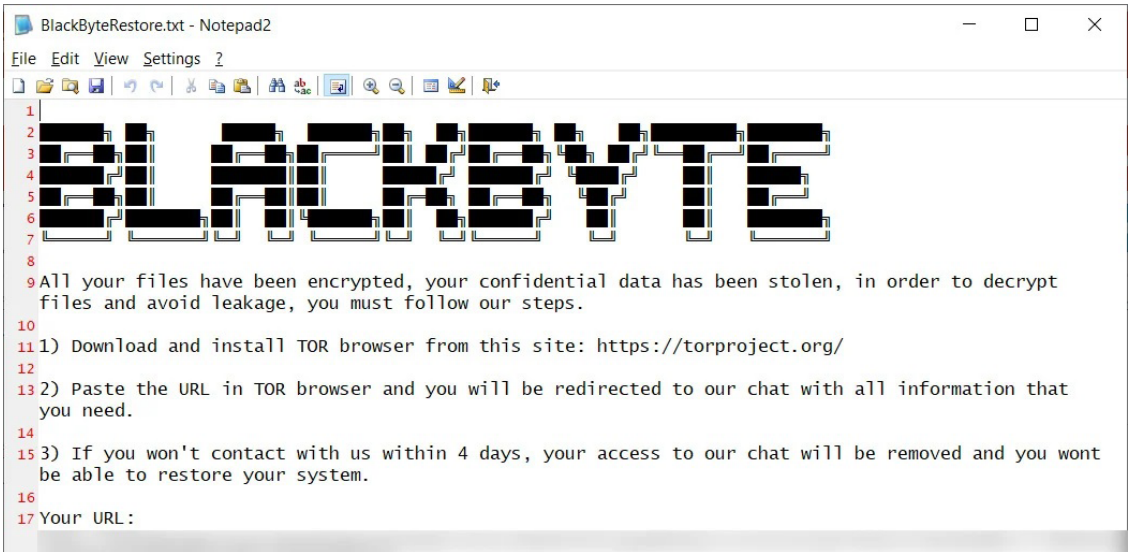


به تازگی کلید رمزگشایی باج‌افزار BlackByte منتشر شده که به قربانیان قبلی این باج‌افزار اجازه می‌دهد فایل‌های خود را به صورت رایگان بازیابی کنند.

BlackByte یک گروه باج‌افزاری است که از اوایل ژوئیه ۲۰۲۱ شروع به هدف قرار دادن شرکت‌هایی از سراسر جهان کرده است. اولین گزارش آلودگی توسط این باج‌افزار در ۲۸ تیر ۱۴۰۰ در تالار گفتگویی به آدرس زیر انتشار یافت. در تالار مذکور، قربانیان برای رمزگشایی فایل‌های خود درخواست کمک نموده بودند.

https://www.bleepingcomputer.com/forums/t/755181/blackbyte-ransomware-blackbyte-support-topic/

تصویر زیر اطلاعیه باج‌گیری (Ransom Note) این باج‌افزار را نمایش می‌دهد.




BlackByte به زبان C# نوشته شده و سعی می‌کند بسیاری از فرآیندهای امنیتی، سرور ایمیل (Mail Server) و پایگاه‌داده‌ها را به منظور رمزگذاری موفق سیستم‌ها، از کار بیندازد. همچنین این باج‌افزار قبل از اقدام به رمزگذاری فایل‌ها، Microsoft Defender را در سیستم‌های قربانیان غیرفعال می‌کند.

اکثر باج‌افزارها پس از اجرا، کلید رمزگذاری منحصر به فردی برای هر فایل یا یک کلید واحد برای هر سیستم ایجاد می‌کنند که از آن‌ها به عنوان کلیدهای Session نام برده می‌شود و برای رمزگذاری سیستم قربانی بکار گرفته می‌شود. این کلیدها سپس با یک کلید RSA عمومی رمزگذاری شده و به انتهای یک فایل رمزگذاری شده یا اطلاعیه باج‌گیری اضافه می‌شوند. حال، این کلید رمزگذاری شده را فقط می‌توان با کلید رمزگشایی خصوصی (Private Key) مرتبط که فقط در اختیار گروه باج‌افزاری قرار دارد، رمزگشایی کرد. مهاجمان از این طریق می‌توانند در صورت پرداخت باج توسط قربانی، کلیدهای رمزگذاری شده را رمزگشایی کنند.

محققان تراست‌ویو هلدینگز (Trustwave Holdings, Inc.) عنوان نموده‌اند که سایر گروه‌های باج‌افزاری از فرآیند رمزنگاری پیچیده‌تری استفاده می‌کنند و رمزنگاری باج‌افزار BlackByte نسبت به سایر باج‌افزارها بسیار ساده‌تر است.

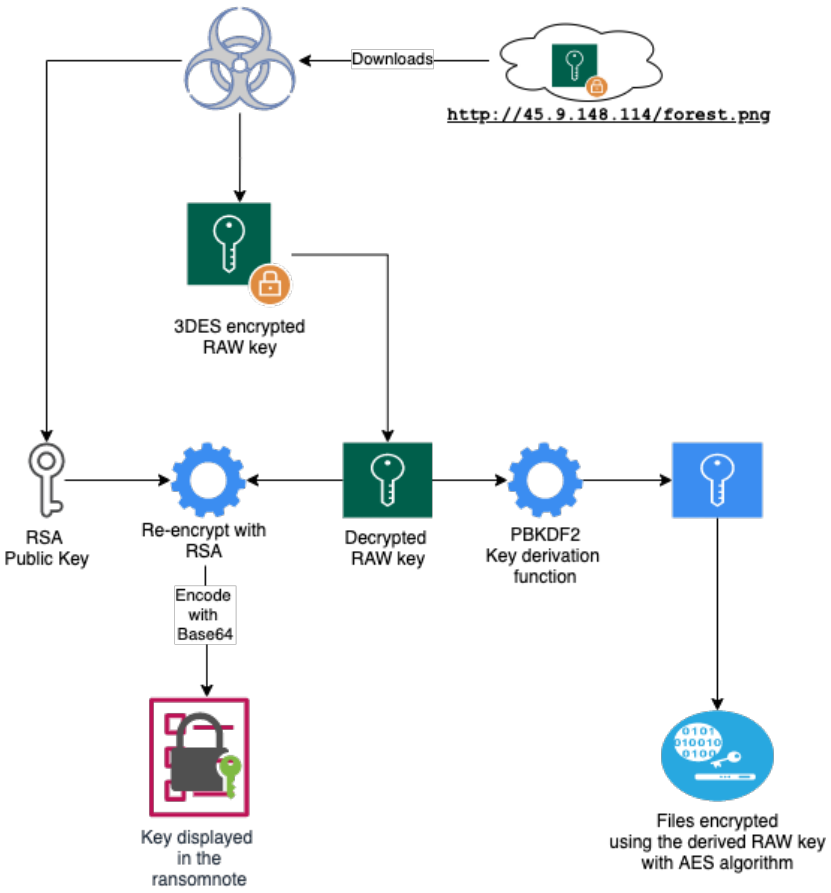
این محققان در تحقیقات خود به این نکته پی برده‌اند که این باج‌افزار فایلی به نام "forest.png" را از یک سایت از راه دور که تحت کنترل آن‌هاست، دانلود می‌کند. نامگذاری فایل مذکور به گونه‌ای است که یک فایل تصویری به نظر برسد، ولی در واقع حاوی کلید رمزگذاری AES است که برای رمزگذاری یک سیستم از آن استفاده می‌شود.

به گفته محققان، فایل تصویری جعلی مذکور، حاوی یک کلید رمزنگاری "Raw" است که باج‌افزار از آن برای استخراج کلیدها جهت رمزگذاری سیستم و فایل‌های قربانی استفاده می‌کند و سپس یک کلید دسترسی ایجاد کرده تا دسترسی قربانی به درگاه Dark Web جهت مذاکره و باج‌خواهی فراهم شود.

به نظر می‌رسد از آنجایی که BlackByte از رمزگذاری متقارن AES استفاده نموده، برای رمزگذاری و رمزگشایی فایل‌ها کلید مشابهی بکار گرفته شده است.

از طرفی محققان تراست‌ویو به این نکته پی بردند که BlackByte، کلید رمزگذاری AES را که دانلود کرده بود، نیز رمزگذاری کرده و به اطلاعیه باج‌گیری اضافه می‌کند لذا این گروه باج‌افزاری از فایل forest.png مشابه برای چندین قربانی به صورت تکراری استفاده می‌کند.

از آنجایی که از کلید رمزگذاری "Raw" مجدداً استفاده می‌شود، محققان تراست‌ویو توانستند از آن برای ساخت کلید رمزگشایی استفاده



با این حال، همواره یکی از معایب انتشار کلیدهای رمزگشاهای رایگان، این است که به گروه‌های باج‌افزاری اشکالات (Bug) موجود در برنامه‌های آنها را هشدار می‌دهد و آن‌ها به سرعت اقدام به برطرف نمودن آن می‌کنند.

پس از انتشار کلید رمزگشا و گزارش منتشر شده توسط تراست‌ویو، گروه باج‌افزاری BlackByte هشدار دادند که آنها از بیش از یک کلید استفاده کرده‌اند و بکارگیری کلید رمزگشای رایگان مذکور و رمزگشایی با کلید اشتباه منجر به از بین رفتن همیشگی فایل‌های قربانیان می‌شود.

> *"we have seen in some places that there is a decryption for our ransom. we would not recommend you to use that. because we do not use only 1 key. if you will use the wrong decryption for your system you may break everything, and you wont be able to restore your system again.we just want to warn you, if you do decide to use that, its at your own risk." - BlackByte.*


قربانیان این باج‌افزار در صورتی که تمایل دارند از کلید رمزگشایی که توسط تراست‌ویو ارائه شده، استفاده کنند، باید Source Code آن را از Github به آدرس زیر دانلود کرده و خود آن را کامپایل نمایند.

https://github.com/SpiderLabs/BlackByteDecryptor

بعد از انتشار کلید رمزگشای رایگان، این احتمال وجود دارد که BlackByte کلیدهای رمزگذاری را که تراست‌ویو از فایل "forest.png" برای استخراج کلید رمزگشا دانلود کرده، تغییر دهد. به همین دلیل اکیداً توصیه می‌شود قبل از رمزگشایی فایل‌ها از آن‌ها نسخه پشتیبان تهیه شود.

علاوه بر این، اگر فایل "forest.png" روی یک سیستم رمزگذاری شده موجود است، باید از آن فایل به جای فایلی که همراه با رمزگشای تراست‌ویو ارائه شده، استفاده شود.

با این که باج‌افزار BlackByte همانند سایر گروهای باج‌افزاری چندان فعال نیست، آنها حملات بسیاری را با موفقیت در سراسر جهان انجام داده‌اند و نباید آن‌ها را دست کم گرفت.


# آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

# سوءاستفاده مهاجمان
## از آسیب‌پذیری حیاتی وی‌ام‌ور

شرکت وی‌ام‌ور (VMware, Inc) تایید کرده که مهاجمان در حال سوءاستفاده از یک آسیب‌پذیری "حیاتی" (Critical) با شناسه CVE-2021-22005 در محصول vCenter هستند.

شدت این آسیب‌پذیری ۹.۸ از ۱۰ - بر طبق استاندارد CVSSv۳ - گزارش شده است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، جزییات CVE-2021-22005 مورد بررسی قرار گرفته است.

سوءاستفاده از CVE-2021-22005 مهاجم را قادر می‌سازد تا با آپلود یک فایل دستکاری شده بر روی پورت ۴۴۳، اقدام به اجرای کد دلخواه خود بر روی سرور vCenter کند.

۳۰ شهریور، وی‌ام‌ور با انتشار نسخ جدید زیر، CVE-2021-22005 را وصله کرد:

- https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u2c-release-notes.html
- https://kb.vmware.com/kb/85718
- https://docs.vmware.com/en/VMware-vSphere/6.7/rn/vsphere-vcenter-server-67u3o-release-notes.html
- https://kb.vmware.com/kb/85719

همچنین به تازگی، یک محقق ویتنامی، PoC (نمونه کد بهره‌جو) این آسیب‌پذیری را در لینک‌های زیر به‌صورت عمومی منتشر و در دسترس قرار داده است:

https://www.youtube.com/watch?v=WVJ8RDR7Xzs
https://gist.github.com/testanull/c2f6fd061c496ea90ddee151d6738d2e

اگر چه این محقق خاطر نشان کرده که بخش‌های کلیدی از کد را از این PoC حذف کرده تا امکان سوءاستفاده از آن فراهم نباشد اما بررسی‌ها نشان می‌دهد که مهاجمان خیلی زود موفق به تکمیل PoC مذکور و بهره‌جویی از آن شده‌اند.

