McAfee

گزارش و آمار فصلی از فعالیت بدافزارها و تهدیدات سایبری

نوامبر ۲۰۲۰

شبکه گستر
امنیت شما | وظیفه ما

چکیده مدیریتی

سال ۲۰۲۰ در حالی آغاز شد که سوءاستفاده از موضوعات مرتبط با همه‌گیری کرونا به فهرست تکنیک‌های مورد استفاده مهاجمان در انتشار بدافزارها و اجرای حملات سایبری افزوده شد. در سه‌ماهه دوم با استمرار شیوع کرونا و تداوم و گسترش بی‌سابقه دورکاری کارکنان، بکارگیری این رویکرد نه تنها کم رنگ نشد که مورد توجه و استفاده مهاجمان بیشتری نیز قرار گرفت. شبکه جهانی مک‌آفی متشکل از بیش از یک میلیارد حسگر[۱] نشان می‌دهد که تهدیدات مبتنی بر کووید-۱۹ در سه‌ماهه دوم ۲۰۲۰ در مقایسه با سه‌ماهه قبل از آن ۶۰۵ درصد افزایش داشتند. مک‌آفی در سامانه زیر نیز جدیدترین آمار و آخرین وضعیت تهدیدات مبتنی بر کووید-۱۹ را در دسترس قرار داده است:

https://www.mcafee.com/enterprise/en-us/lp/covid-19-dashboard.html

مدیران امنیت اطلاعات[۲] و گروه‌های امنیتی با تهدیدات دائماً در حال تکامل روبرو شده‌اند که از لحاظ تعداد و دامنه همواره در حال افزایش و گسترده‌تر شدن هستند. مهاجمان بدخواه نیز با تکنیک‌هایی که روزبه‌روز پیچیده‌تر می‌شوند کسب‌وکارها، دولت‌ها، مراکز آموزشی و نیروی کاری را که همچنان با چالش‌های ناشی از محدودیت‌های کووید-۱۹، آسیب‌پذیری‌های بالقوه دستگاه‌های از راه دور و امنیت کانال‌های ارتباطی دست به گریبان هستند هدف قرار می‌دهند.

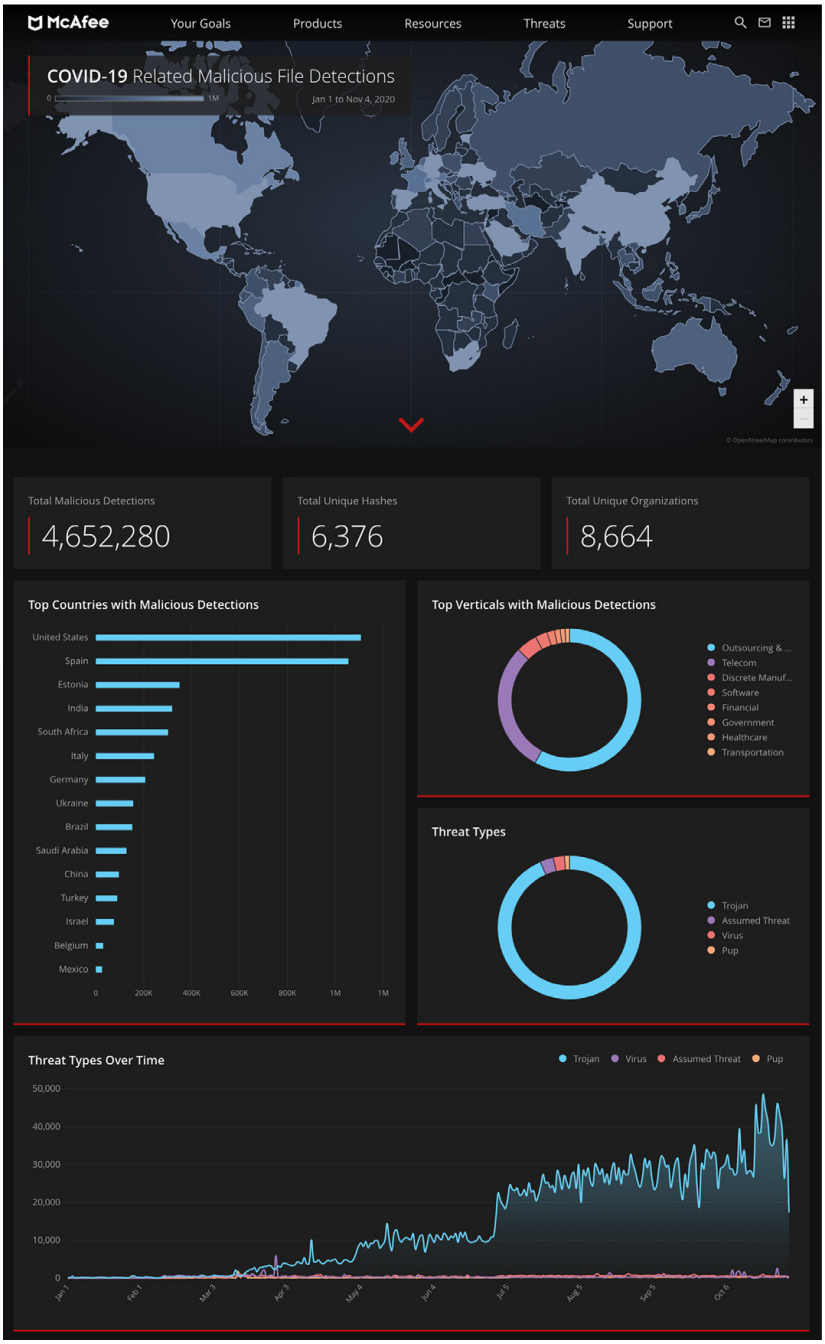
با چالش‌ها و ابهامات متعدد موجود، رعایت الزامات امنیتی توسط کاربران نظیر مراقبت و حساسیت در زمان باز کردن پیوست ایمیل‌ها یا کلیک بر روی لینک‌های بالقوه مخرب فیشینگ در کنار آگاهی از ترفندهای مهاجمان نقشی کلیدی در ایمن ماندن از گزند تهدیدات و حملات سایبری این روزها دارد.

همچون همیشه محققان مک‌آفی بر روی تاکتیک‌ها و تکنیک‌های مورد استفاده تبهکاران سایبری تمرکز دارند. مک‌آفی با رصد اطلاعات استخراج شده از یک میلیارد حسگر خود که در سرتاسر جهان پراکنده‌اند بینشی جامع را در راستای حفاظت از کسب‌وکار و دارایی‌های شما فراهم می‌کند.

در این گزارش آزمایشگاه‌های مک‌آفی[۳] با نگاهی موشکافانه تهدیدات مطرح در سه‌ماهه دوم ۲۰۲۰ را مورد بررسی قرار داده‌اند. همچنین برخی یافته‌های بخش تحقیق تهدیدات پیشرفته شرکت مک‌آفی[۴] که همواره هوشیار و پرتکاپو در حال ردیابی، شناسایی و کالبدشکافی جدیدترین کارزارهای سایبری و بررسی علت و اثرات آنهاست در این گزارش ارائه شده است.