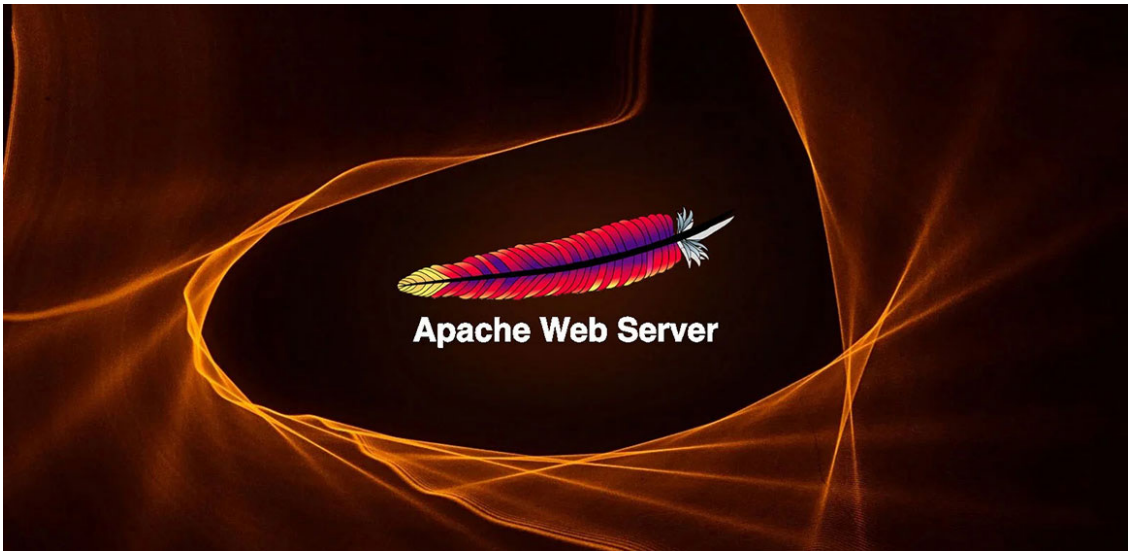
در حال حاضر هزاران سرور vCenter بر روی اینترنت در دسترس قرار دارند و به طور بالقوه می‌توانند از طریق آسیب‌پذیری CVE-2021-22005 مورد سوءاستفاده مهاجمان قرار بگیرند.


به تمامی راهبران بسترهای مجازی‌سازی وی‌ام‌ور توصیه اکید می‌شود تا با مراجعه به راهنمای فنی زیر نسبت به اعمال به‌روزرسانی مربوطه بر روی vCenter اقدام نمایند:

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

# سوءاستفاده مهاجمان

## از دو آسیب‌پذیری روز-صفر آپاچی



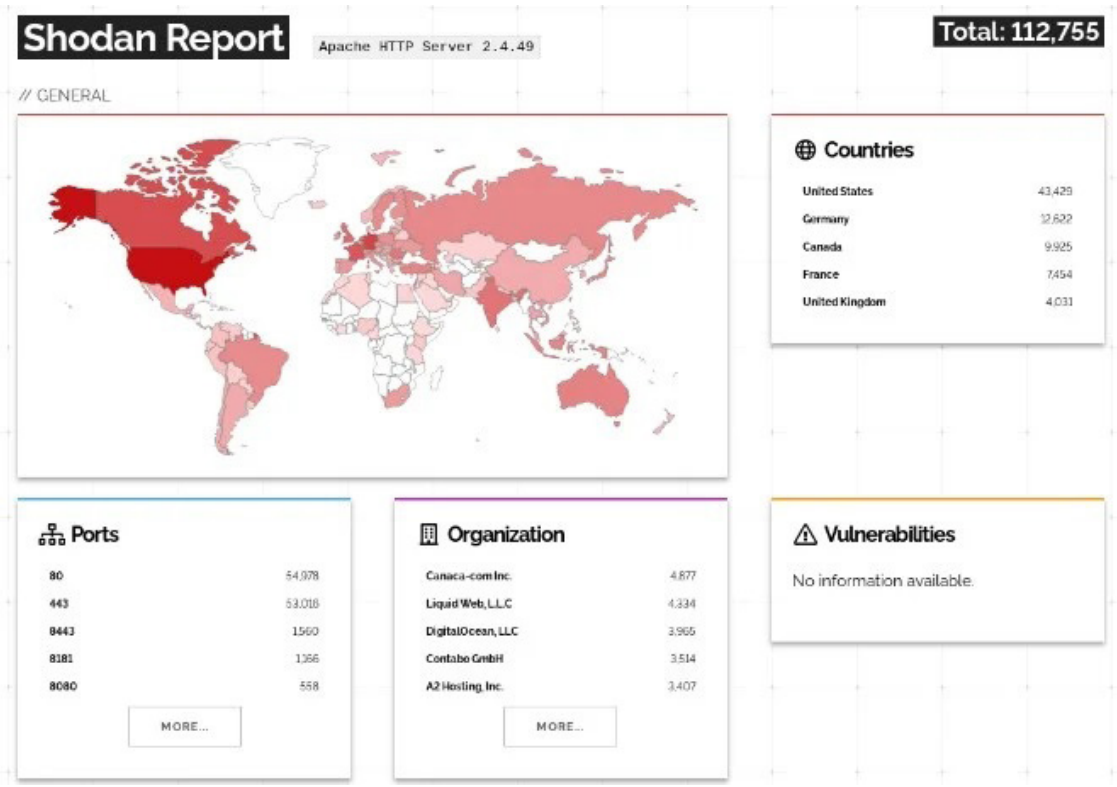

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده جزییات نسخه جدید Apache HTTP Server مورد بررسی قرار گرفته است.

در پی شناسایی وجود یک آسیب‌پذیری در دو نسخه اخیر Apache HTTP Server، بنیاد نرم‌افزاری آپاچی (Apache Software Foundation) با انتشار نسخه‌ای جدید نسبت به وصله آن اقدام کرده است.

Apache HTTP Server یک سرویس‌دهنده وب چندبستری است که در میزبانی حدود ۲۵ درصد از سایت‌های موجود در اینترنت نقش دارد.

۱۲ مهر، بنیاد آپاچی با انتشار نسخه ۲.۴.۵۰ این محصول از ترمیم یک آسیب‌پذیری پویش مسیر (Path Traversal) با شناسه CVE-2021-41773 خبر داد. سوءاستفاده از ضعف مذکور دسترسی به محتوای فایل‌های ذخیره شده بر روی سرور آسیب‌پذیر را برای مهاجمان فراهم می‌کرد. بر اساس توضیحات این بنیاد، تنها نسخه ۲.۴.۴۹ از آسیب‌پذیری CVE-2021-41773 متاثر می‌شود. با این توضیح که بهره‌جویی از آسیب‌پذیری مذکور در صورتی موفق خواهد بود که قابلیت "Require all denied" فعال نباشد. ضمن آنکه سوءاستفاده موفق از CVE-2021-41773 می‌تواند منجر به نشت کد منبع (Source Code) فایل‌هایی نظیر اسکریپت‌های CGI شود.

بر اساس آمار موتور جستجوگر Shodan بیش از ۱۱۲ هزار سرور آسیب‌پذیر Apache HTTP Server بر روی اینترنت قابل دسترس هستند و ممکن است هر یک از آنها مورد نفوذ مهاجمان قرار گرفته یا در آینده‌ای نزدیک قرار بگیرند.




خیلی زود پس از انتشار نسخه ۲.۴.۵۰، محققان امنیتی از آسیب‌پذیری این نسخه جدید خبر دادند و نمونه‌هایی از بهره‌جوهای قابل اجرا نیز بر روی اینترنت در دسترس قرار گرفت. سوءاستفاده از این آسیب‌پذیری جدید که به آن شناسه CVE-2021-42013 تخصیص داده شده می‌تواند در صورت غیرفعال بودن گزینه "Require all denied" منجر به اجرای کد به‌صورت از راه دور بر روی سرور شود.

به منظور وصله کردن این آسیب پذیری روز-صفر جدید، بنیاد آپاچی در ۱۵ مهر ماه اقدام به انتشار نسخه ۲.۴.۵۱ کرد.

بر طبق توصیه‌نامه آپاچی، مهاجم با اجرای یک حمله پویش مسیر می‌تواند در صورت غیرفعال بودن گزینه "Require all denied" با تطابق نشانی‌های URL به فایل‌هایی خارج از پوشه‌های Alias-like دسترسی پیدا کند.

هر دو آسیب‌پذیری CVE-2021-41773 و CVE-2021-42013 توسط مهاجمان در حال بهره‌جویی هستند. لذا به تمامی راهبران Apache HTTP Server توصیه اکید می‌شود که در صورت استفاده از هر یک از نسخ ۲.۴.۴۹ و ۲.۴.۵۰ در اسرع وقت نسبت به ارتقای این محصول به نسخه ۲.۴.۵۱ اقدام کنند.

توصیه‌نامه آپاچی در لینک زیر قابل مطالعه است:

https://httpd.apache.org/security/vulnerabilities_24.html

# Windows 11

## و سازگاری محصولات McAfee Enterprise و Bitdefender


بر طبق اعلام قبلی شرکت Microsoft، سیستم عامل Windows 11 حدود دو هفته دیگر رسما به‌صورت عمومی عرضه می‌شود.

بر اساس توصیه نامه شرکت McAfee Enterprise محصولات McAfee Agent و McAfee Endpoint Security به ترتیب از نسخه ۵.۷.۴ و September 2021 Update با این سیستم‌عامل جدید سازگار خواهند بود. در خصوص سازگاری سایر محصولات McAfee Enterprise با Windows 11 مطالعه راهنمای فنی زیر توصیه می‌شود:

https://kc.mcafee.com/corporate/index?page=content&id=KB94901

ضمن اینکه محصولات McAfee Agent و McAfee Endpoint Security به ترتیب از نسخه ۵.۷.۳ و June 2021 Update با سیستم عامل Windows Server 2022 که حدود دو ماه از عرضه رسمی آن می‌گذرد سازگار شده‌اند. جزییات کامل در خصوص سازگاری محصولات McAfee Enterprise با Windows Server 2022 در راهنمای فنی زیر قابل مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=KB94790

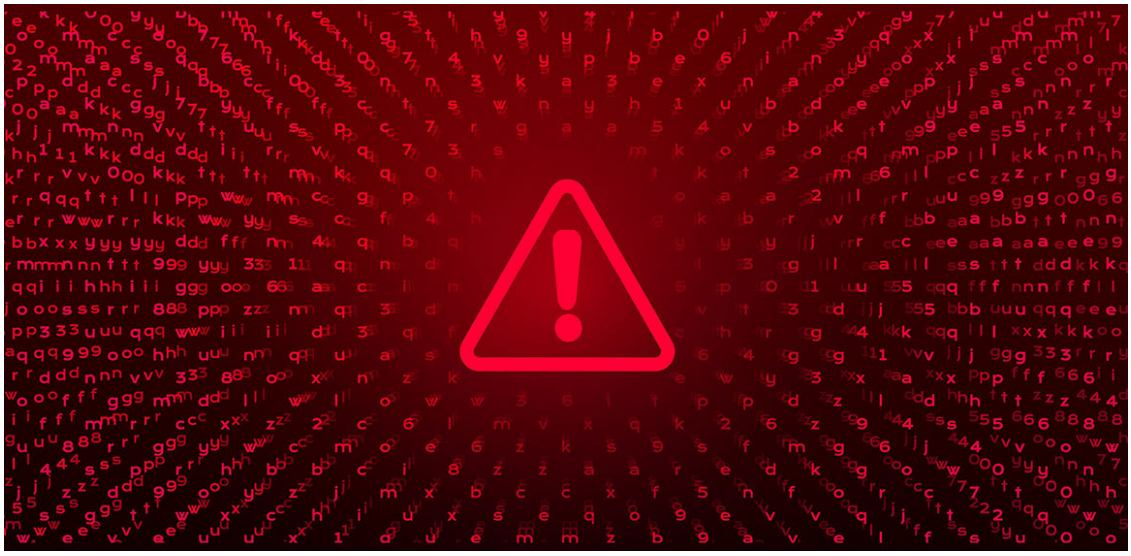
مشترکین محصولات سازمانی Bitdefender در ایران نیز آگاه باشند که نسخه ۷.۲.۲.۹۲ نرم‌افزار Bitdefender Endpoint Security Tools و نسخ بعد از آن با Windows 11 و Windows Server 2022 سازگار اعلام شده است.

همچنین بر طبق اعلام شرکت McAfee Enterprise، از اکتبر ۲۰۲۱. برخی امضاهای شناسایی تهدیدات مبتنی بر Exploit از ماژول ENS Exploit Prevention و محصول Host IPS حذف خواهد شد. امضاهای مذکور مربوط به شناسایی آن دسته کدهای Exploit است که تنها سیستم‌های عامل از رده خارج Vista، XP و Server 2003 از آنها متأثر می‌شوند. جزییات بیشتر و فهرست امضاهای مذکور در مقاله فنی زیر قابل دسترس است:

https://kc.mcafee.com/corporate/index?page=content&id=KB94952

لازم به ذکر است که در دی ماه ۱۳۹۸، پشتیبانی Microsoft از سیستم‌های عامل Windows 7 و Windows Server 2008/2008 R2 و عرضه عمومی اصلاحیه‌های امنیتی برای آنها توسط این شرکت پایان یافت. لذا به تمامی راهبرانی که همچنان از این سیستم‌های عامل از رده خارج استفاده می‌کنند توصیه اکید می‌شود که در اسرع وقت اقدام به ارتقای دستگاه‌های با Windows 7 و Windows Server 2008 R2 خود به نسخ جدیدتر و قابل پشتیبانی کنند.

# سوءاستفاده تبهکاران سایبری
## از آسیب‌پذیری‌های قدیمی



محققان امنیتی شرکت کوالیس (Qualys, Inc.) حملات بزرگ باج‌افزاری را در پنج سال گذشته به طور کامل مطالعه کرده و مشخص کرده‌اند که در این حملات حدوداً ۱۱۰ ضعف امنیتی (CVE) مورد سوءاستفاده قرار گرفته است. آن‌ها دریافتند که برای اکثر این ۱۱۰ ضعف امنیتی، توصیه‌نامه یا وصله‌ای از طرف شرکت مربوطه ارائه شده است.

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

تحلیل بیشتر محققان این شرکت نشان می‌دهد که علاوه بر بهره‌جویی از ضعف‌های امنیتی معروف و شناخته شده، مهاجمان از برخی آسیب‌پذیری‌های بسیار قدیمی نیز برای توزیع باج‌افزار سوءاستفاده می‌کنند. ضعف‌های امنیتی قدیمی، خصوصاً در سیستم‌های متصل به اینترنت، مورد علاقه مهاجمان هستند. ازآنجایی که بسیاری از سازمان‌ها اعمال به روزرسانی‌های امنیتی را مورد توجه قرار نمی‌دهند، مهاجمان همچنان در حال سوءاستفاده از آن‌ها می‌باشند.

محققان کوالیس فهرستی از پنج آسیب‌پذیری را که بیشتر از سایر ضعف‌های امنیتی در حملات باج‌افزاری سال‌های اخیر مورد سوءاستفاده قرار گرفته، ارائه کرده‌اند. این پنج ضعف امنیتی علی‌رغم قدیمی بودن همچنان بسیاری از سازمان‌های مختلف را به علت بی‌توجهی در اعمال به‌روزرسانی‌های امنیتی در سراسر جهان در معرض خطر قرار داده است. جدول زیر پنج CVE را که در حملات باج‌افزارهای معروف بیشترین بهره‌جویی از آن‌ها صورت گرفته، نمایش می‌دهد.

| CVE | Used by Ransomware Family | Patch Available from Vendor | Patch Available Since | Patchable From Qualys |
|---|---|---|---|---|
| CVE-2013-1493 | Exxroute | Yes | March 2013 | Yes |
| CVE-2013-0431 | Reveton | Yes | February 2013 | Yes |
| CVE-2012-1723 | Urausy | Yes | June 2012 | Yes |
| CVE-2019-1458 | NetWalker | Yes | December 2019 | Yes |
| CVE-2018-12808 | Ryuk/Conti | Yes | August 2018 | Yes |

براساس گزارشی که این شرکت ارائه داده، برخی از این ضعف‌های امنیتی تقریباً یک دهه است که شناخته شده‌اند و وصله‌های آن‌ها نیز توسط شرکت‌های مرتبط در دسترس قرار گرفته است. اما از آنجا که بسیاری از سازمان‌ها هنوز به‌روزرسانی‌های امنیتی موجود را اعمال نکرده‌اند، همچنان در برابر حملات باج‌افزاری آسیب‌پذیر هستند.

قدیمی‌ترین آسیب‌پذیری که توسط این محققان مورد بررسی قرار گرفته دارای شناسه CVE-2012-1723 است؛ این ضعف‌امنیتی که تاریخ شناسایی آن به سال ۲۰۱۲ برمی‌گردد، Java Runtime Environment - به اختصار JRE را متاثر می‌کند. سوءاستفاده از این آسیب‌پذیری منجر به "دسترسی از راه دور" و دانلود و نصب فایل‌های بدافزاری مهاجم بر روی سیستم قربانی می‌شود.

به گفته محققان، از آسیب‌پذیری مذکور معمولاً برای توزیع باج‌افزار Urausy سوءاستفاده می‌شود. این باج‌افزار علی‌رغم عملکرد ساده خود موفق به آلوده‌سازی تعداد قابل توجهی از سازمان‌ها به دلیل عدم استفاده از وصله امنیتی مربوطه که حدود یک دهه از انتشار آن می‌گذرد، شده است.

CVE-2013-0431 و CVE-2013-1493 دو آسیب‌پذیری رایج دیگری هستند که اصلاحیه آنها از سال ۲۰۱۳ در دسترس قرار گرفته است. CVE-2013-0431 یک آسیب‌پذیری در JRE بوده که بارها توسط باج‌افزار Reveton مورد سوءاستفاده قرار گرفته است.

CVE-2013-1493 نیز یک ضعف امنیتی در Oracle Java است که باج‌افزار Exxroute آن را مورد هدف قرار می‌دهد. آسیب‌پذیری CVE-2013-1493 برای اولین بار در فوریه ۲۰۱۳ به عنوان یک ضعف امنیتی از نوع "روز صفر" کشف شد. سپس شرکت اورکل (Oracle Corporation) توصیه‌نامه‌ای و در ادامه اصلاحیه‌ای برای آن منتشر کرد.

CVE-2018-12808 نیز آسیب‌پذیری دیگری است که در گزارش کوالیس به آن اشاره شده است. سوءاستفاده از این آسیب‌پذیری سه ساله که Adobe Acrobat از آن متاثر می‌شود، تبهکاران سایبری را قادر به انتشار باج‌افزار از طریق ایمیل‌های فیشینگ و فایل‌های مخرب PDF کرده است. باج‌افزار Ryuk و باج‌افزار Conti که آن را جایگزین یا نسخه جدید Ryuk می‌دانند نیز از این روش در حملات خود استفاده می‌کنند. ضعف امنیتی مذکور از نوع "اجرای کد دلخواه" (Arbitrary Code Execution) بوده و شدت آن "حیاتی" (Critical) گزارش شده است. جزییات بیشتر در نشانی زیر قابل مطالعه است.

https://helpx.adobe.com/security/products/acrobat/apsb18-29.html

جدیدترین آسیب‌پذیری در فهرست مذکور CVE-2019-1458 است که اشکالی از نوع "ترفیع امتیازی" (Privilege Escalation) در بخش Win 32k سیستم‌عامل Windows است و در دسامبر ۲۰۱۹ جزییات آن توسط شرکت مایکروسافت (Microsoft Corp.) در نشانی زیر منتشر شد. بهره‌جویی از آسیب‌پذیری مذکور، مهاجم را قادر به ارتقای دسترسی خود در سطح هسته (Kernel) بر روی دستگاه می‌کند.

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-1458

آسیب‌پذیری مذکور توسط گروه باج‌افزاری NetWalker مورد سوءاستفاده قرار می‌گیرد.

مهاجمان سایبری به طور فعال در حال بررسی و شناسایی آسیب‌پذیری‌هایی هستند که امکان اجرا و استقرار کدهای باج‌افزاری و دیگر تهدیدات سایبری را برای آن‌ها فراهم می‌کند. از این‌رو تا زمانی که به‌روزرسانی‌ها و وصله‌های موجود اعمال نشوند، تبهکاران سایبری قادر به سوءاستفاده از آن‌ها و ادامه حملات موفق خود هستند.

گزارش محققان حاکی از آن است که میانگین زمان صرف شده جهت رفع آسیب‌پذیری‌های مهم از ۱۹۷ روز در آوریل ۲۰۲۱ به ۲۰۵ روز در می ۲۰۲۱ افزایش یافته است. امسال نیز محققان کوالیس در گزارش خود اعلام نموده‌اند که به طور متوسط ۱۹۴ روز از زمانی که یک ضعف امنیتی در سیستم‌های سازمان کشف می‌شود تا زمانی که همه موارد وصله می‌شوند زمان می‌برد.

سازمان‌ها باید فوراً این آسیب‌پذیری‌ها را اولویت‌بندی و وصله‌های لازم را اعلام کنند، به ویژه در سیستم‌ها، پایگاه‌داده‌ها و زیرساخت‌های حیاتی متصل به اینترنت که اولین هدف مهاجمان هستند. تیم‌های امنیتی باید همواره زمانی را برای مدیریت آسیب‌پذیری و اعمال به‌روزرسانی‌های امنیتی مهم اختصاص دهند، به ویژه اگر مشخص شود که ضعف‌های مذکور توسط تبهکاران سایبری مورد سوءاستفاده قرار گرفته است. مدیریت آسیب‌پذیری ترکیبی از ارزیابی ضعف‌های امنیتی، اولویت‌بندی آن‌ها و اعمال وصله‌های مربوطه است.

مشروح گزارش کوالیس در لینک زیر قابل مطالعه است:

https://blog.qualys.com/product-tech/2021/10/05/assess-risk-ransomware-attacks-qualys-research

# به‌روزرسانی‌ها و اصلاحیه‌های

## مهر ۱۴۰۰


### مایکروسافت

سه‌شنبه ۲۰ مهر، شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی اکتبر منتشر کرد. اصلاحیه‌های مذکور بیش از ۷۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند.

درجه اهمیت ۳ مورد از آسیب‌پذیری‌های ترمیم شده این ماه "حیاتی" (Critical) و تقریباً دیگر موارد "مهم" (Important) اعلام شده است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به برخی از با اهمیت‌ترین اصلاحیه‌های ماه اکتبر مایکروسافت پرداخته شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را به شرح زیر در محصولات مختلف مایکروسافت ترمیم می‌کنند:

- "ترفیع امتیازی" (Elevation of Privilege)
- "اجرای کد به صورت از راه دور" (Remote Code Execution)
- "افشای اطلاعات" (Information Disclosure)
- "جعل" (Spoofing)
- "عبور از سد امکانات امنیتی" (Security Feature Bypass)
- "منع سرویس" (Denial of Service - به اختصار DoS)

۴ مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع "روز-صفر" (شناسه‌های CVE-2021-41335، CVE-2021-40469، CVE-2021-41338، CVE-2021-40449) می‌باشند. 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.

اولین ضعف امنیتی "روز-صفر" که در این ماه ترمیم شده، دارای شناسه CVE-2021-40449 بوده که سوءاستفاده از آن به تعامل کاربر نیازی ندارد و قابلیت "ترفیع امتیازی" را برای بدافزارها یا مهاجم در نسخه‌های مختلف سیستم‌عامل Windows (از طریق Win32k Kernel driver) فراهم می‌کند. آسیب‌پذیری مذکور به طور فعال مورد سوءاستفاده قرار گرفته و دارای درجه شدت ۷/۸ از ۱۰ می‌باشد.

این ضعف امنیتی از یک آسیب‌پذیری در راه‌انداز Win32k که در گذشته ناشناخته بوده، استفاده می‌کند و بهره‌جویی از آن تا حد زیادی به تکنیکی برای نشت آدرس‌های اصلی ماژول‌های Kernel متکی است.

شرکت کسپرسکی (.Kaspersky Lab) در گزارش خود که جزییات کامل آن در نشانی زیر ارائه شده، اعلام نموده که این آسیب‌پذیری توسط مهاجمان در "کمپین‌های گسترده جاسوسی علیه شرکت‌های فناوری اطلاعات، پیمانکاران نظامی/دفاعی و نهادهای دیپلماتیک" استفاده شده است.

https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

در بخشی از حملات، بکارگیری و نصب بدافزارهای موسوم به Remote Access Trojan - به اختصار RAT - توسط مهاجمان، منجر به سوءاستفاده از آسیب‌پذیری روز صفر مذکور در Windows و ارتقاء سطح دسترسی شده بود. محققان کسپرسکی این نوع فعالیت بدافزاری را MysterSnail نامگذاری کرده‌اند و به علت شباهت کد و استفاده مجدد از زیرساخت کنترل و فرمان‌دهی (C2) آن را به مهاجمان IronHusky و تهدیدات مستمر و پیشرفته (Advanced Persistent Threat - به اختصار APT) چینی مرتبط با ۲۰۱۲ نسبت داده‌اند.

دستیابی به سطح دسترسی بالا در سیستم‌های آسیب‌پذیر اولین قدم برای تبدیل شدن به یک مدیر دامنه و اطمینان از دسترسی کامل به شبکه یک سازمان است. از آنجایی که مهاجمان در حال حاضر از این ضعف امنیتی جهت نفوذ به سازمان‌ها و به دست آوردن سطح دسترسی بالا (Administrator) استفاده می‌کنند، راهبران امنیتی باید وصله این آسیب‌پذیری را در اولویت قرار دهند.

دیگر ضعف امنیتی از نوع "روز-صفر" این ماه، آسیب‌پذیری با شناسه CVE-2021-41338 است که "عبور از سد امکانات امنیتی" را در Windows AppContainer Firewall برای مهاجم فراهم می‌کند و درجه شدت آن ۵/۵ از ۱۰ است.

سومین ضعف‌امنیتی ازنوع "روز-صفر" این ماه، آسیب‌پذیری با شناسه CVE-2021-40469 می‌باشد که مربوط به Windows DNS و از نوع "اجرای کد از راه دور" است. درجه شدت ضعف امنیتی مذکور ۷/۲ از ۱۰ می‌باشد.

آخرین آسیب‌پذیری "روز-صفر" ترمیم شده در این ماه، ضعفی با درجه شدت ۷/۸ از ۱۰ و با شناسه CVE-2021-41335 است که از نوع "ترفیع امتیازی" در Windows Kernel می‌باشد.

CVE-2021-40461 یکی از آسیب‌پذیری حیاتی ماه اکتبر است که با سوءاستفاده از ضعفی در Network Virtualization Service Provider "اجرای کد از راه دور" را بر روی سیستم قربانی برای مهاجم فراهم می‌کند. این آسیب‌پذیری دارای درجه شدت ۸ از ۱۰ می‌باشد.

آسیب‌پذیری حیاتی دیگر، CVE-2021-38672 نیز ناشی از باگی در Windows Hyper-V است و منجر به "اجرای کد از راه دور" بر روی سیستم موردنظر شده و درجه شدت آن نیز مشابه CVE-2021-40461 می‌باشد.