۱ Sensor
۲ CISO
۳ McAfee Labs
۴ Advanced Threat Research - به اختصار ATP

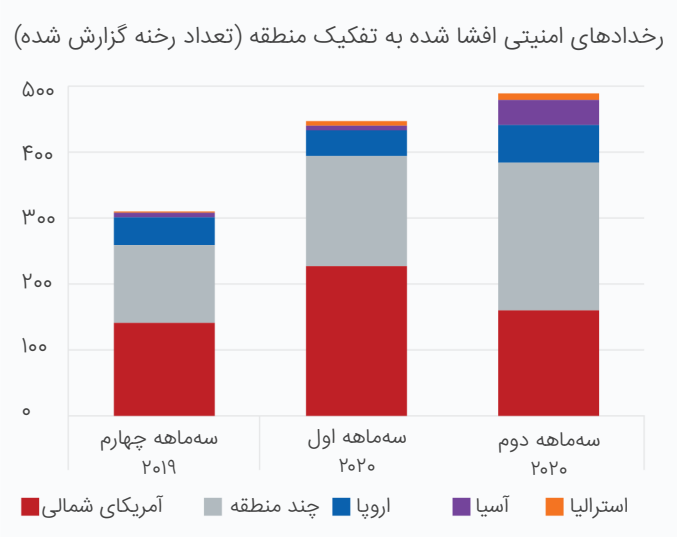
فهرست مطالب



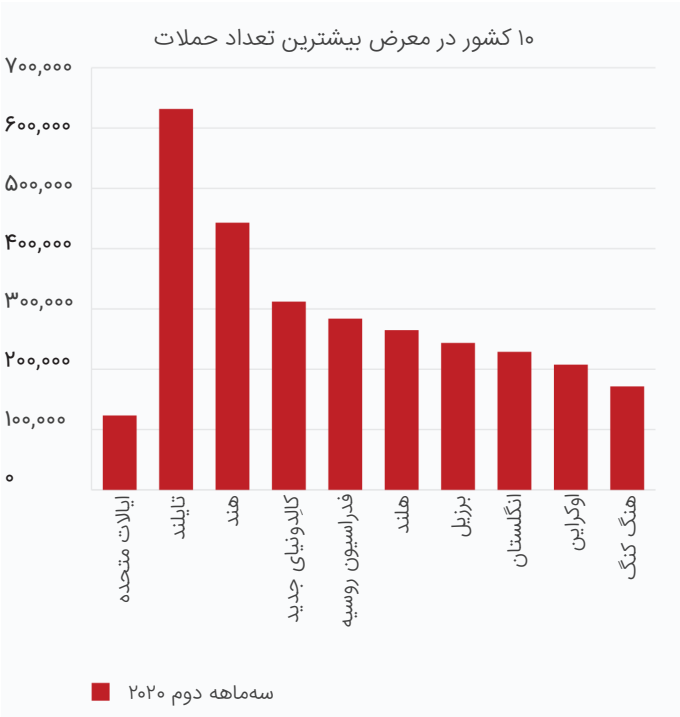
بر طبق آمار شبکه جهانی مک‌آفی متشکل از یک میلیارد حسگر تهدیدات مبتنی بر کووید-۱۹ در سه‌ماهه دوم ۲۰۲۰ در مقایسه با سه‌ماهه قبل از آن ٦٥٥ درصد افزایش داشتند.

اهداف و روش‌های اجرای این تهدیدات

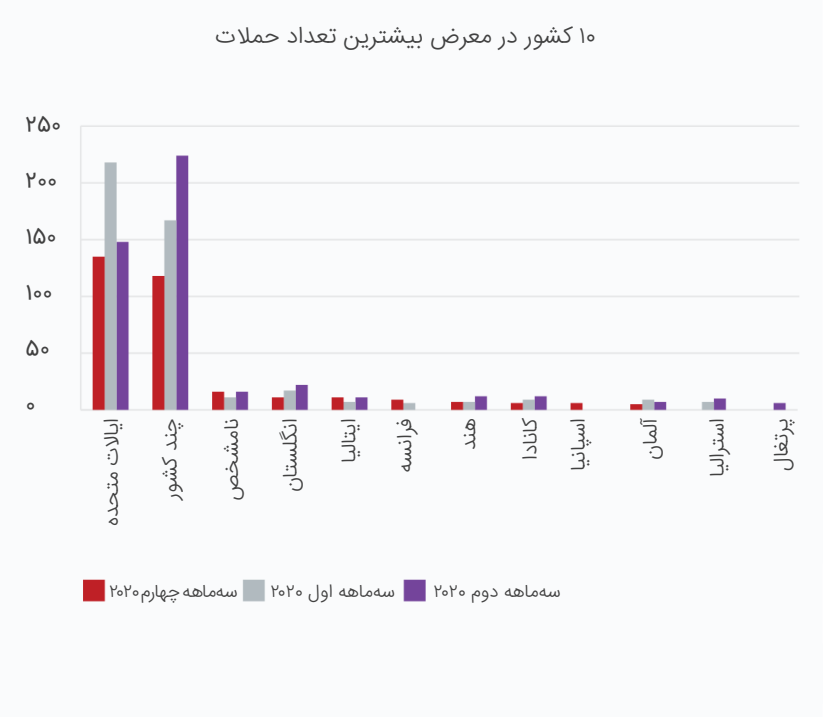
آزمایشگاه‌های مک‌آفی در سه‌ماهه دوم ۲۰۲۰ به‌طور میانگین ۴۱۹ تهدید جدید را در هر دقیقه گزارش کردند که ۴۴ مورد (۱۲ درصد) افزایش را در مقایسه با دوره قبل نشان می‌دهد.



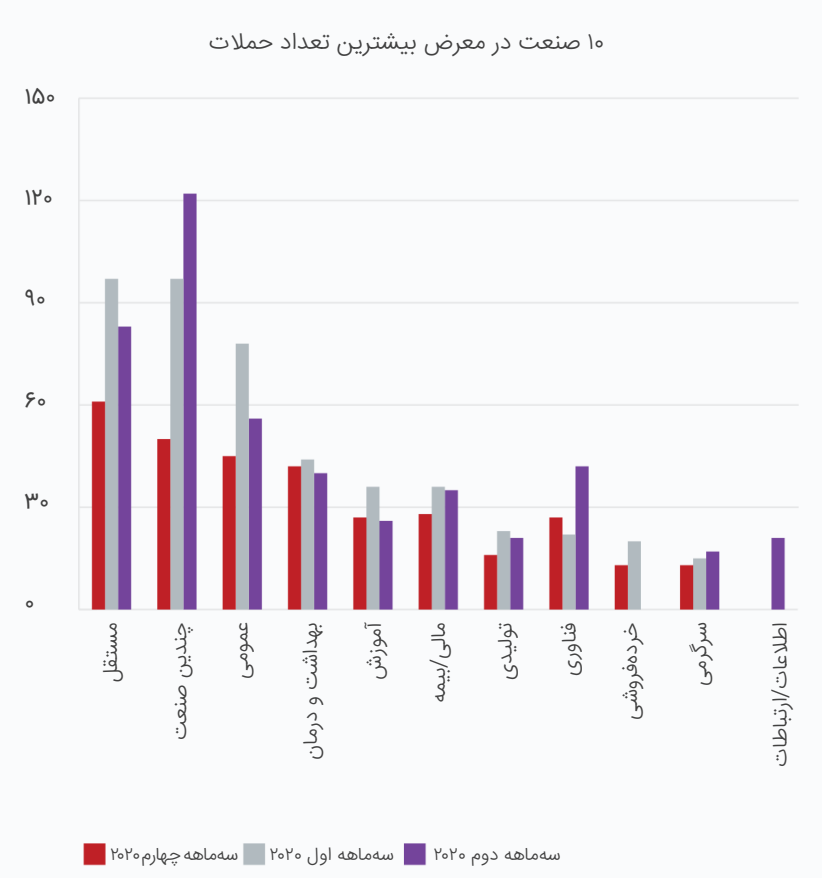
محققان مک‌آفی در سه‌ماهه اول سال ۲۰۲۰، حدود ۵۶۱ رخداد امنیتی را که به‌صورت عمومی افشا شده بودند مورد رصد قرار دادند. در این میان، حملاتی که در آنها منطقه جغرافیایی خاصی هدف مهاجمان نبوده افزایشی ۲۲ درصدی نسبت به سه‌ماهه اول ۲۰۲۰ داشت. رخدادهای افشا شده‌ای که در آنها آمریکای شمالی هدف قرار گرفته بودند ۲۹ درصد کل رخدادهای این دوره را تشکیل داده‌اند که کاهشی ۳۰ درصدی را نسبت به سه‌ماهه قبلی نشان می‌دهد. منطقه اروپا نیز ۱۰ درصد از مجموع رخدادهای این دوره را تشکیل می‌دهد.



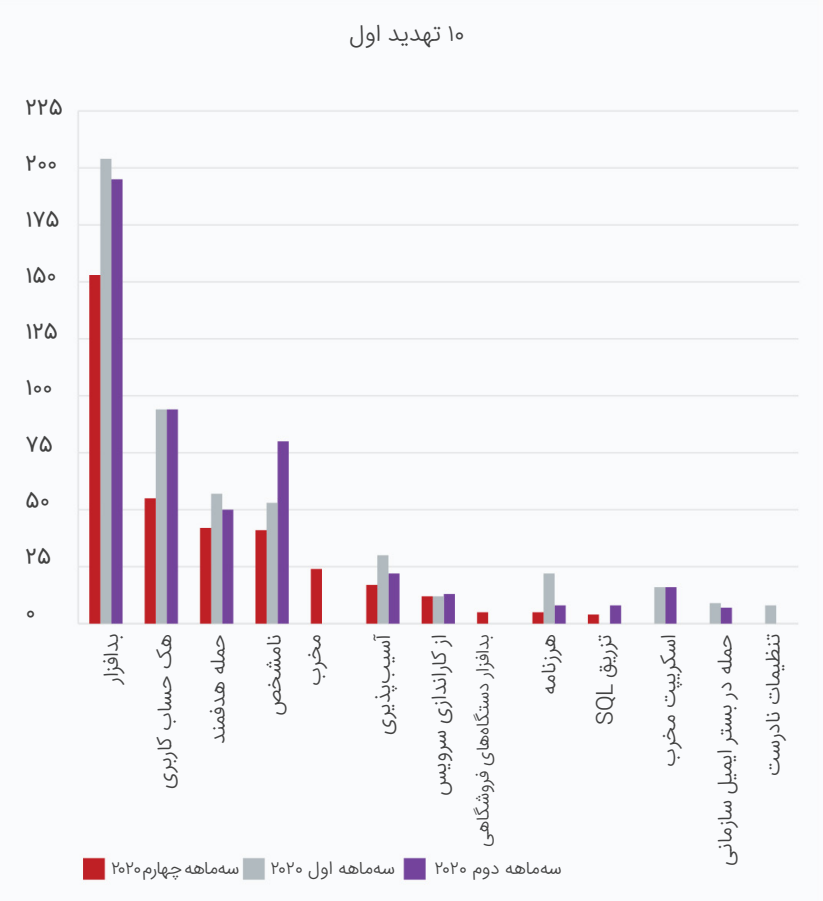
در این دوره مک‌آفی حدود ۷٫۵ میلیون حمله به حساب‌های کاربری رایانش ابری را رصد کرده است. این حملات متوجه حوزه‌های مهمی در سرتاسر جهان شامل خدمات مالی، بهداشت و درمان، خدمات عمومی، آموزشی، خرده‌فروشی، فناوری، تولیدی، انرژی، خدمات رفاهی، امور قانونی، بنگاه‌های املاک و مستغلات، حمل‌ونقل و خدمات کسب‌وکار بوده است.



در سه‌ماهه دوم ۲۰۲۰ در مقایسه با دوره قبل، رخدادهای گزارش شده در ایالات متحده ۴۷ درصد کاهش، انگلستان ۲۹ درصد افزایش و کانادا ۲۵ درصد افزایش داشته است.



تعداد رخدادهای افشا شده‌ای که در سه‌ماهه دوم ۲۰۲۰ بخش های فعال در حوزه علم و صنعت از آنها تأثیر پذیرفتند در مقایسه با سه‌ماهه قبل از آن ۹۱ درصد افزایش داشته است.



به‌طور کلی، بدافزارها با ۳۵ درصد بیشترین سهم از رخدادهای امنیتی گزارش شده در سه‌ماهه دوم ۲۰۲۰ را به خود اختصاص دادند. هک حساب‌های کاربری با ۱۷ درصد و حملات هدفمند با ۹ درصد در جایگاه‌های بعدی قرار دارند.

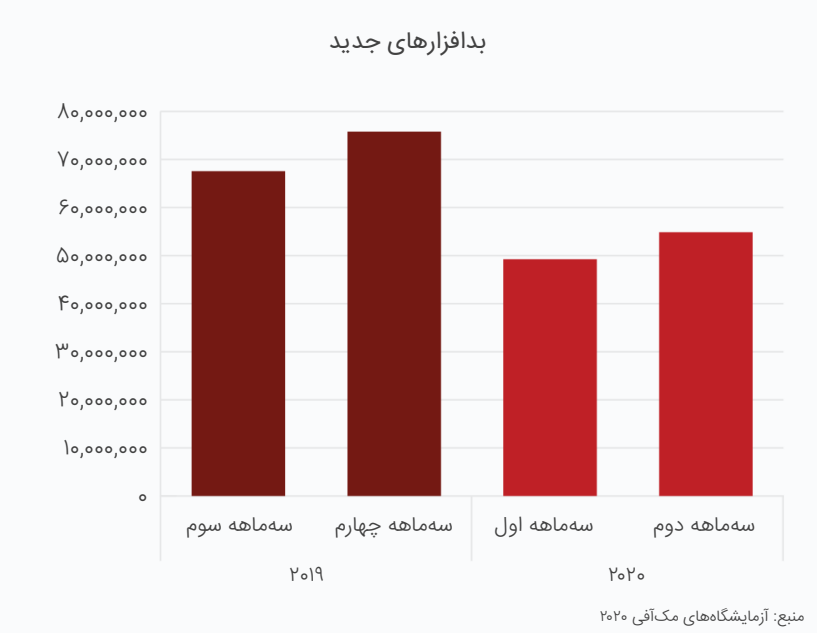
آمار تهدیدات بدافزاری

در سه‌ماهه دوم ۲۰۲۰ شاهد تغییرات قابل توجه در چندین دسته از تهدیدات سایبری بودیم؛ از شاخص‌ترین آنها می‌توان به موارد زیر اشاره کرد:

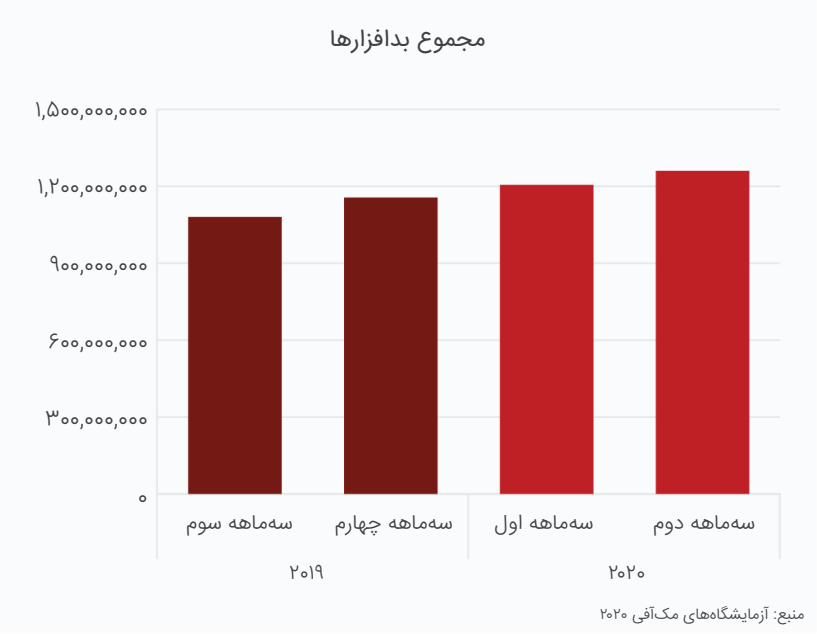
- آزمایشگاه‌های مک‌آفی به‌طور میانگین در هر دقیقه ۴۱۹ تهدید جدید را رصد کردند که حدود ۱۲ درصد افزایش را در مقایسه با دوره قبل نشان می‌دهد.
- نمونه‌های جدید از بدافزارهای مبتنی بر PowerShell در مقایسه با دوره قبل ۱۱۷ درصد افزایش یافتند. بدافزار Donoff نقشی پررنگ در افزایش این آمار داشته است.
- بدافزارهای جدید مبتنی بر مجموعه نرم‌افزاری Office نیز ۱۰۳ درصد افزایش داشتند. یکی از عوامل تأثیرگذار در این افزایش، انتشار گسترده Donoff که در قالب اسناد مخرب توزیع و با بهره‌گیری از پروسه معتبر PowerShell اجرا می‌شود بوده است.
- تعداد کدهای مخرب دودویی امضاشده[1] جدید در مقایسه با دوره قبل ۲۵ درصد افزایش یافتند؛ در این افزایش آگهی‌افزار Android Mobby Adware نقش داشته است.
- بدافزارهای جدید موسوم به استخراج‌کننده ارز رمز[2] ۲۵ درصد افزایش داشتند.
- بدافزارهای جدید مبتنی بر سیستم عامل Linux افزایش ۲۲ درصدی داشتند که فعالیت Gafgyt و Mirai از اصلی‌ترین دلایل این سیر صعودی بوده است.
- بدافزارهای جدید موبایلی افزایشی ۱۵ درصدی داشته‌اند؛ در این افزایش Android Mobby Adware نقشی کلیدی داشته است.
- بدافزارهای جدید موسوم به اینترنت اشیاء[3] به ویژه به دلیل گسترش Gafgyt و Mirai افزایشی ۷ درصدی داشتند.

[1] Malicious Signed Binaries
[2] Coin Miner
[3] IoT - به اختصار Internet of Things

- آمار باج‌افزارها در مقایسه با سه‌ماهه اول ۲۰۲۰ در روندی ثابت تغییر محسوسی با دوره قبل نداشت.
- بدافزارهای جدید تحت iOS در نتیجه کاهش چشمگیر انتشار Tiniv که بخش قابل‌توجهی از موارد شناسایی شده در دوره قبل را به خود اختصاص داده بود ۷۷ درصد کاهش یافتند.
- بدافزارهای جدید بهره‌جو[1] در نتیجه کاهش بدافزارهای مبتنی بر بهره‌جوی Exploit-CVE-2010-2568 و کنار گذاشته شدن Parasitic افتی ۲۱ درصدی داشتند.
- نمونه‌های جدید از بدافزارهای مبتنی بر JavaScript به دلایل مختلف از جمله تنزل استخراج‌کنندگان تحت این نوع اسکریپت‌ها ۱۸ درصد کاهش یافتند.
- نمونه‌های جدید از بدافزارهای مبتنی بر macOS تقریبا ۸ درصد کاهش یافتند؛ تغییرات در میزان انتشار درب‌پشتی Shlayer و آگهی‌افزار Bundlore نقشی اساسی در این کاهش داشته است.