از دیگر آسیب‌پذیری‌های بااهمیت این ماه می‌توان به ضعف امنیتی با شناسه CVE-2021-40486 اشاره کرد که در صورت بهره‌جویی منجر به "اجرای کد از راه دور" می‌شود.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های اکتبر 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/235046/237266/244577/

## سیسکو

شرکت سیسکو (Cisco Systems, Inc) در مهر ماه در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها، ۳۷ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱۵ مورد از آنها از نوع "بالا" (High) و ۲۲ مورد از نوع "متوسط" (Medium) گزارش شده است. آسیب‌پذیری به حملاتی همچون "منع سرویس"، "تزریق کد از طریق سایت" (Cross-Site Scripting)، "ترفیع امتیازی"، "تزریق فرمان" (Command Injection)، "افشای اطلاعات" و "سرریز حافظه" (Buffer Overflow) از جمله مهمترین اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی 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

## مک‌آفی

۲۹ مهر، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) اقدام به انتشار Update 11 نرم‌افزار McAfee ePolicy Orchestrator 5.10 - به اختصار ePO - کرد. در به‌روزرسانی جدید، اصلاحاتی شامل بهینه‌سازی میزان استفاده از حافظه و رفع چند باگ لحاظ شده است. شرکت مک‌آفی اینترپرایز، ارتقای ePO 5.10 به Update 11 را "الزامی" (Mandatory) گزارش کرده است. مشروح اطلاعات فنی به‌روزرسانی مذکور در لینک زیر قابل دریافت است:

https://docs.mcafee.com/bundle/epolicy-orchestrator-5.10.0-release-notes/page/GUID-E4B08A18-77A1-404C-A1D5-D333CA74D77A.html

## وی‌ام‌ور

در ۲ مهر، شرکت وی‌ام‌ور (VMware, Inc) با انتشار توصیه‌نامه‌های امنیتی، نسبت به ترمیم محصولات زیر اقدام کرد:

- VMware Cloud Foundation
- VMware vCenter Server
- VMware vRealize Operations
- VMware vRealize Orchestrator
- VMware vRealize Automation
- VMware vRealize Log Insight
- VMware vRealize Suite Lifecycle Manager

سوءاستفاده از برخی از این ضعف‌های امنیتی ترمیم شده توسط این به‌روزرسانی‌ها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. جزییات بیشتر آن در لینک‌های زیر قابل مطالعه است:

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

https://www.vmware.com/security/advisories/VMSA-2021-0024.html

https://www.vmware.com/security/advisories/VMSA-2021-0023.html

https://www.vmware.com/security/advisories/VMSA-2021-0022.html

https://www.vmware.com/security/advisories/VMSA-2021-0021.html

## اوراکل

۲۷ مهر ۱۴۰۰، شرکت اوراکل (Oracle Corp) مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه به‌روزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۴۱۹ آسیب‌پذیری امنیتی در ده‌ها محصول ساخت این شرکت کرد. سوءاستفاده از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور بدون نیاز به هر گونه اصالت‌سنجی می‌کند. جزییات کامل در خصوص آنها در لینک زیر قابل دریافت است:

https://www.oracle.com/security-alerts/cpuoct2021.html

## ادوبی

در مهر ماه، شرکت ادوبی (Adobe, Inc.) مجموعه اصلاحیه‌های امنیتی ماه اکتبر را منتشر کرد. اصلاحیه‌های مذکور، در مجموع ۱۰ آسیب‌پذیری را در ۶ محصول زیر ترمیم می‌کنند:

- Adobe Acrobat and Reader
- Adobe Connect
- Adobe Acrobat Reader for Android
- Adobe ops-cli
- Adobe Commerce
- Adobe Campaign Standard

بیشترین آسیب‌پذیری ترمیم شده این ماه ادوبی، مرتبط به Adobe Acrobat and Reader با ۴ مورد بوده است. اهمیت ۲ مورد از ضعف‌های امنیتی مذکور "حیاتی" و ۲ مورد "متوسط" اعلام شده است. آسیب‌پذیری‌های "حیاتی" مذکور می‌توانند منجر به "اجرای کد از راه دور" شوند که مهاجم را قادر می‌سازد دستوراتی را در رایانه‌های آسیب‌پذیر اجرا کنند. در حالی که ضعف‌های امنیتی "متوسط" ترمیم شده در Adobe Acrobat and Reader می‌تواند "ترفیع امتیازی" را برای مهاجم فراهم کنند.

به گزارش شرکت مهندسی شبکه گستر، با نصب به‌روزرسانی ماه اکتبر، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۱.۰۰۷.۲۰۰۹۹، نگارش‌های ۲۰۲۰ به ۲۰.۰۰۴.۳۰۰۱۷ و نگارش‌های ۲۰۱۷ آنها به ۱۷.۰۱۱.۳۰۲۰۴ تغییر خواهد کرد.

لازم به ذکر است که تمامی ضعف‌های امنیتی ترمیم شده این ماه به نوعی به تعامل کاربر مانند مرور یک صفحه وب یا باز کردن یک فایل PDF نیاز دارند. اگر چه موردی مبنی بر سوءاستفاده از آسیب‌پذیری‌های ترمیم شده در ۲۰ مهر گزارش نشده، اما ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب به‌روزرسانی‌ها کنند.

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه اکتبر ادوبی در لینک زیر قابل مطالعه است:

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

https://helpx.adobe.com/security/products/acrobat/apsb21-104.html

https://helpx.adobe.com/security/products/connect/apsb21-91.html

https://helpx.adobe.com/security/products/reader-mobile/apsb21-89.html

https://helpx.adobe.com/security/products/ops_cli/apsb21-88.html

https://helpx.adobe.com/security/products/magento/apsb21-86.html

https://helpx.adobe.com/security/products/campaign/apsb21-52.html

## گـوگـل

شرکت گوگل (Google, LLC) در مهر ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. این شرکت در دوم مهر ماه، نسخه ۹۴.۰.۴۶۰۶.۶۱ را برای مرورگر فوق ارائه نمود. این نسخه از مرورگر، ضعف امنیتی به شناسه CVE-2021-37973 را ترمیم می‌کند. آخرین نسخه این مرورگر که در ۲۸ مهر انتشار یافت، نسخه ۹۵.۰.۴۶۳۸.۵۴ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_24.html

https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html

https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html

## اپـل

در مهر ماه، شرکت اپل (Apple, Inc) با انتشار به‌روزرسانی، ضعف‌هایی امنیتی متعددی را در چندین محصول خود از جمله iOS، MacOS و iPadOS 15.0.2 ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. توصیه می‌شود با مراجعه به نشانی‌های زیر، به‌روزرسانی مربوطه هر چه سریع‌تر اعمال شود.

https://support.apple.com/en-us/HT212824

https://support.apple.com/en-us/HT212825

https://support.apple.com/en-us/HT212846

## مـوزیـلا

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 ۸ آسیب‌پذیری را محصولات مذکور ترمیم می‌کنند. درجه حساسیت ۵ مورد از آنها "بالا" و ۳ مورد "متوسط" گزارش شده است. توضیحات بیشتر در لینک زیر قابل مطالعه است:

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

## آپاچی

۱۲ مهر، بنیاد نرم‌افزاری آپاچی (Apache Software Foundation)، با انتشار نسخه ۲.۴.۵۰ این محصول از ترمیم یک آسیب‌پذیری پویش مسیر (Path Traversal) با شناسه CVE-2021-41773 خبر داد. سوءاستفاده از ضعف مذکور دسترسی به محتوای فایل‌های ذخیره شده بر روی سرور آسیب‌پذیر را برای مهاجمان فراهم می‌کرد. بر اساس توضیحات این بنیاد، تنها نسخه ۲.۴.۴۹ از آسیب‌پذیری CVE-2021-41773 متاثر می‌شود. با این توضیح که بهره‌جویی از آسیب‌پذیری مذکور در صورتی موفق خواهد بود که قابلیت "Require all denied" فعال نباشد. ضمن آنکه سوءاستفاده موفق از CVE-2021-41773 می‌تواند منجر به نشت کد منبع (Source Code) فایل‌هایی نظیر اسکریپت‌های CGI شود.

خیلی زود پس از انتشار نسخه ۲.۴.۵۰، محققان امنیتی از آسیب‌پذیری این نسخه جدید خبر دادند و نمونه‌هایی از بهره‌جوهای قابل اجرا نیز بر روی اینترنت در دسترس قرار گرفت. سوءاستفاده از این آسیب‌پذیری جدید که به آن شناسه CVE-2021-42013 تخصیص داده شده می‌تواند در صورت غیرفعال بودن گزینه "Require all denied" منجر به اجرای کد به‌صورت از راه دور بر روی سرور شود.

به منظور وصله کردن این آسیب پذیری روز-صفر جدید، بنیاد آپاچی در ۱۵ مهر ماه اقدام به انتشار نسخه ۲.۴.۵۱ کرد.

هر دو آسیب‌پذیری CVE-2021-41773 و CVE-2021-42013 توسط مهاجمان در حال بهره‌جویی هستند. لذا به تمامی راهبران Apache HTTP Server توصیه اکید می‌شود که در صورت استفاده از هر یک از نسخ ۲.۴.۴۹ و ۲.۴.۵۰ در اسرع وقت نسبت به ارتقای این محصول به نسخه ۲.۴.۵۱ اقدام کنند.

در ۲۳ مهر نیز این بنیاد، با انتشار توصیه‌نامه‌ای، ضعفی به شناسه CVE-2021-42340 را در چندین نسخه از Apache Tomcat رفع کرد که سوءاستفاده از آسیب‌پذیری مذکور مهاجم را قادر به حمله‌ای از نوع "منع سرویس" می‌کند. توصیه‌نامه‌های آپاچی در لینک‌های زیر قابل مطالعه است:

https://httpd.apache.org/security/vulnerabilities_24.html

http://mail-archives.us.apache.org/mod_mbox/www-announce/202110.mbox/%3C9b8b83e3-7fec-a26d-7780-e5d4a85f7df6%40apache.org%3E

## جونیپر نت‌ورکز

جونیپر نت‌ورکز (Juniper Networks, Inc) هم در مهر ماه با ارائه به‌روزرسانی چندین ضعف امنیتی را محصولات مختلف این شرکت ترمیم کرد. سوءاستفاده از ضعف‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

# گزارش‌ها

# مروری بر Tomiris؛
## بدافزار دیگر گروه Nobelium

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، جزییات بدافزار جدید گروه Nobelium مورد بررسی قرار گرفته است.

۱۸ آذر سال ۹۹، شرکت امنیتی فایرآی (FireEye) رسماً اعلام کرد که سیستم‌هایش در جریان حمله‌ای بسیار پیچیده، مورد رخنه قرار گرفته است. به گفته فایرآی، مهاجمان این حمله با بکارگیری تکنیک‌های جدید موفق به سرقت ابزارهایی دیجیتال شده‌اند که این شرکت از آنها با عنوان Red Team یاد می‌کند. فایرآی از ابزارهای Red Team به‌منظور شناسایی آسیب‌پذیری سیستم‌ها در شبکه مشتریان خود استفاده می‌کرده است. گفته می‌شود که از این ابزارها به‌شدت مراقبت می‌شده است.

در آن زمان تصور می‌شد که هدف اصلی مهاجمان، سرقت ابزارهای Red Team بوده است.

اما خیلی زود مشخص شد که اهداف حملات بسیار گسترده‌تر از یک شرکت امنیتی بوده و بسیاری از شرکت‌ها و حتی سازمان‌ها و نهادهای مطرح نه فقط در ایالات متحده که در کشورهای متعدد در تسخیر مهاجمان قرار گرفته بودند.

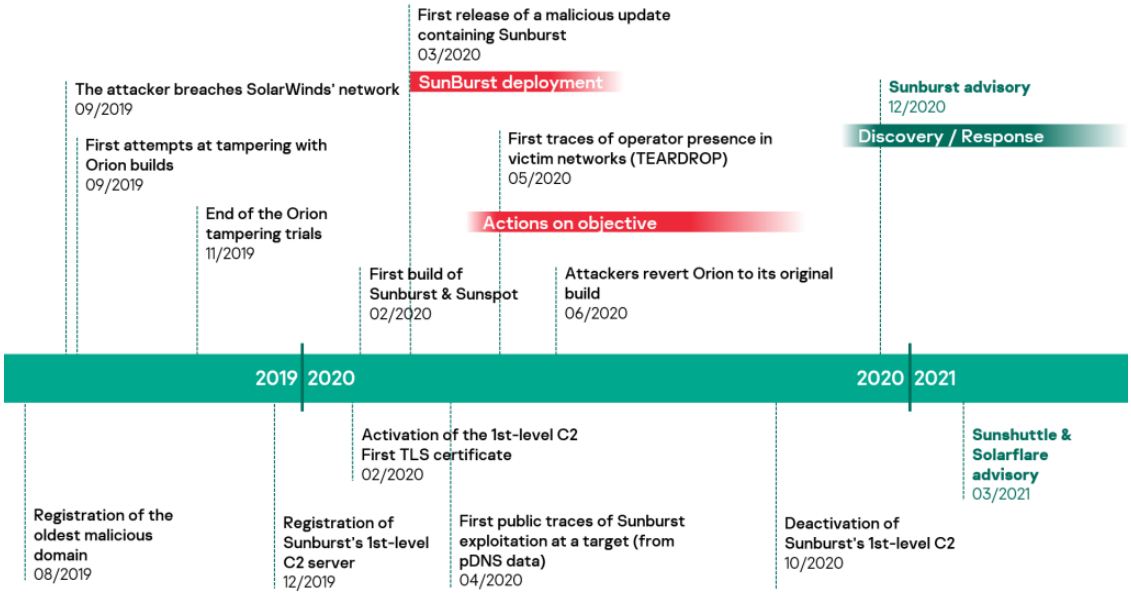
تمامی شرکت‌ها و سازمان‌های هک شده در یک چیز مشترک بودند و آن استفاده از یکی از نرم‌افزارهای ساخت شرکت سولاروینذز (SolarWinds, LLC) بوده است.

در جریان حمله فوق، مهاجمان Nobelium با بهره‌گیری از تکنیک موسوم به زنجیره تأمین (Supply Chain Attack) پس از هک شرکت سولاروینذز اقدام به تزریق کد آلوده به یکی از فایل‌های نرم‌افزار SolarWinds Orion با نام SolarWinds.Orion.Core.BusinessLayer.dll و تبدیل آن به یک درب‌پشتی (Backdoor) کردند. فایل مذکور نیز از طریق قابلیت به‌روزرسانی خودکار این نرم‌افزار به شبکه مشتریان سولاروینذز راه یافته بود. در عمل موجب شد که شبکه مشتریان این نرم‌افزار در هر نقطه از جهان به تسخیر آنها در بیاید.