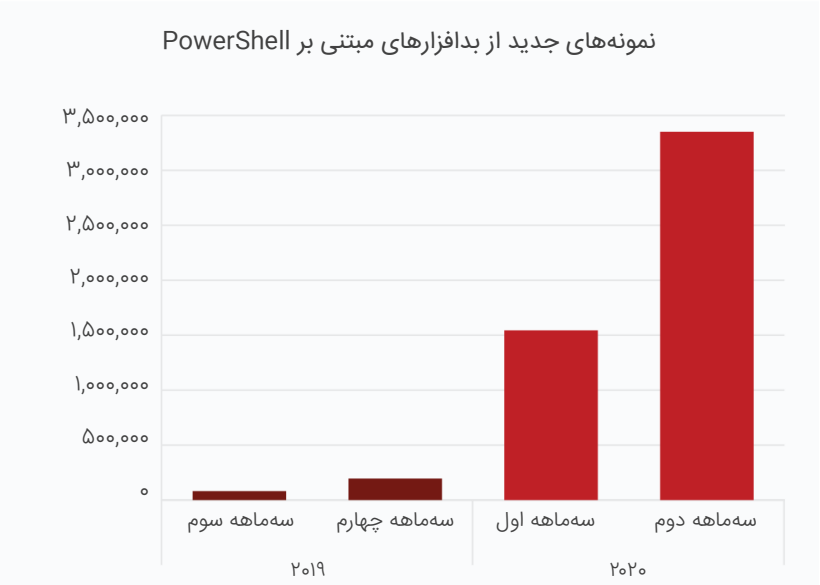


منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰

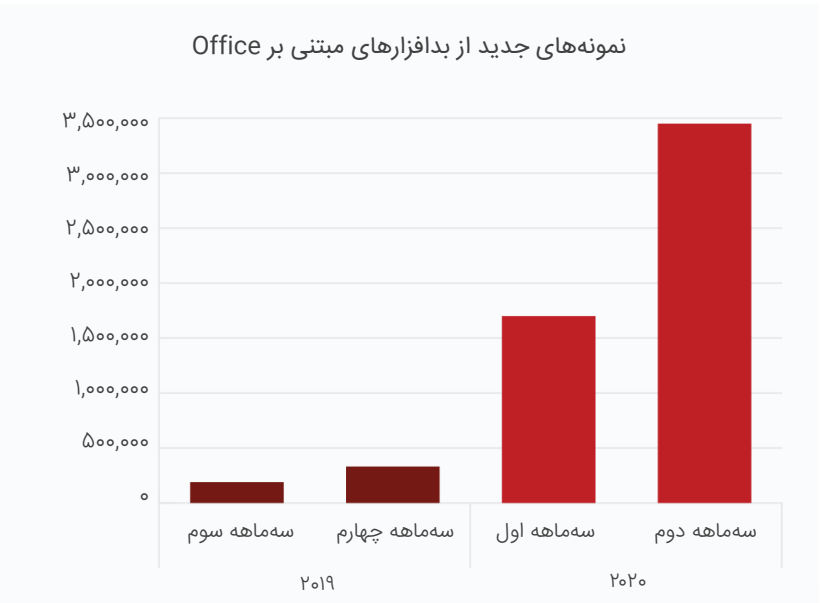


منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰

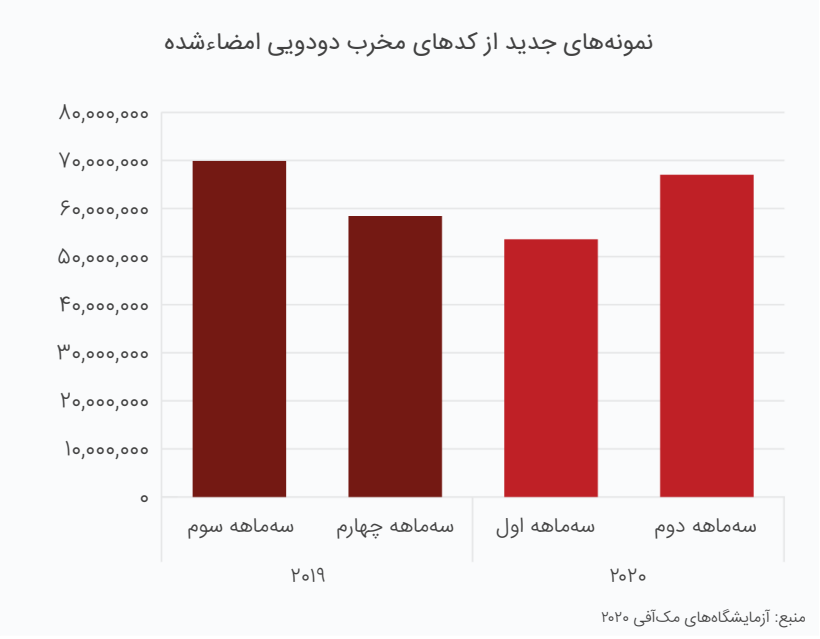
[1] Exploit Malware



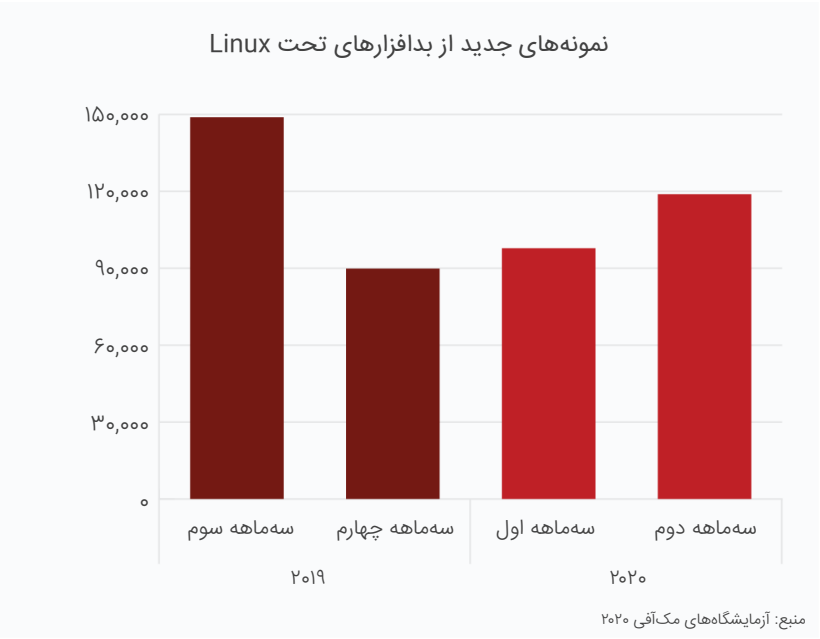
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



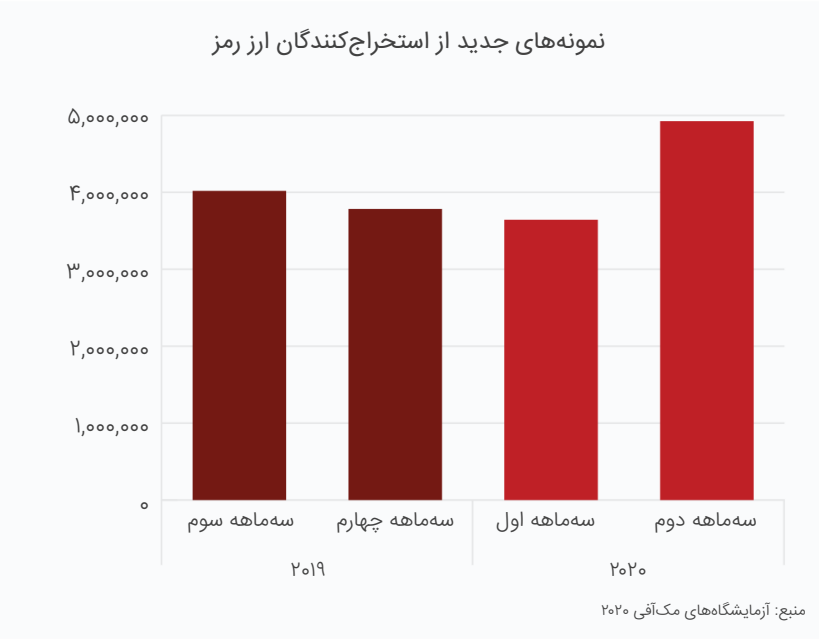
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



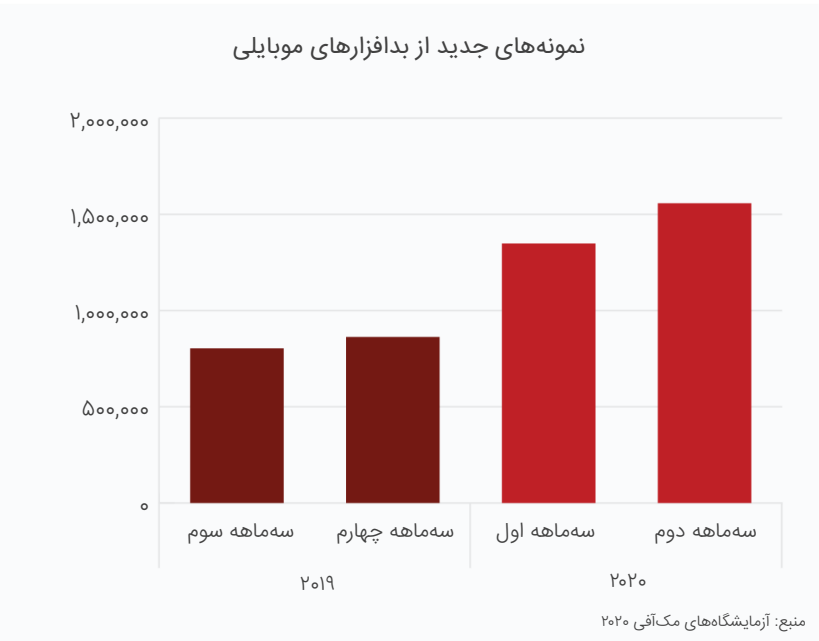
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



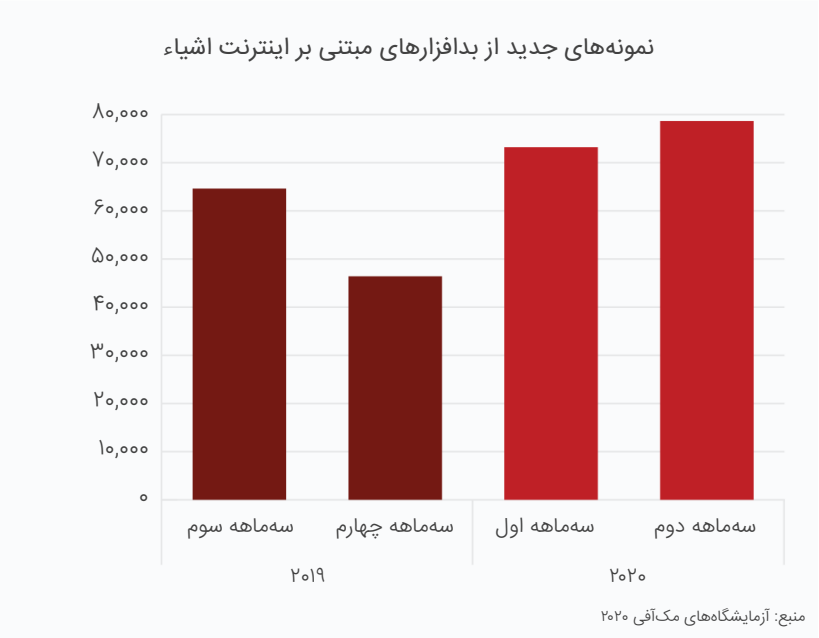
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



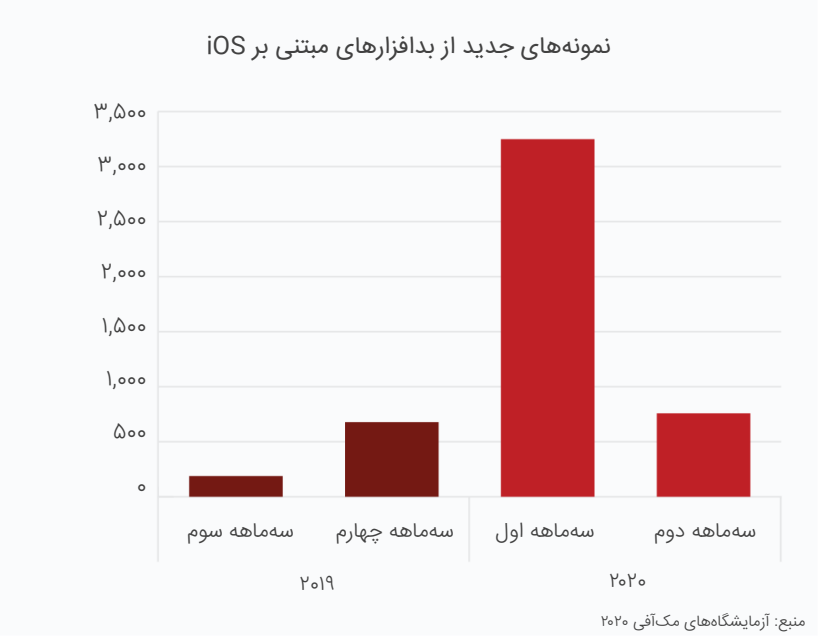
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



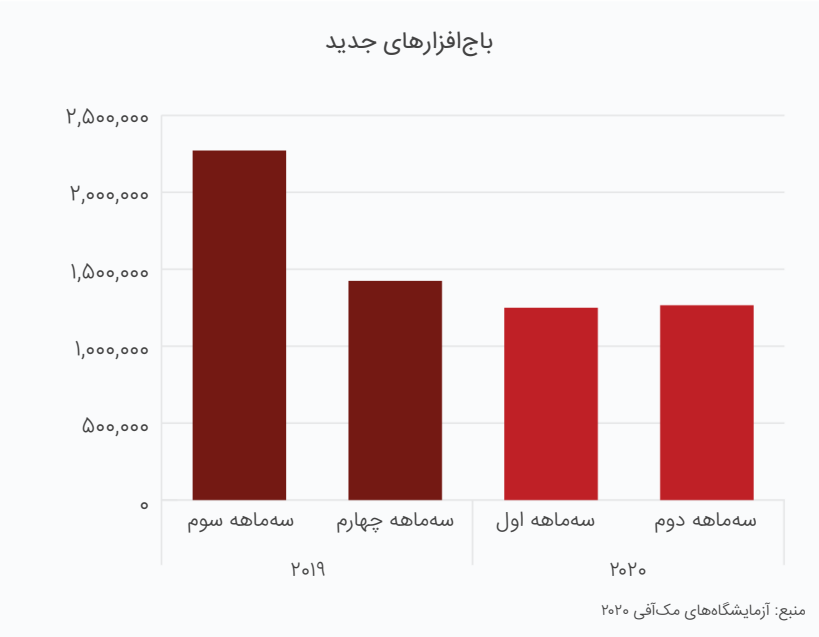
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



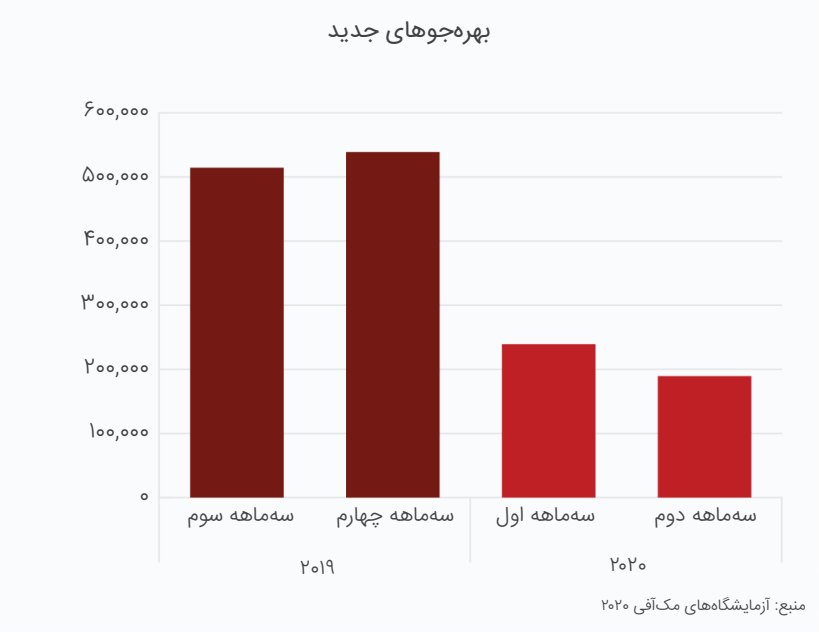
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



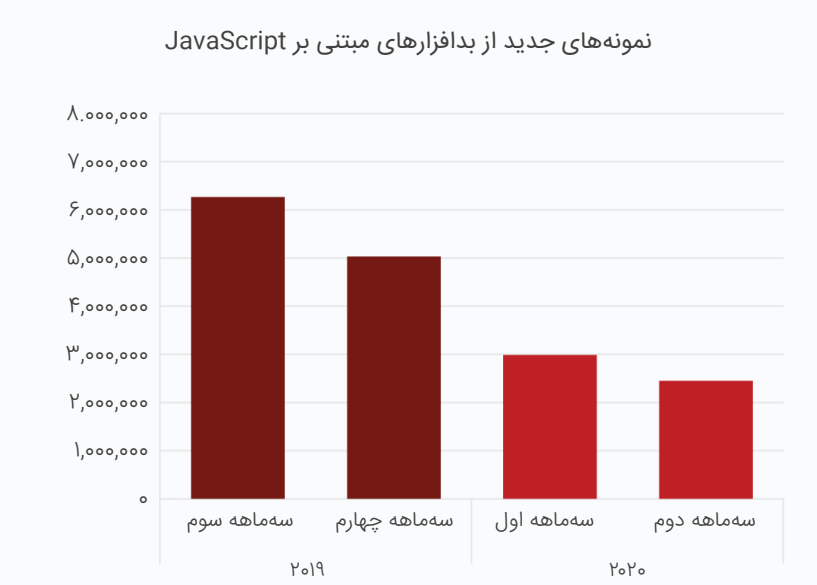
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