حملات زنجیره تامین حملات سایبری هستند که با هدف قرار دادن عناصر با امنیت کمتر در شبکه، به کل سازمان آسیب می‌رسانند. در واقع در این حملات، مهاجمان با بهره‌جویی از اجزای آسیب‌پذیر یک نرم‌افزار معتبر در زنجیره تامین یک سازمان به آن رخنه و یا آن را دچار اختلال می‌کنند.

Nobelium، گروهی است که برخی منابع آن را منتسب به سازمان اطلاعات خارجی غیرنظامی فدراسیون روسیه (Russian Foreign Intelligence Service - به اختصار SVR) می‌دانند. از Nobelium با نام‌های APT29، The Dukes، DarkHalo یا Cozy Bear نیز یاد می‌شود.

اعتقاد بر این است که وقتی فایرآی اولین آثار حمله را کشف کرد، مهاجمان Nobelium بیش از یک سال بود که روی آن کار می کردند. شواهد جمع آوری شده تاکنون نشان می‌دهد که آن‌ها شش ماه در شبکه‌های سولارویندز حضور داشتند تا حمله خود را کامل کنند. حدس زده می‌شود که مهاجمان Nobelium از این دسترسی برای جمع آوری اطلاعات استفاده کرده‌اند.
جدول زمانی زیر مراحل مختلف این حمله را به طور خلاصه نمایش می‌دهد:




در آن زمان چندین شرکت امنیتی این حمله زنجیره تامین را مورد بررسی قرار دادند که برخی نمونه‌های آن در لینک‌های زیر قابل مطالعه است.

https://securelist.com/sunburst-connecting-the-dots-in-the-dns-requests/99862/
https://securelist.com/sunburst-backdoor-kazuar/99981/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/sunburst-malware-and-solarwinds-supply-chain-compromise/
https://www.mcafee.com/blogs/other-blogs/executive-perspectives/why-solarwinds-sunburst-is-a-wake-up-call/
https://symantec-enterprise-blogs.security.com/blogs/solarwinds/sunburst-supply-chain-attack-targets-solarwinds-users
https://symantec-enterprise-blogs.security.com/blogs/solarwinds/solarwinds-attacks-stealthy-attackers-attempted-evade-detection-0

براساس گزارش‌هایی در مارس ۲۰۲۱، شرکت‌های فایرآی و مایکروسافت (Microsoft Corp) اطلاعاتی در خصوص بدافزار دیگری تحت عنوان Sunshuttle (که GoldMax نیز نامیده می‌شود) و در کارزار فوق مورد استفاده قرار گرفته بود منتشر کردند.

https://www.fireeye.com/blog/threat-research/۰۳/۲۰۲۱/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html
https://www.microsoft.com/security/blog/۰٤/۰۳/۲۰۲۱/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

سپس در ۶ خرداد ۱۴۰۰ مایکروسافت کارزار فیشینگی را که سازمانی مستقر در ایالات متحده را هدف حمله قرار داده بود به Nobelium نسبت داد، جزئیات این حمله در گزارشی به نشانی زیر منتشر شده است:

https://www.microsoft.com/security/blog/۲۷/۰۵/۲۰۲۱/new-sophisticated-email-based-attack-from-nobelium/

در آن زمان Nobelium مدتها بود که عملیات خود را متوقف کرده بود و حملات دیگری به آن منتسب نشده بود. سپس در ژوئن ۲۰۲۱، محققان آثار DNS Hijacking را بر روی یکی از اعضای کشورهای مشترک المنافع کشف کردند.

در حملات موسوم به DNS Hijacking مهاجم پس از هک DNS Server، تغییراتی در رکوردها و نشانی‌های IP درج شده در آن ایجاد می‌کند و به واسطه تغییر IP، ترافیک را از سرورهای اصلی به سرور جدید که تحت کنترل خود قرار دارد، هدایت می‌کند. هنگامی که مهاجم نام دامنه‌ای را می‌رباید، کاربران را به سایت‌های مخرب و جعلی هدایت می‌کند. این سایت‌های جعلی اغلب به گونه‌ای طراحی شده‌اند که مانند سایت اصلی به نظر می‌رسند و هدف آنها فریب قربانیان برای وارد کردن اطلاعات اصالت‌سنجی و سپس ربودن آنها است.

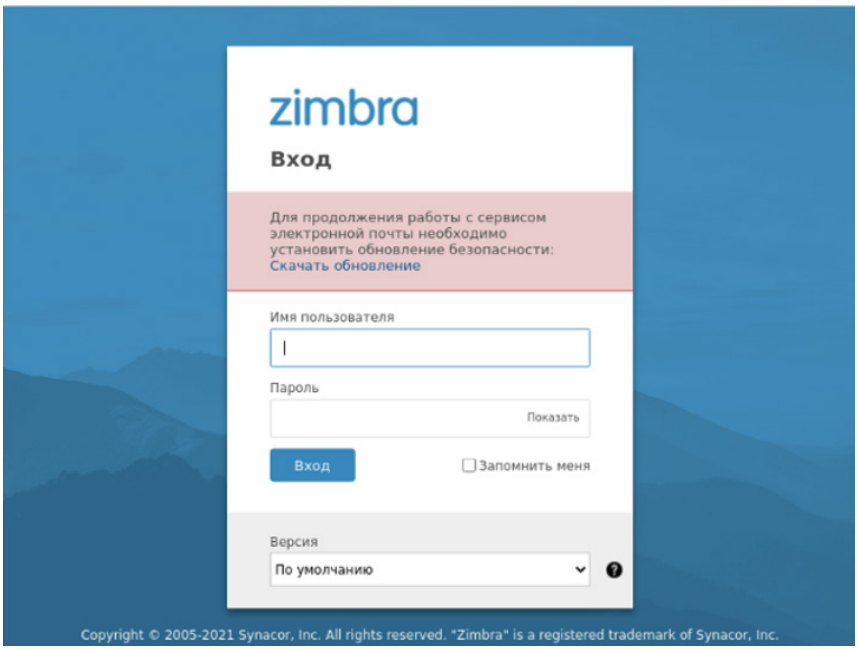
حملات DNS Hijacking اجرا شده توسط Nobelium در دوره‌های کوتاهی بین دسامبر ۲۰۲۰ تا ژانویه ۲۰۲۱ رخ دادند و مهاجمان ترافیک را از سرورهای ایمیل دولتی به دستگاههای تحت کنترل خودشان هدایت می‌کردند.

| Zone | Period during which the authoritative servers were malicious | Hijacked domains |
|---|---|---|
| mfa.*** | December 22-23, 2020 and<br>January 13-14, 2021 | mail.mfa.***<br>kk.mfa.*** |
| invest.*** | December 28, 2020 to January 13, 2021 | mail.invest.*** |
| fiu.*** | December 29, 2020 to January 14, 2021 | mx1.fiu.***<br>mail.fiu.*** |
| infocom.*** | January 13-14, 2021 | mail.infocom.*** |

به نقل از محققان شرکت کسپرسکی (Kaspersky, Lab.)، این حملات DNS Hijacking در بیشتر موارد نسبتاً مختصر بوده و به نظر می‌رسد که سرورهای ایمیل سازمان‌های موردنظر را عمدتاً هدف قرار می‌دادند. البته محققان نمی‌دانند که مهاجمان چگونه توانستند به این هدف برسند، اما فرض بر این است که آنها به نحوی موفق به کشف اطلاعات اصالت‌سنجی و ورود به کنسول مدیریتی سامانه شده بودند.

هنگامی که به واسطه تغییر IP در DNS Server، تغییرمسیر فعال می‌شود، قربانیان به صفحات Webmail login جعلی که همانند صفحات Webmail login اصلی به‌نظر می‌رسد و رفتار آن را تقلید می‌کنند، هدایت می‌شوند. مهاجمان از طریق این صفحات وب جعلی، اطلاعات اصالت‌سنجی ایمیل قربانیان را ربوده و در برخی موارد، آنها را متقاعد به نصب یک درب پشتی به نام Tomiris در قالب یک به‌روزرسانی نرم‌افزاری می‌کنند.

پس از این‌که مهاجمان نام‌های دامنه مختلف (Domain name) را از طریق DNS Hijacking تحت کنترل خود گرفتند، برای همه این صفحات جعلی گواهینامه‌های SSL معتبر Let's Encrypt (Let's Encrypt Certificate) دریافت می‌کنند. و این امر باعث می‌شود مهاجمان بدون هیچ خطای Certificate موفق به برقراری اتصال شوند و قربانیان غیرحرفه‌ای و غیرمتخصص متوجه حمله نشوند.




تصویر بالا، صفحه ورود به ایمیلی که توسط مهاجمان راه اندازی شده را نشان می‌دهد. هرگونه اطلاعات اصالت‌سنجی که در این صفحه تایپ می‌شود، توسط مهاجمان جمع‌آوری و ربوده شده و در مراحل بعدی حمله مجدداً مورد استفاده قرار می‌گیرد.

آنها پیامی را به صورت زیر به این صفحه Login اضافه نمودند و لینک مخربی را جهت فریب کاربر قرار می‌دهند تا یک "به روزرسانی امنیتی" از نوع بدافزاری را نصب کند.

"to continue working with the email service, you need to install a security update: download the update".

لینک فوق منجر به یک فایل اجرایی می‌شود که یک دانلود کننده (Downloader) بدافزار است که اکنون با نام Tomiris نامگذاری شده است.

Tomiris یک درب پشتی است که به زبان برنامه‌نویسی Go نوشته شده و پس از استقرار در سیستم قربانی به طور مداوم به سرور کنترل و فرماندهی (C2) متصل شده تا فایل‌های اجرایی مخرب بیشتری را بر روی سیستم هک شده دانلود کند اما قبل از انجام هرگونه عملیات مخرب، حداقل ۹ دقیقه به حالت خواب (Sleep) می‌رود تا بتواند سیستم‌های تحلیلی مبتنی بر سندباکس (Sandbox-based analysis systems) را دور بزند و توسط آن‌ها قابل شناسایی نباشد.

این درب‌پشتی برای برای ماندگاری در سیستم، از طریق اجرای یک فایل از نوع batch که حاوی دستور زیر است، اقدام به ایجاد یک فرمان زمان‌بندی شده می‌کند:

```
SCHTASKS /CREATE /SC DAILY /TN StartDVL /TR "[path to self]" /ST 10:00
```

آدرس سرور کنترل و فرماندهی (C2) مستقیماً در داخل Tomiris جاسازی نشده است. در عوض، به یک سرور واسط (Signalization) متصل می‌شود تا URL و درگاهی را که درب پشتی باید به آن متصل شود، استخراج کند. سپس Tomiris درخواست‌های GET را به URL مذکور ارسال می‌کند تا اینکه سرور C2 به صورت یک JSON Object با ساختاری شبیه به آنچه در ادامه می‌بینید پاسخ دهد:

```
{"filename": "[filename]", "args": "[arguments]", "file": "[base64-encoded executable]"}
```

این Object یک فایل اجرایی را مشخص می‌کند که روی سیستم قربانی دانلود شده و با پارامترهای خاص اجرا می‌شود. این ویژگی و این واقعیت که Tomiris هیچ گونه قابلیتی فراتر از دانلود ابزارهای بیشتری را ندارد، نشان می‌دهد که بدافزارهای دیگری نیز در این مجموعه ابزار وجود دارند، که تاکنون محققان نتوانسته‌اند آن‌ها را شناسایی و بازیابی کنند.

محققان همچنین نمونه دیگری از Tomiris (با نام "SBZ" که هش آن در زیر قابل دسترس است) را شناسایی کردند که در نقش یک درب‌پشتی به طور خودکار فایل‌هایی را که با پسوندهای از پیش تعریف شده مطابقت دارد (.rar, .pdf, .docx, .doc) سرقت می‌کند.

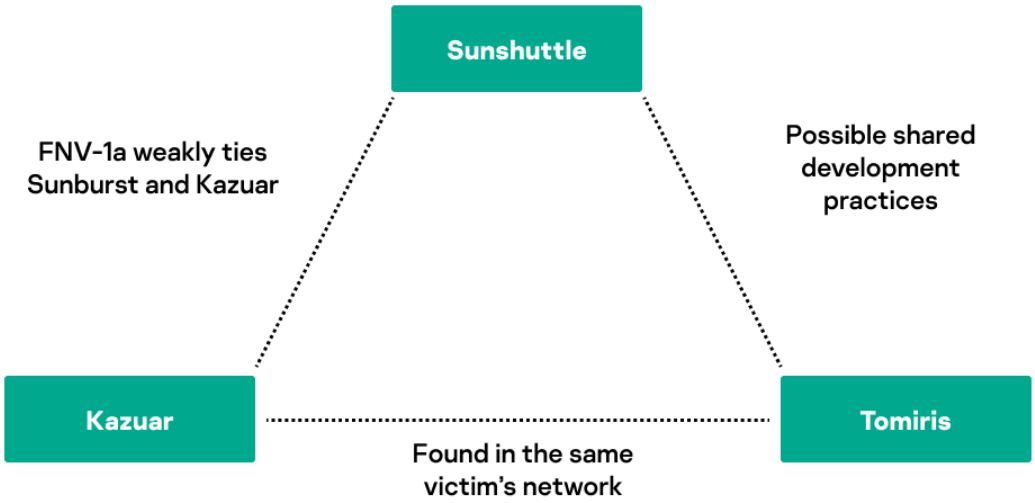
51AA89452A9E57F646AB64BE6217788E

برخی سرنخ‌های کوچک یافت شده در طول این تحقیق نشان می‌دهد که احتمالاً گردانندگان Tomiris روسی زبان هستند.

محققان هنگام تحلیل Tomiris، متوجه شباهت‌ها آن با بدافزار Sunshuttle شدند. برخی از مهمترین آن‌ها عبارتند از زبان برنامه نویسی یکسان، الگوریتم‌های رمزگذاری/مبهم‌سازی مشابه جهت ارتباط با سرور کنترل و فرمان‌دهی (C2)، بهره‌گیری از فرامین زمان‌بندی شده جهت ماندگاری در سیستم، ساز و کار تاخیر در اجرا (Sleep) و وجود اشتباهات و غلط‌های املائی مشابه در آن‌ها.

تشابه دیگر این است که دستگاه‌های دیگری که در شبکه به Tomiris آلوده شده‌اند، با درب پشتی Kazuar نیز هک شده‌اند. محققان کسپرسکی نتوانستند از داده‌های موجود به این نکته پی ببرند که آیا یکی از این بدافزارهای مخرب منجر به استقرار بدافزار دیگر شده است یا این که از دو رویداد مستقل نشات گرفته‌اند.

علی‌رغم وجود شباهت‌های زیادی یافت شده بین این دو درب پشتی، با اطمینان نمی‌توان Tomiris و Sunshuttle را یکسان دانست. ممکن است بخشی از این شباهت‌ها کاملاً تصادفی باشند، اما برنامه‌نویسی آنها توسط گروه یکسان یا بکارگیری کدهای برنامه‌نویسی مشابه، محتمل به نظر می‌رسد. نمودار بعدی پیوندهای ضعیفی را بین این سه بدافزار ذکر شده نشان می‌دهد:

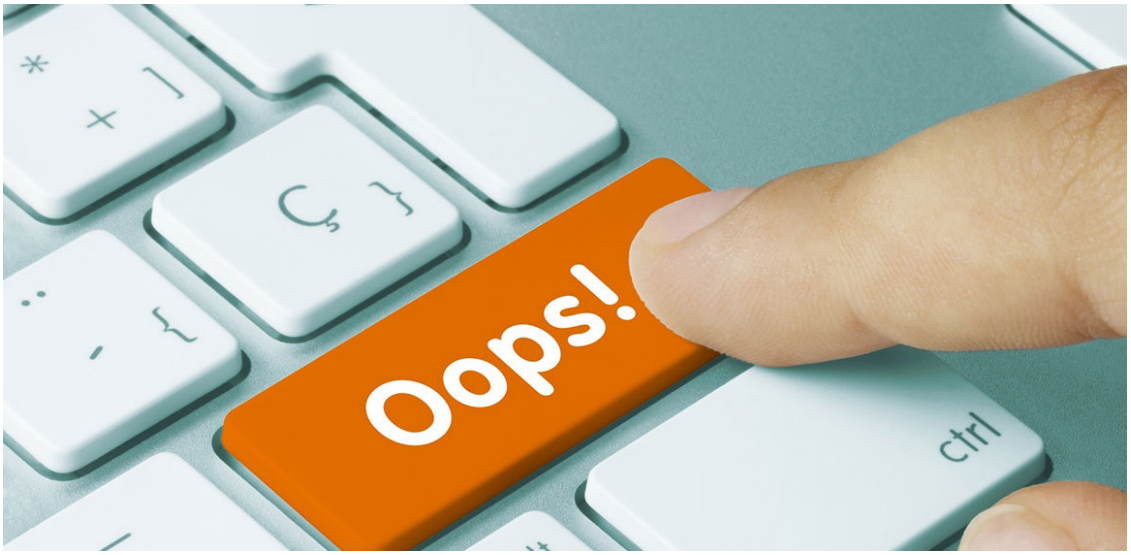



با وجود اینکه شکل مذکور به تعدادی سرنخ جهت ارتباط بین Kazuar، Sunburst و Tomiris اشاره می‌کند، اما به نظر می‌رسد که هنوز مدرک اصلی توسط محققان کشف نشده تا بتوان همه آن‌ها را به یک گروه نسبت داد.

یک فرضیه این است که به دلیل گستردگی حملات Sunshuttle سایر مهاجمان به طور هدفمند سعی در بازتولید روش بدافزار مذکور داشته باشند تا تحلیل‌گران و متخصصان امنیتی را گمراه کنند. اولین نمونه Tomiris که محققان از آن مطلع هستند در فوریه ۲۰۲۱ یعنی یک ماه قبل از کشف Sunshuttle در جهان ظاهر شد.

در حالی که ممکن است گردانندگان تهدیدات مستمر و پیشرفته (Advanced Persistent Threat - به اختصار APT) از وجود این بدافزار در آن زمان مطلع بوده باشند، اما بعید است که سعی در بکارگیری این بدافزار قبل از افشا شدن داشته باشند. یک فرضیه بسیار محتمل‌تر این است که نویسندگان بدافزارهای Sunshuttle، در دسامبر ۲۰۲۰ هنگامی که حملات به شبکه مشتریان شرکت سولارویندز کشف شد، شروع به توسعه Tomiris کرده‌اند تا آن را جایگزین بدافزار فاش شده خود کنند.

# ۱۰ اشتباه رایج امنیتی




تیم تحقیقاتی شرکت سوفوس (Sophos, Ltd) فهرستی از رایج‌ترین اشتباهات امنیتی موجود در طیف وسیعی از سازمان‌ها که در ۱۲ ماه گذشته هنگام بررسی و خنثی‌سازی حملات سایبری با آنها مواجه شده‌اند را ارائه کرده است.

در ادامه، فهرستی از ده اشتباه رایج امنیتی که بر اساس تجربیات و مشاهدات تیم پاسخ به رویداد شرکت سوفوس هنگام مقابله با حملات با آن مواجه شده‌اند، مورد بررسی قرار می‌گیرد:

- اشتباه شماره ۱. ما هدف نیستیم. ما بسیار کوچک هستیم و/یا هیچ دارایی ارزشمندی برای مهاجم نداریم.

بنا بر گزارش سوفوس، بسیاری از قربانیان حملات سایبری تصور می‌کنند که آنها بسیار کوچک هستند، یا فاقد هرگونه دارایی ارزشمند و جذاب برای مهاجمان هستند. حقیقت این است که اینطور نیست؛ اگر سازمانی توانایی پردازش و حضور دیجیتالی دارد، یکی از اهداف جذاب برای حمله مهاجمان است. با وجود عناوین رسانه‌ای، اکثر حملات توسط مهاجمان با پشتوانه دولتی انجام نمی‌شود. آنها توسط فرصت‌طلبانی که به دنبال طعمه آسان هستند، صورت می‌گیرند مانند سازمان‌هایی که باگ، شکاف امنیتی یا تنظیماتی نادرست دارند و تبهکاران سایبری می‌توانند به راحتی از آنها سوءاستفاده کنند.

اگر سازمانی معتقد است که برای مهاجمان جذاب نیست و مورد هدف آن‌ها قرار نمی‌گیرد، احتمالاً به دنبال کشف فعالیت مشکوک در شبکه خود نیست (مانند حضور Mimikatz) که یک برنامه منبع باز است و به کاربران امکان مشاهده و ذخیره اطلاعات اصالت‌سنجی را بر روی کنترلر دامنه (Domain Controller) می‌دهد. این امر موجب می‌شود که نشانه‌های اولیه حمله توسط سازمان قابل شناسایی و تشخیص نباشد.

- اشتباه شماره ۲. ما نیازی به فناوری‌های امنیتی و حفاظتی پیشرفته که همه جا نصب کرده‌اند، نداریم.

برخی از مدیران فناوری اطلاعات هنوز معتقدند که نرم‌افزارهای امنیتی نقطه پایانی برای جلوگیری از تمام انواع تهدیدات کافی است یا نیازی به ایمن‌سازی سرورهای خود ندارند. مهاجمان نیز از چنین فرضیاتی نهایت استفاده را می‌برند. هرگونه اشتباه در پیکربندی، اعمال وصله‌ها یا تمهیدات حفاظتی (ایمن‌سازی)، سرورها را برخلاف گذشته به یک هدف اصلی تبدیل می‌کند نه یک هدف ثانویه.

تعداد و انواع حملاتی که در آن سعی می‌شود که توسط تیم‌های امنیتی فناوری اطلاعات شناسایی نشوند و نرم‌افزارهای نقاط پایانی را دور بزنند یا غیرفعال کنند، روزبه‌روز بیشتر می‌شوند. به عنوان مثال می‌توان به حملاتی اشاره کرد که از مهندسی اجتماعی سوءاستفاده کرده و با بکارگیری نقاط آسیب‌پذیری متعدد، کدهای بدافزاری بسیاری را بسته‌بندی و مبهم‌سازی نموده و مستقیماً به حافظه تزریق می‌کنند. حملات بدافزاری بدون‌فایل (Fileless) همچون بارگذاری فایل DLL و حملاتی که علاوه بر تکنیک‌های متداول و مورد استفاده توسط راهبران امنیتی، از ابزارهای دسترسی از راه دور مجاز همچون Cobalt Strike استفاده می‌کنند. تکنولوژی‌های اولیه ضدویروس برای تشخیص و مسدودسازی چنین فعالیت‌هایی دائماً در حال تلاش هستند.

به طور مشابه، این فرض که نقاط پایانی محافظت شده می‌توانند مانع از ورود مهاجمان به سرورهای محافظت نشده شوند، کاملاً اشتباه است. با توجه به رویدادهایی که اخیراً محققان سوفوس مشاهده و بررسی کرده‌اند، سرورها اکنون هدف شماره یک حملات مهاجمان هستند و تبهکاران سایبری به راحتی می‌توانند با استفاده از اطلاعات اصالت‌سنجی به سرقت رفته، مسیر مستقیم را جهت نفوذ به آن‌ها پیدا کنند. اکثر مهاجمان راه نفوذ به سیستم‌های تحت Linux را نیز می‌دانند. در واقع، مهاجمان غالباً پس از هک سیستم‌های تحت Linux، از طریق نصب درب پشتی از آنها به عنوان مسیری امن جهت دسترسی و گسترش در شبکه هدف استفاده می‌کنند.

اگر سازمانی فقط متکی به سیستم‌های امنیتی و حفاظتی ساده و ابتدایی باشد و فاقد هرگونه ابزارهای پیشرفته و یکپارچه همچون راهکارهای مبتنی بر رفتار و تشخیص بر پایه هوش‌مصنوعی باشد و در عین حال یک مرکز حفاظتی شبانه‌روزی تحت هدایت انسان (SOC 7*24) نداشته باشد، مهاجمان سرانجام از سد دفاعی آن سازمان عبور خواهند کرد.

نکته آخر و مهم این است که هرچند پیشگیری از حملات، هدف هر سازمانی است اما تشخیص به موقع حملات نیز بسیار ضروری است.

- اشتباه شماره ۳. ما سیاست‌های امنیتی (حفاظتی) قوی داریم.

داشتن سیاست‌های امنیتی برای برنامه‌های کاربردی و کاربران بسیار حیاتی است. با این حال، با اضافه شدن ویژگی‌ها و قابلیت‌های جدید به دستگاه‌های متصل به شبکه، سیستم‌های حفاظتی نیز باید به طور مداوم بررسی و به‌روز شوند. با استفاده از تکنیک‌هایی مانند تست نفوذ (Penetration testing)، سناریوها و اجراهای آزمایشی (Tabletop exercises and trial runs)، برنامه‌های بازیابی رویداد و سیاست‌های سازمان تأیید و آزمایش شوند.

- اشتباه شماره ۴. دسترسی های از راه دور (Remote Desktop Protocol) را می‌توان با تغییر درگاه‌هایی که روی آن‌ها قرار دارند و با بکارگیری احراز هویت چند عاملی (Multi-Factor Authentication) در برابر مهاجمان محافظت کرد.

درگاه استانداردی که برای خدمات RDP مورد استفاده قرار می‌گیرد، ۳۳۸۹ است. بنابراین اکثر مهاجمان درگاه مذکور را به منظور یافتن سرورهای دسترسی از راه دور باز، پویش می‌کنند. با این حال، این پویش هرگونه سرویس باز را بدون در نظر گرفتن درگاهی که در آن قرار دارند شناسایی می‌کند. لذا تغییر درگاه‌ها به خودی خود هیچ گونه حفاظتی را تامین نمی‌کند یا حفاظت بسیار کمی را ارائه می‌دهد.

علاوه بر این، اگرچه احراز هویت چندعاملی بسیار مهم است اما تنها در صورتی که این خط‌مشی برای همه کاربران و دستگاه‌ها اعمال شود، امنیت را افزایش می‌دهد. فعالیت RDP نیز باید در محدوده حفاظتی یک شبکه خصوصی مجازی (VPN) بکارگرفته شود و در صورتی که مهاجمان از قبل در شبکه وجود داشته باشند، MFA نمی‌تواند به طور کامل از یک سازمان محافظت کند. ترجیحاً اگر استفاده از آن ضروری باشد، باید استفاده از RDP در داخل و خارج، محدود یا غیرفعال شود.

- اشتباه شماره ۵. مسدودکردن نشانی‌های IP مناطق پرخطری همچون روسیه، چین و کره شمالی از ما در برابر حملات صورت گرفته از آن مناطق جغرافیایی محافظت می‌کند.

مسدودکردن نشانی‌های IP مناطق خاص بعید است که آسیبی به همراه داشته باشد اما اگر فقط برای افزایش امنیت به این موضوع اتکا شود می‌تواند احساس امنیت کاذب ایجاد کند. کشورهای دیگری نیز همچون ایالات متحده، هلند و بقیه اروپا میزبان زیرساخت‌های بدافزاری مهاجمان هستند.

- اشتباه شماره ۶. نسخه پشتیبان تهیه شده، سازمان را در برابر عواقب حمله باج‌افزاری مصون نگه می‌دارد.

داشتن نسخه پشتیبان به‌روز از اسناد و مدارک اهمیت بسیاری دارد. با این حال، اگر نسخه پشتیبان شما به شبکه متصل باشد، در دسترس مهاجمان قرار دارد و ممکن است در حمله باج‌افزاری مورد رمزگذاری، حذف یا در معرض غیرفعال شدن قرار گیرد. شایان ذکر است که حتی محدود کردن تعداد افرادی که به نسخه پشتیبان سازمان دسترسی دارند نیز ممکن است امنیت را به میزان قابل توجهی افزایش ندهد زیرا مهاجمان در شبکه به دنبال این افراد و دسترسی به اطلاعات اصالت‌سنجی آن‌ها خواهند بود.