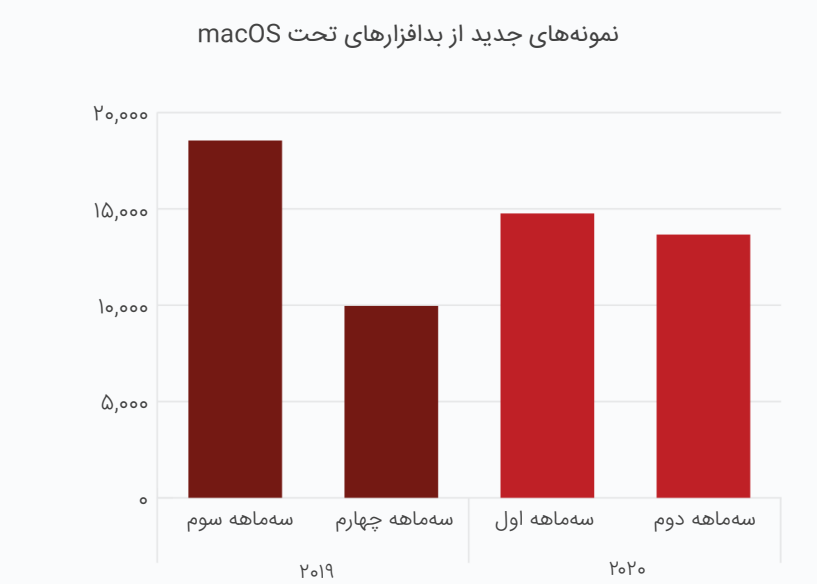
منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰



منبع: آزمایشگاه‌های مک‌آفی ۲۰۲۰

چالش‌های چندابری

در فاصله ژانویه تا آوریل سال ۲۰۲۰ در نتیجه سیاست‌های دولت‌ها در فاصله‌گذاری اجتماعی، استمرار تصمیم شرکت‌ها در دورکار کردن کارکنان که دیگر در حال تبدیل شدن به روالی عادی است و نیاز به سرویس‌های ابری اشتراکی، استفاده از رایانش ابری در نهادهای ایالات متحده ۴۵ درصد افزایش یافت.

معماری‌های موسوم به ترکیبی[۱] و چند ابری[۲] با انعطاف‌پذیری، امنیت و ظرفیت بالای خود می‌توانند پاسخگوی نیازهای امروز و فردای سازمان‌ها با هر اندازه‌ای باشند. اما هنوز این بسترها در ابتدای راه خود قرار دارند و پیاده‌سازی معماری های چند ابری و ترکیبی با چالش‌های زیادی روبروست. سازگار کردن یک رویکرد ابری هوشمند با زیرساخت سازمان پروسه‌ای پیچیده و پردغدغه برای مدیران امنیت اطلاعات است.

نشست مدیران مک‌آفی با رهبران بخش‌های دولتی و خصوصی نشان می‌دهد اگر چه فناوری‌های بکاررفته در زیرساخت بسترهای ترکیبی و چندابری در سال‌های اخیر پیشرفت‌های چشمگیری داشته اما تا حاصل شدن اعتماد کامل به امنیت این بسترها به‌خصوص در سازمان‌های با عملکرد و اطلاعات حساس راه درازی باقی مانده است.

از جمله چالش‌ها در استراتژی‌های توسعه و پیاده‌سازی بسترهای چندابری و ترکیبی می‌توان به موارد زیر اشاره کرد:

۱- استاندارد واحدی که برای تمامی بسترهای ترکیبی قابل اجرا باشد وجود ندارد. سازمان‌ها قابلیت‌های مختلفی را بکار گرفته‌اند که هر کدام دارای اشکالاتی منحصربه‌فرد هستند. توسعه یک سامانه شفاف در خصوص اینکه چگونه سازمان‌ها با موفقیت این اشکالات را برطرف کنند زمان خواهد برد. به‌عبارت دیگر یک فناوری واحد در بسترهای ترکیبی یا چندابری برای سازمان‌هایی که به دنبال پیاده‌سازی این معماری‌ها در زیرساخت خود هستند وجود ندارد.

۲- اعتماد صفر[۳] بر پایه تعریف آن در حال تکامل است. اعتماد صفر، رویکردی است که نیازمند بررسی دقیق و موشکافانه معماری فعلی سازمان است. این یک فناوری خاص نیست. بلکه رویکردی است که باید در تمامی جوانب زیرساخت سازمان برای رسیدن به یک بستر ترکیبی یا چند ابری لحاظ شود.

۳- استراتژی‌های حفاظت از داده‌ها باید با یک سیاست منسجم اعمال شوند. اعمال مستمر سیاست، اساس استراتژی حفاظت از داده‌ها و مدیریت تهدید و بقای آن است. امکان تعیین دسترسی شرطی و متنی به داده‌ها نیازی اساسی برای سازمان‌ها در پیاده‌سازی امن بسترهای اشتراکی مبتنی بر رایانش ابری است.

یکپارچگی موفق بسترهای چندابری چالشی واقعی برای تمامی بخش‌ها، به خصوص سازمان‌های بزرگ با ساختار پیچیده است. مدیریت امنیت در چندین بستر ابری مختلف در اکثر مواقع برای کارکنان بخش فناوری اطلاعات پرچالش بوده و همین موضوع نیاز به ابزارهایی جهت خودکارسازی فرامین آنها و فراهم کردن حفاظت مستمر از اطلاعات حساسی است که میان ابرها و دنیای بیرون تبادل می‌شوند.

مطالعه مقاله زیر در حوزه تهدیدات بسترهای چندابری توصیه می‌شود:

https://www.mcafee.com/blogs/enterprise/cloud-security/multi-cloud-environment-challenges-for-government-agencies/

[۱] Hybrid
[۲] Multi-cloud
[۳] Zero-trust

سوءاستفاده از فراداده‌ها برای رخنه به برنامه‌های AWS

بهره‌گیری از معماری ابری در استفاده از برنامه‌های سازمانی مزایای فراوانی همچون مقیاس‌پذیری و چابکی بالا را به همراه دارد. در عین حال سازمان از اجرای امور طاقت‌فرسایی نظیر نصب اصلاحیه‌ها و ارتقای زیرساخت سرورها رهایی می‌یابد.

اما بکارگیری هر بستر ابری[۱] ریسک‌های خود را دارد. تهدیدات مبتنی بر رایانش ابری از قابلیت‌های جدید و پیکربندی‌ها در بستر ابری سرچشمه می‌گیرند. به‌طور تاریخی تنظیمات پیش‌فرض نظیر دسترسی عمومی به اشیاء ذخیره‌سازی[۲]، داده‌های حساس را به‌سادگی در معرض سرقت شدن توسط هر مهاجمی که این ضعف‌ها را کاوش می‌کند قرار می‌دهد.

طبیعی است که با تنظیماتی که به‌طور مستمر به‌عنوان قابلیت جدید از سوی سرویس‌دهندگان رایانش ابری ارائه می‌شوند بروز اشتباهات نیز افزایش پیدا کند. مسئولیت پیکربندی بسترهای ابری همیشه بر عهده سازمان است. AWS و سایرین کنترلی بر روی نحوه استفاده سازمان از این سرویس‌ها ندارند. صرفاً الگویی برای ساخته شدن از اساس را در اختیار قرار می‌دهند. عدم اطلاع از اثرات پیکربندی‌های اعمال شده و نحوه ساخت برنامه‌های مبتنی بر ابر می‌تواند پیامدهای جبران‌ناپذیری داشته باشد.

در جریان کنفرانس RSA امسال، محققان مک‌آفی نشان دادند که چگونه یکی از قابلیت‌های AWS با عنوان Instance Metadata می‌تواند جهت سرقت داده‌های حساس مورد سوءاستفاده قرار بگیرد؛ در ادامه این گزارش به جزییات این ارائه مک‌آفی پرداخته شده است.

حملات Instance Metadata

تمامی سرویس‌دهندگان رایانش ابری دارای قابلیت‌هایی به‌منظور مدیریت اطلاعات اصالت‌سنجی مورد نیاز جهت دسترسی به منابع برنامه‌های ابری هستند. در صورتی که به‌درستی مورد استفاده قرار بگیرند این قابلیت‌ها مانع از ذخیره اطلاعات اصالت‌سنجی به‌صورت غیرامن یا در انباره منبع کد[۳] می‌شوند. در AWS سرویس Instance Metadata Service - به اختصار IMDS - اطلاعات در خصوص Instance، شبکه آن و ذخیره‌ساز قابل دسترس برای نرم‌افزار اجرا شده بر روی آن Instance را ایجاد می‌کند. همچنین IMDS سبب می‌شود تا اطلاعات اصالت‌سنجی موقت را برای هر نقش IAM الحاق شده به Instance ایجاد کند. برای مثال، نقش‌های IAM الحاق شده به Instance ممکن است تعیین کنند که آن Instance و نرم‌افزار اجرا شده بر روی آن به داده‌های بر روی ذخیره‌ساز S3 دسترسی داشته باشد.

به یک سناریوی متداول نگاه کنیم.

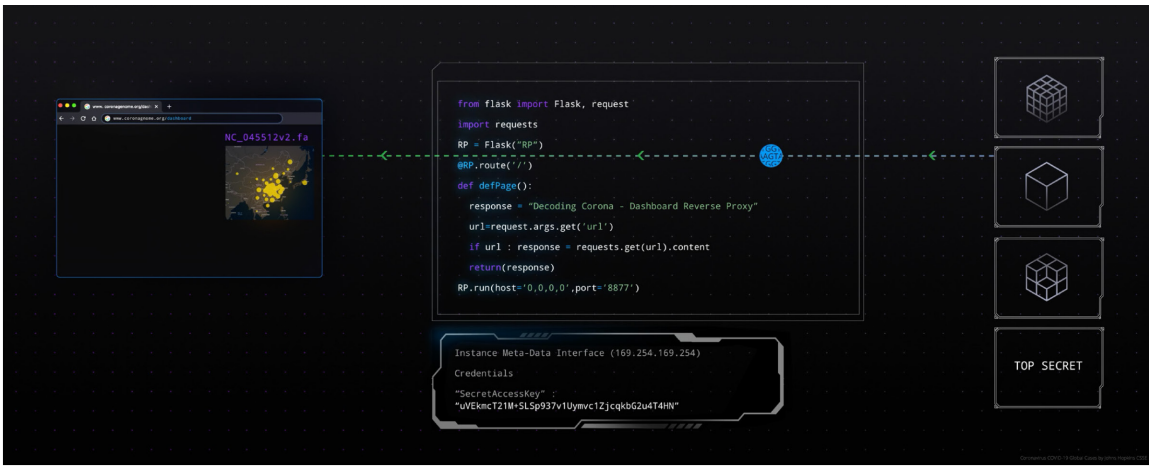
گروهی از متخصصان اپیدمیولوژی برنامه‌ای مبتنی بر رایانش ابری در AWS ساخته‌اند که در آن یافته‌های آنها در خصوص روند تحلیل یک ویروس ژنوم در قالب یک داشبورد به‌صورت عمومی نمایش داده می‌شود.

[۱] AWS، Azure، GCP و...

[۲] Storage Object

[۳] Source Code Repository

در فاز توسعه برنامه، این گروه با یک چالش روبرو شدند. قرار بر این بود که اکثر منابعی که در Virtual Private Cloud - به اختصار VPC - ذخیره شده‌اند بر روی اینترنت قابل دسترس نباشند. تنها منبع بر روی VPC که می‌بایست بر روی اینترنت در دسترس باشد داشبورد برنامه بود. بخش S3 میزبان داده‌ها هم نیاز بود که خصوصی باشد. برای استخراج داده‌های S3 بر روی داشبورد عمومی آنها اقدام به افزودن یک پراکسی معکوس[۱] به‌عنوان یک مرد میانی[۲] کردند. با یک جستجوی سریع در Google و افزودن چند خط کد به برنامه این امر میسر شد.

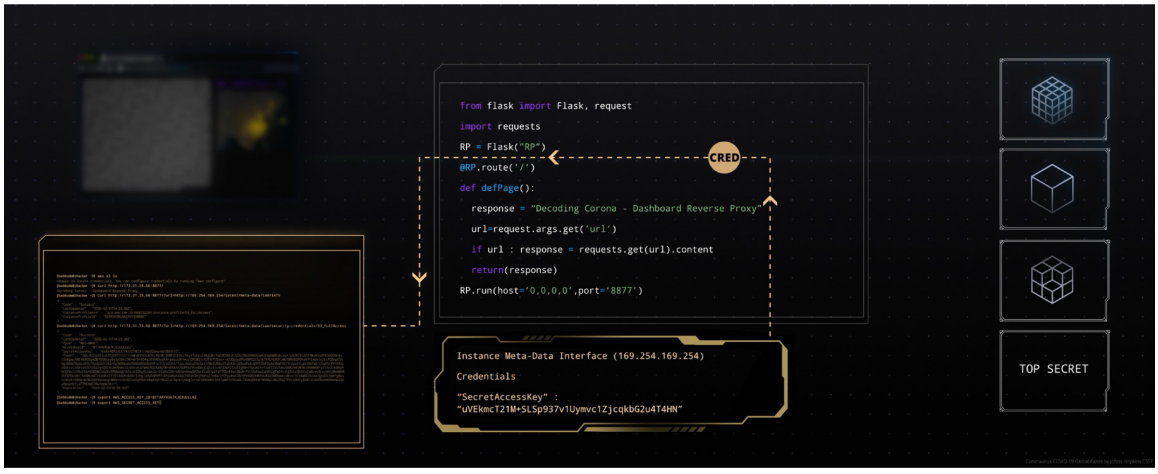


در این سناریو پراکسی معکوس راهکاری است که کاملا مساله آنها را حل می‌کند. اما چیزی که این محققان به آن توجه نکرده‌اند آن است که اکنون با این پیاده‌سازی، آنها در معرض یک حمله سرقت اطلاعات قرار گرفته‌اند.

به Instance که پراکسی معکوس را اجرا کرده یک نقش IAM دارای دسترسی به بخش خصوصی S3 تخصیص داده شده است. اطلاعات اصالت‌سنجی مورد استفاده پراکسی معکوس جهت دسترسی به S3 نیز از Instance Metadata استخراج شده است.

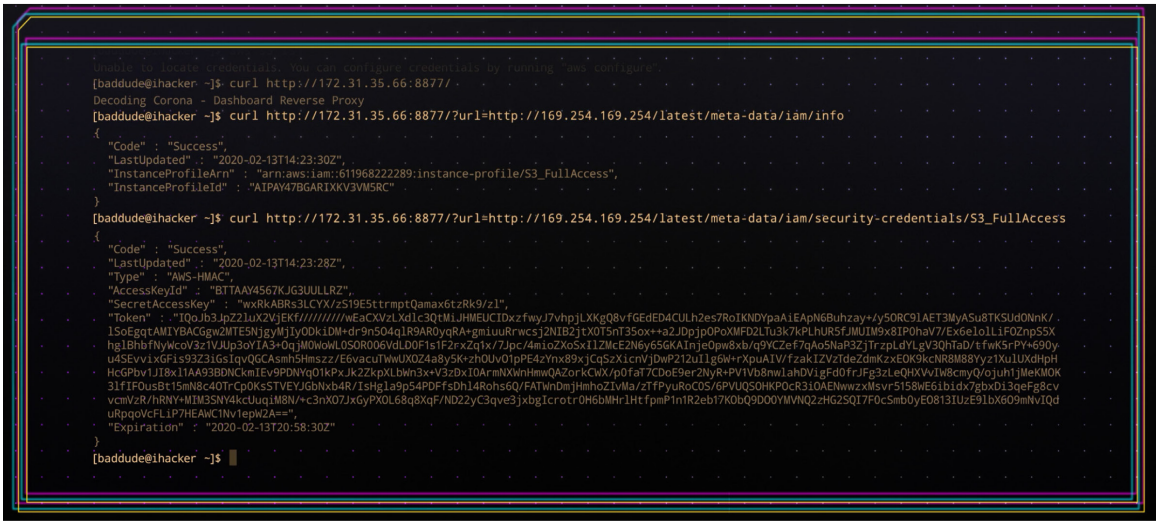
مهاجمی با مرور سایت آنها درمی‌یابد که در داشبورد به نشانی IP پراکسی معکوس اشاره شده است. پس از تلاش برای اتصال به آن و برقراری ارتباط، مهاجم امکان دسترسی به Instance Metadata را مورد بررسی قرار می‌دهد.

در نهایت از طریق پراکسی معکوس و Instance Metadata مهاجم به اطلاعات اصالت‌سنجی لازم جهت دسترسی به بخش خصوصی ذخیره‌ساز S3 دست پیدا می‌کند.



حالا با فراهم شدن دسترسی به S3، مهاجم می‌تواند داده‌های بسیار حساس این محققان را که در برنامه نگهداری می‌شده سرقت کند. تنها کافی است مهاجم باکت S3 آنها را با باکت S۳ خود بر روی یک حساب کاربری AWS دیگر همسانسازی[۳] کند.