به طور مشابه، ذخیره نسخه پشتیبان در فضای ابری نیز باید با احتیاط انجام شود. اخیراً در یکی از حملات، تیم تحقیقاتی سوفوس مشاهده نمودند که مهاجمان بعد از سرقت اطلاعات اصالت‌سنجی مدیر فناوری اطلاعات، به ارائه‌دهنده خدمات ابری ایمیل ارسال کردند

فرمول استاندارد تهیه نسخه پشتیبان که می‌توان برای بازیابی داده‌ها و سیستم‌ها پس از حمله باج‌افزاری مورد استفاده قرار گیرد پیروی از قاعده ۱-۲-۳ است. بر طبق این قاعده، به طور دوره‌ای از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه بعنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.

آخرین نکته احتیاطی این است که پشتیبان‌گیری آفلاین در محل، اطلاعات شما را در برابر حملات باج‌افزارهایی که هدفشان اخاذی است، محافظت نمی‌کند. تبهکاران سایبری پس از سرقت فایل‌ها تهدید می‌کنند که داده‌های شما را رمزگذاری و/یا منتشر خواهند کرد.

اشتباه شماره ۷. کارکنان سازمان‌ها امنیت را درک می‌کنند.

براساس گزارش سوفوس از باج‌افزارها در سال ۲۰۲۱ که جزئیات آن در نشانی زیر منتشر شده است، ۲۲ درصد از سازمان‌ها معتقدند که در ۱۲ ماه آینده مورد حمله باج‌افزارها قرار خواهند گرفت زیرا پیشگیری از به خطر انداختن امنیت توسط کاربران نهایی دشوارتر است.

https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

تشخیص تاکتیک‌های مهندسی اجتماعی همچون ایمیل‌های فیشینگ مشکل‌تر شده است. پیام‌ها غالباً دستی و بصورت دقیق نوشته می‌شوند. از این رو متقاعدکننده هستند و با دقت هدف‌گذاری می‌شوند. کارکنان سازمان‌ها باید بدانند که چگونه پیام‌های مشکوک را تشخیص داده و هنگام دریافت چنین پیام‌هایی چه کنند. آنها باید بدانند که به چه کسی اطلاع دهند تا سایر کارکنان نیز در حالت آماده باش قرار گیرند.

اشتباه شماره ۸. تیم‌های واکنش به رویداد می‌توانند داده‌های سازمان را پس از حمله باج‌افزاری بازیابی کنند.

این بسیار بعید است. امروزه مهاجمان اشتباهات بسیار کمتری مرتکب می‌شوند و فرایند رمزگذاری خود را بهبود داده‌اند، بنابراین اتکا به تیم پاسخ به رویداد جهت یافتن روزنه‌ای که بتواند آسیب را برطرف کند بسیار نادر است.

علاوه بر بازنویسی داده‌های اصلی ذخیره شده روی دیسک، اکثر باج‌افزارهای مدرن، پشتیبان‌گیری خودکار مانند Windows Volume Shadow Copies را نیز حذف می‌کنند که این امر موجب می‌شود تنها راه بازیابی از طریق پرداخت باج باشد.

اشتباه شماره ۹. پس از حمله باج‌افزاری و پرداخت باج توسط سازمان، مهاجمان داده‌های سازمان را پس می‌دهند.

براساس گزارش سوفوس از باج‌افزارها در سال ۲۰۲۱، سازمانی که باج مطالبه شده را پرداخت می‌کند، به طور متوسط تنها حدود ۳/۲ (۶۵ درصد) از داده‌های خود را دریافت می‌کند. فقط ۸ درصد از سازمان‌ها همه اطلاعات خود را پس گرفتند و ۲۹ درصد کمتر از نیمی از اطلاعات سرقت شده را دریافت کردند. پرداخت باج حتی زمانی که به نظر می‌رسد گزینه ساده‌تری است و یا تنها گزینه تحت پوشش بیمه‌نامه سایبری سازمان است، راه حل مناسبی برای رهایی از مشکل نیست.

علاوه بر این، بازیابی داده‌ها تنها بخشی از فرایند ترمیم و پاکسازی باج‌افزار است. در بیشتر موارد باج‌افزار، کامپیوترها را کاملاً غیرفعال و قفل می‌کند به گونه‌ای که قبل از بازیابی داده‌ها، ابتدا باید نرم افزارها و سیستم‌ها از ابتدا بازسازی شوند. گزارش سال ۲۰۲۱ نشان می‌دهد که به طور متوسط هزینه‌های بازیابی ده برابر بیشتر از باج مطالبه شده است.

اشتباه شماره ۱۰. انتشار باج‌افزار کل حمله است، اگر سازمان از انتشار باج‌افزار در امان باشد، مشکلی وجود ندارد.

متأسفانه این مورد به ندرت اتفاق می‌افتد. مهاجمان می‌خواهند از طریق انتشار باج‌افزار راهبران سازمان را از حضور خود در شبکه سازمان مطلع و آنچه که انجام داده‌اند، مطلع کنند.

به احتمال زیاد همانطور که در لینک زیر اشاره شده است، مهاجمان اگر از چند هفته قبل در شبکه یک سازمان نباشند، چند روز قبل از انتشار باج‌افزاردر شبکه بوده‌اند و به کاوش، غیرفعالسازی، حذف نسخه‌های پشتیبان، یافتن سیستم‌های حاوی اطلاعات با ارزش و حیاتی و یا برنامه‌های کاربردی به منظور رمزگذاری، حذف اطلاعات و نصب کدهای بدافزاری همچون درب‌های پشتی پرداخته‌اند. حضور و ماندگاری در شبکه‌های قربانی به مهاجمان اجازه می‌دهد در صورت تمایل حمله دوم خود را انجام دهند.

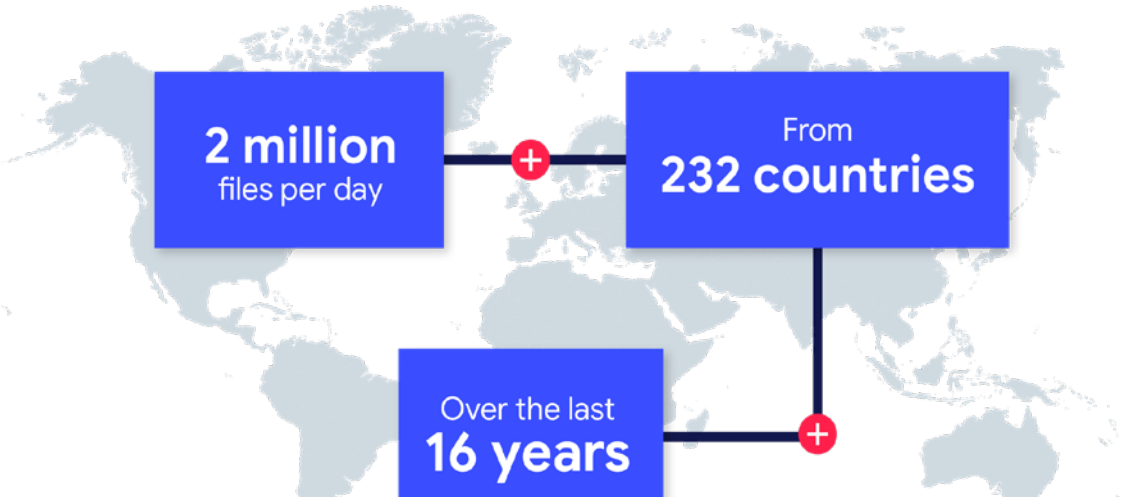
https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/

# گزارش سایت VirusTotal

## درخصوص فعالیت باج‌افزارها

اخیراً سایت VirusTotal گزارش خود را تحت عنوان Ransomware Activity Report منتشر کرده است.

این سایت طی ۱۶ سال گذشته، روزانه بیش از ۲ میلیون فایل ارسالی از ۲۳۲ کشور را بررسی و پردازش کرده است.

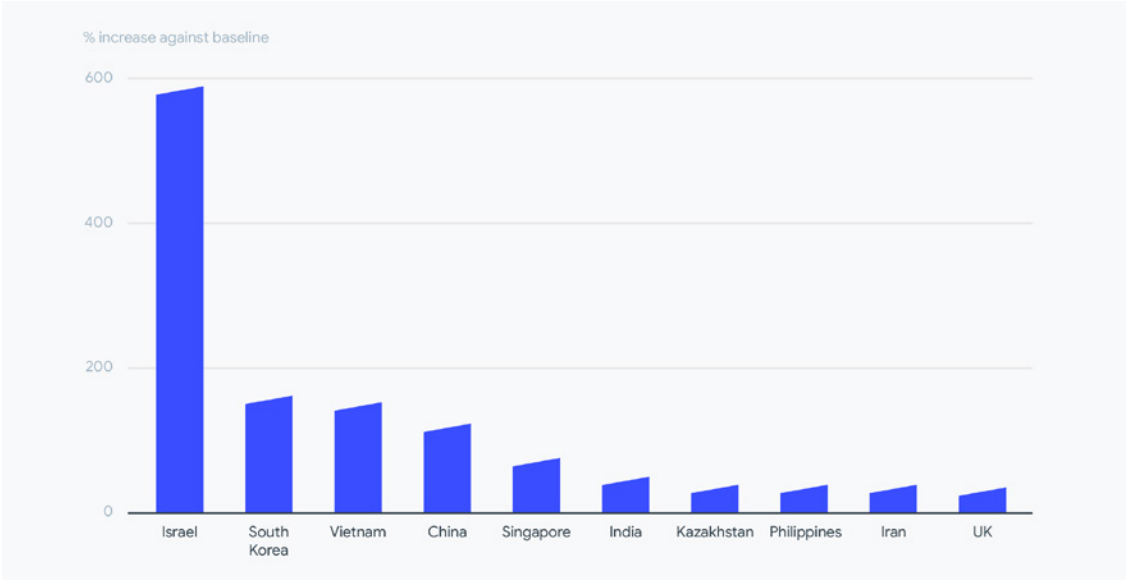



در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده چکیده‌ای از گزارش VirusTotal ارائه شده است.

سایت VirusTotal هر فایل ارسالی را توسط ۷۰ ضدویروس بررسی کرده و گزارش شناسایی یا عدم شناسایی آن‌ها را در اختیار کاربر قرار می‌دهد.

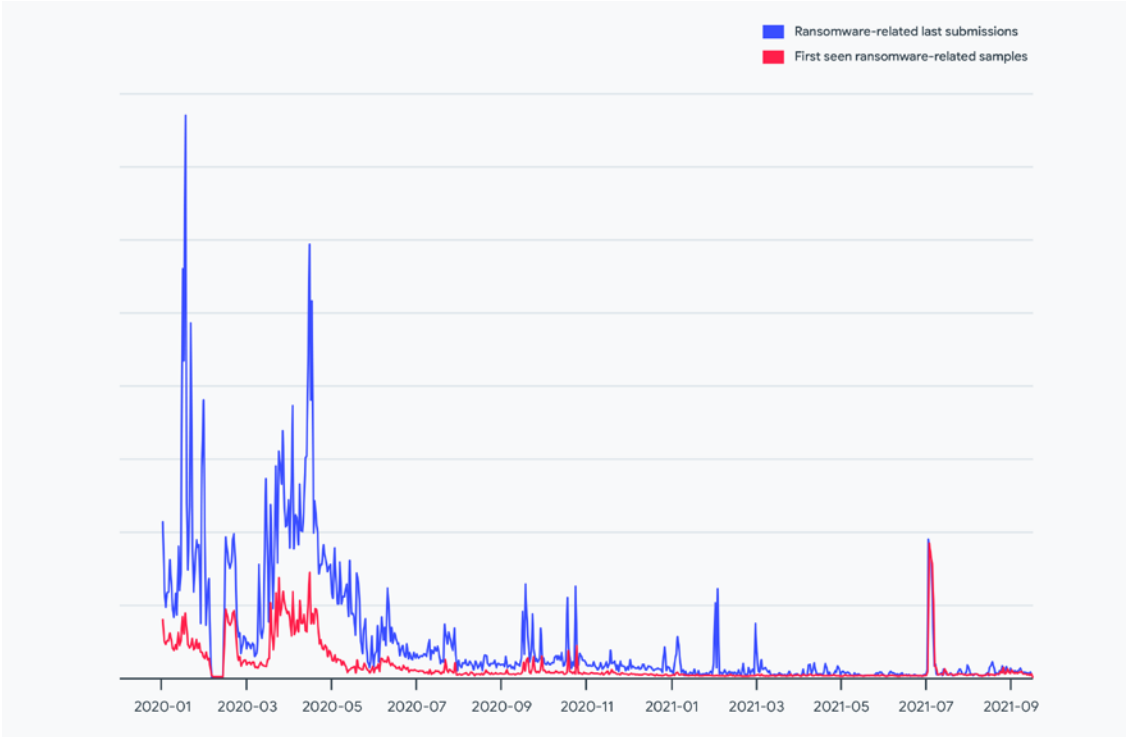
در این گزارش، سایت VirusTotal فعالیت‌های باج‌افزارها را با توجه به فایل‌های ارسالی مرتبط با سال ۲۰۲۰ به بعد که شامل بررسی ۸۰ میلیون نمونه باج‌افزار از ۱۴۰ کشور جهان بوده مورد تحلیل قرار داده است.

نمودار زیر فهرست کشورهایی که بیشترین نمونه‌های باج‌افزاری را جهت بررسی به سایت مذکور ارسال کرده‌اند، نشان می‌دهد.

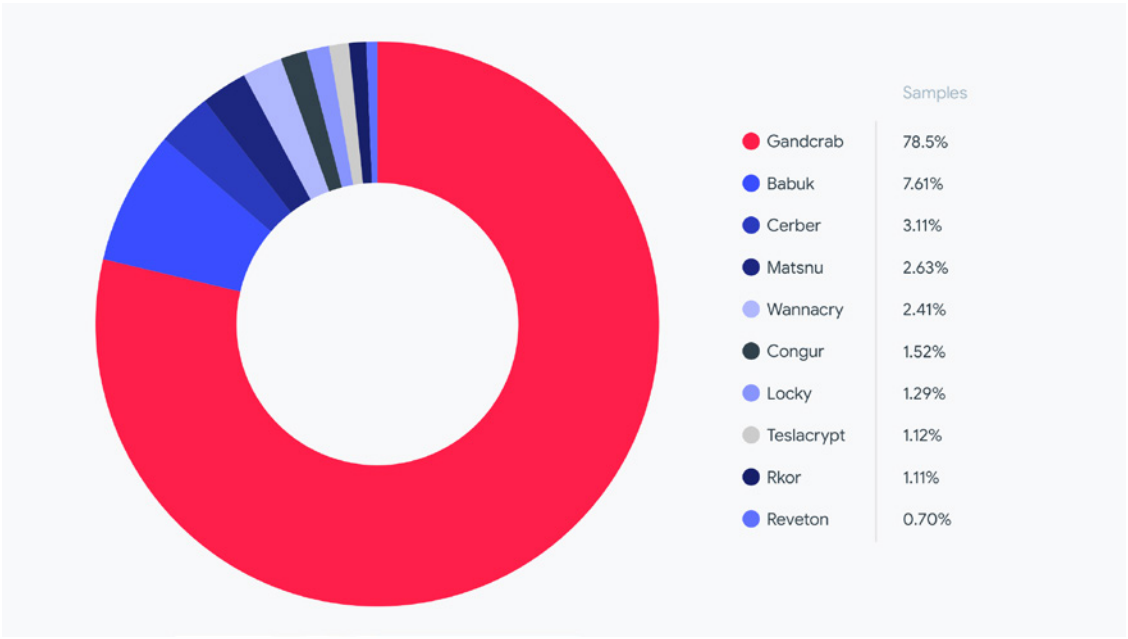



تمایزهای جغرافیایی قابل توجهی در نمودار فوق وجود دارد، البته به این معنا نیست که کشورهایی که بیشترین آمار فایل‌های ارسالی را در این نمودار دارند، بیشترین حمله در آن‌ها صورت گرفته است. محققان VirusTotal معتقدند آمار بیشتر می‌تواند مربوط به بسیاری از شرکت‌ها و ارسال خودکار فایل از آن‌ها باشد.

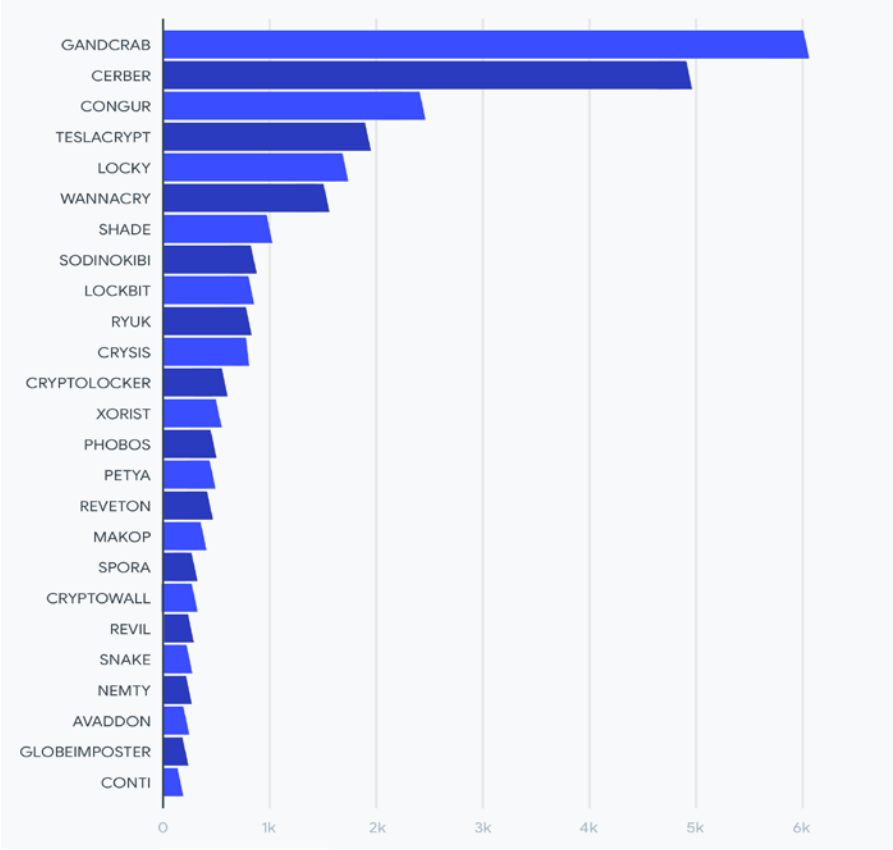
در نموداری از این گزارش به توزیع زمانی باج‌افزارهای جدید و باج‌افزارهای شناخته‌شده از ابتدای سال ۲۰۲۰ پرداخته شده است. این نمودار بیانگر این نکته است که با وجود این‌که مهاجمان سایبری در حملات خود از نمونه‌های جدیدی باج‌افزاری استفاده می‌کنند، با این حال، با بررسی قله‌های نمودار کاملاً مشهود است که در سه ماهه اول سال ۲۰۲۱ اکثر حملات توسط باج‌افزارهای شناخته‌شده صورت گرفته است.

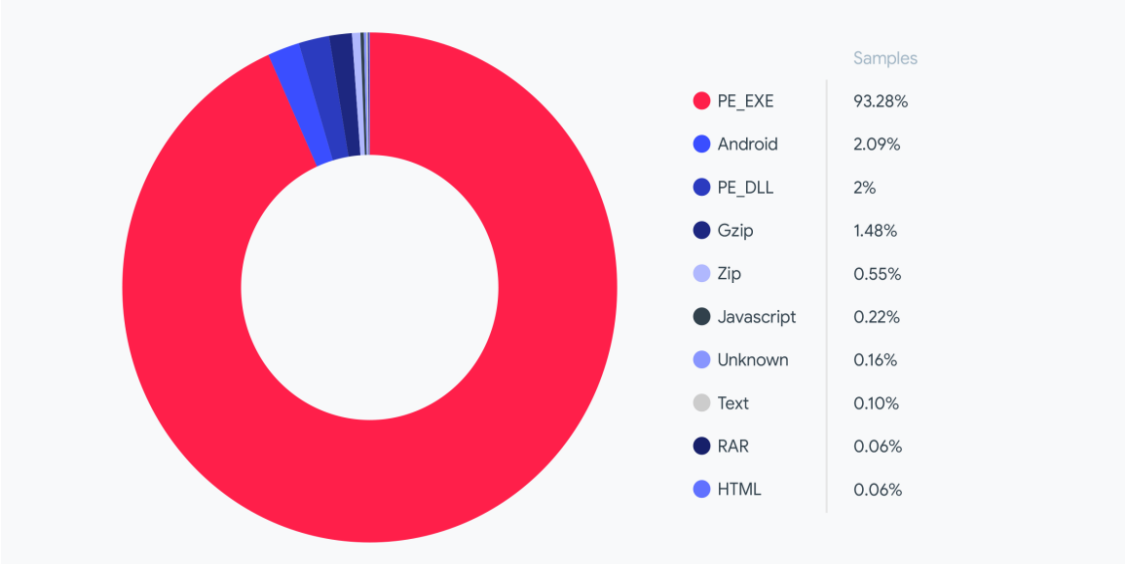


به گزارش محققان VirusTotal، از ابتدای سال ۲۰۲۰، فعالیت باج‌افزارها در دو فصل اول سال ۲۰۲۰ در اوج خود بوده که آن را به فعالیت گروه باج‌افزاری GandCrab نسبت دادند. GandCrab با ۷۸.۵ درصد در اوایل ۲۰۲۰ در صدر حملات سایبری قرار داشت و پس از آن به طرز چشمگیری کاهش یافت و همچنان نیز با آمار کمتری فعال می‌باشد. Babuk نمونه قابل توجه دیگری است که با ۷.۶۱ درصد در جایگاه دوم این نمودار قرار گرفته است.




محققان در این تحقیق، حداقل ۱۳۰ خانواده مختلف باج‌افزاری را شناسایی نموده‌اند. نمودار زیر خانواده باج‌افزارهای مورد بررسی در این تحقیق را نشان می‌دهد.






بر اساس این گزارش، حدود ۹۵ درصد از فایل‌های باج‌افزاری شناسایی شده از نوع PE_EXE و PE_DLL بوده است. به نقل از Virus-Total این امر کاملاً منطقی است زیرا نمونه‌های باج‌افزاری معمولاً با استفاده از مهندسی اجتماعی و/یا توسط فایل‌های فراخوانی‌کننده بدافزار (dropper) اجرا می‌شوند.

روش انتشار ۵ درصد از نمونه‌های بررسی شده، سوءاستفاده از آسیب‌پذیری‌های امنیتی بوده است. "ترفیع امتیازی" (Privilege Es-calation)، "افشای اطلاعات" (Information disclosure) و "اجرای کد از راه دور" (Remote Execution) اصلی ترین نوع از این آسیب‌پذیری‌ها بوده‌اند. از میان ۱۰ آسیب‌پذیری برتر، تنها دو مورد از آن‌ها در سال ۲۰۲۰ کشف شده بودند.

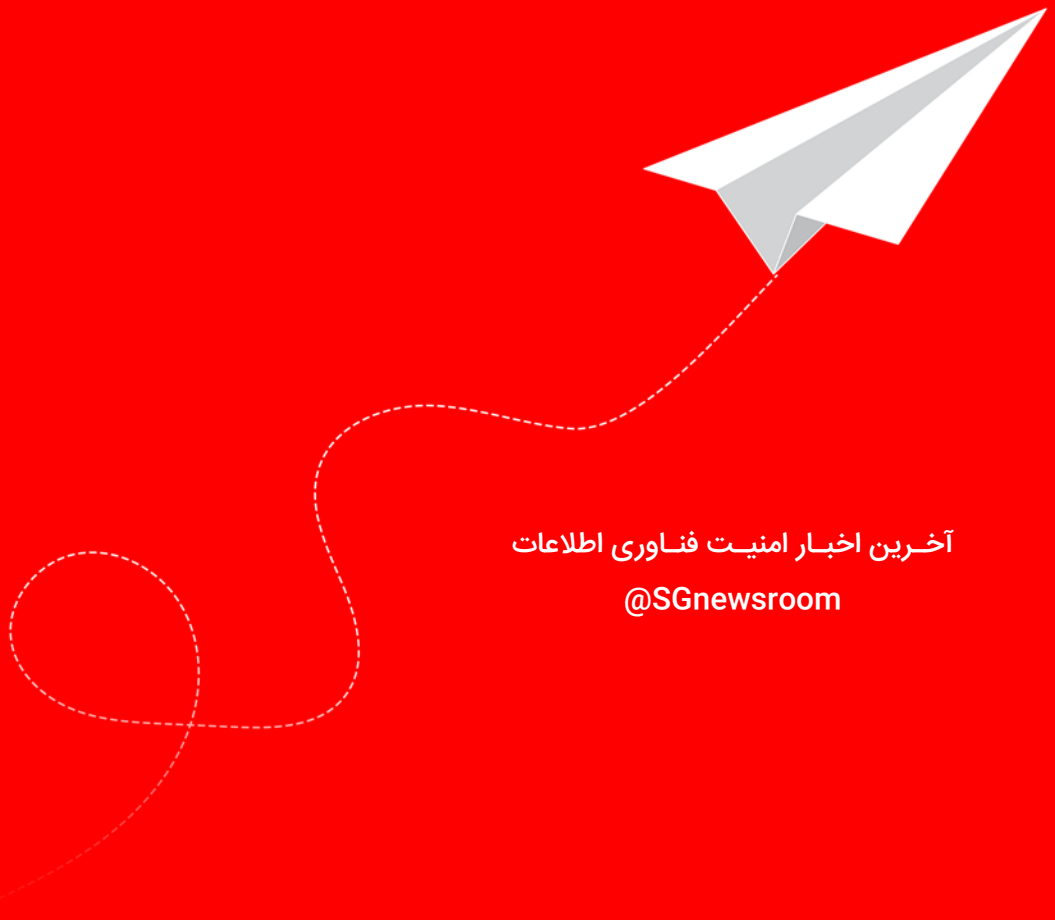
قبلاً در گزارش شرکت مهندسی شبکه‌گستر نیز که مشروح آن در نشانی زیر قابل مطالعه است، به نقل از محققان کوالیس (Qualys, Inc)، مشاهده شده که در حملات بزرگ باج‌افزاری پنج سال گذشته، مهاجمان علاوه بر بهره‌جویی از ضعف‌های امنیتی شناخته شده و جدید، در بیشتر موارد از برخی آسیب‌پذیری‌های بسیار قدیمی برای توزیع باج‌افزار سوءاستفاده می‌کنند.

https://newsroom.shabakeh.net/22650/criminals-are-still-exploiting-old-vulnerabilities.html

در این گزارش اینطور نتیجه‌گیری شده که فعالیت باج‌افزارها هرگز متوقف نمی‌شود و همواره بین ۱۰۰۰ تا ۲۰۰۰ دسته باج‌افزاری در طول بازه زمانی تحلیل فعال بوده اند.

مشروح گزارش VirusTotal در نشانی زیر قابل مطالعه است:

https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf



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