۱ Reverse Proxy
۲ Middleman
۳ Sync



این روش حمله تنها یکی از ۴۳ تکنیکی است که MITRE آن را در نسخه بسترهای ابری ATT&CK ارائه کرده است:

https://attack.mitre.org/matrices/enterprise/cloud/

راهکارهای مقاوم سازی AWS در برابر حملات Instance Metadata را در لینک زیر بخوانید:

https://www.mcafee.com/blogs/enterprise/cloud-security/how-an-attacker-could-use-instance-metadata-to-breach-your-app-in-aws/

آسیب‌پذیری‌های یک ربات با کالبدشکافی مک‌آفی

در ادامه فعالیت‌های مستمر بخش تحقیق تهدیدات پیشرفته شرکت مک‌آفی در راستای کمک به برنامه‌نویسان در توسعه محصولات سازمانی و خانگی امن‌تر به‌تازگی محققان این بخش اقدام به بررسی temi که یک ربات ساخت شرکت روبوتمی گلوبال است نموده است. این تحقیقات منجر به کشف چهار آسیب‌پذیری زیر در ربات temi شد:

۱- CVE-2020-16170 - استفاده از اطلاعات اصالت‌سنجی تزریق شده در کد[۱]
۲- CVE-2020-16168 - خطای اعتبارسنجی منبع[۲]
۳- CVE-2020-16167 - عدم اصالت‌سنجی صحیح برای یک تابع حیاتی[۳]
۴- CVE-2020-16169 - عبور از سد اصالت‌سنجی با استفاده از یک مسیر جایگزین کانال[۴]

این آسیب‌پذیری‌ها می‌توانند به‌نحوی مورد سوءاستفاده قرار بگیرند که مهاجم بدخواه را قادر به جاسوسی تماس‌های ویدئویی temi، شنود تماس‌های برقرار شده با کاربر دیگر و حتی هدایت از راه دور ربات، همگی بدون نیاز به هر گونه اصالت‌سنجی کنند.

بر اساس سیاست افشای آسیب‌پذیری شرکت مک‌آفی، این محققان یافته‌های خود را در ۱۵ اسفند ۱۳۹۸ به شرکت روبوتمی گلوبال گزارش کردند. با همکاری مشترک محققان بخش تحقیق تهدیدات پیشرفته مک‌آفی با شرکت روبوتمی گلوبال آسیب‌پذیری‌های مذکور در ۲۵ تیر ۱۳۹۹ ترمیم و اصلاح شدند. این اصلاحیه‌ها در نسخه ۱۲۰ سیستم عامل Robox OS و تمامی نسخ بعد از ۱۶۳۷۹۳۱ بر نامه تحت Android این ربات لحاظ شده‌اند. مک‌آفی از روبوتمی به جهت واکنش سریع و حسن همکاری در این فرایند تمجید کرده است. به نحوی که روبوتمی یکی از پاسخگوترین، فعال‌ترین و کارامدترین سازندگانی توصیف شده که مک‌آفی افتخار کار با آن را داشته است.

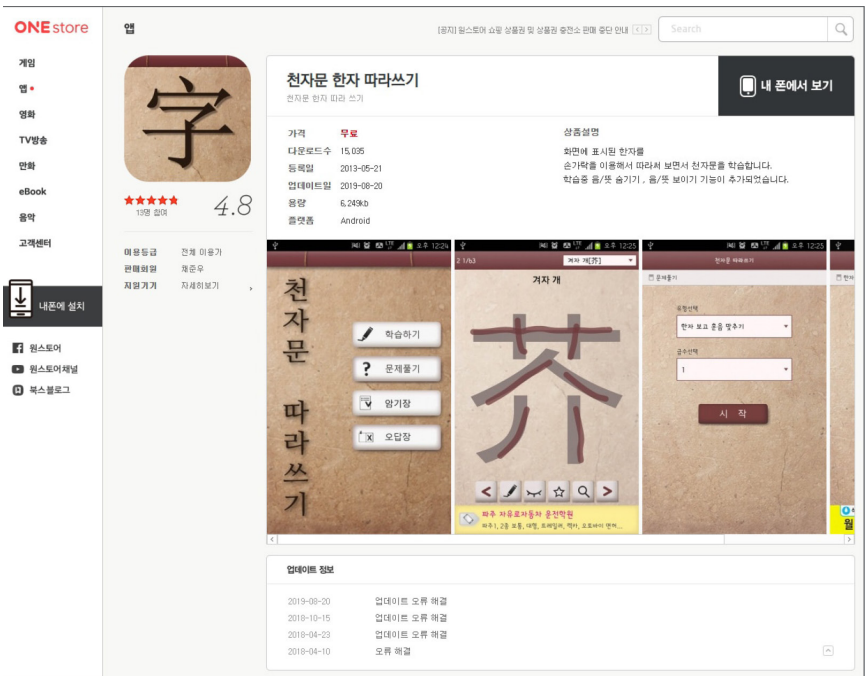
[۱] Use of Hard-Coded Credentials
[۲] Origin Validation Error
[۳] Missing Authentication for Critical Function
[۴] Authentication Bypass Using an Alternate Path of Channel

تغییر بازار از Play Store به ONE Store توسط گرداننده MalBus

بخش تحقیقات موبایل مک‌آفی[1] نسخه دیگری از MalBus را در برنامه‌ای آموزشی که توسط یک برنامه‌نویس اهل کره جنوبی توسعه داده شده کشف کرده است. در نمونه قبلی MalBus، بدافزار از طریق Play Store توزیع می‌شد؛ اما نسخ جدید در روشی مشابه در ONE Store توزیع می‌شوند. ONE Store، سرمایه‌گذاری مشترک سه شرکت مطرح در حوزه مخابرات در کره جنوبی است که بر روی اکثر تلفن‌های با سیستم عامل Android که در این کشور به فروش می‌رسند به‌صورت پیش‌فرض نصب شده است. ONE Store دارای ۳۵ میلیون کاربر است که از اواخر ۲۰۱۸ از Apple App Store پیشی گرفته است.

برنامه موضوع بحث همزمان از طریق Play Store و ONE Store توزیع می‌شده است. نسخه آلوده برنامه از طریق توابعی مخرب کد رمزگذاری شده را دریافت و اجرا می‌کند.

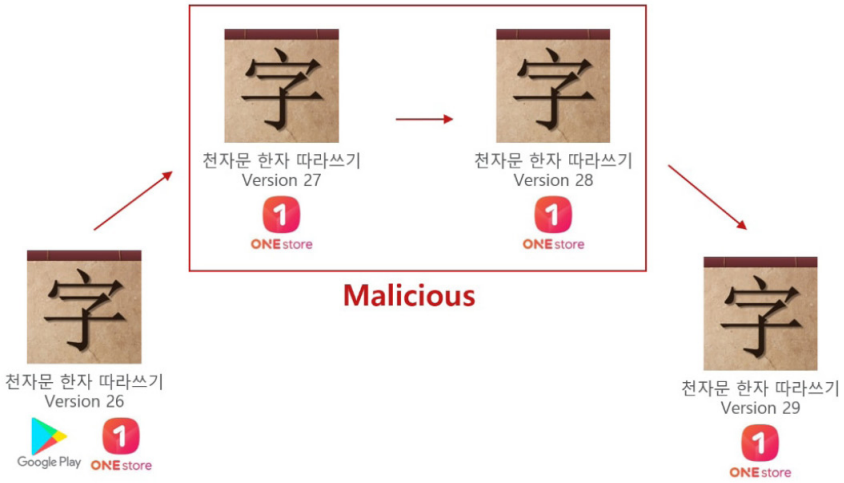
مک‌آفی این تهدید را با عنوان Android/Malbus شناسایی می‌کند.



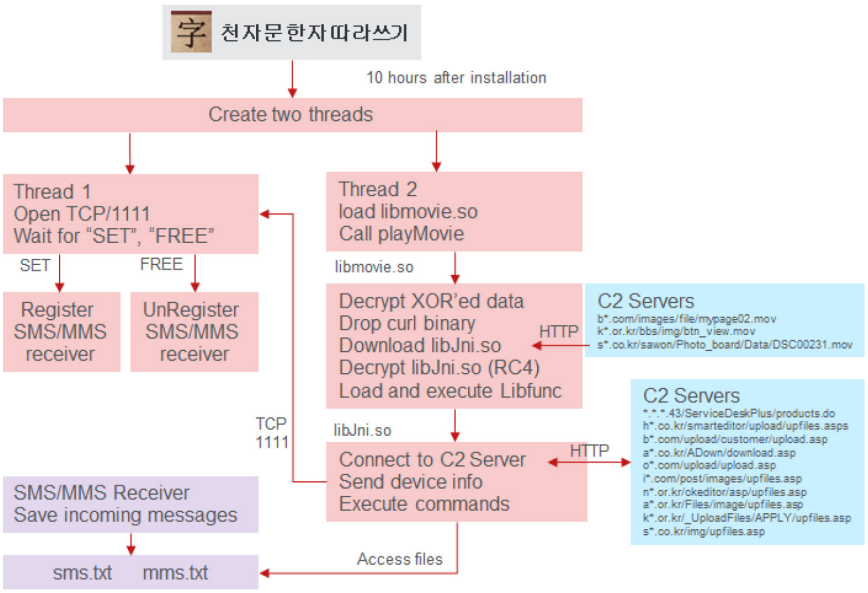
کارزار

کد مخرب از طریق یک حساب کاربری به نسخ ۲۷ و ۲۸ برنامه که در بستر ONE Store قابل دسترس است تزریق شده است. گواهینامه موسوم به App Signature Certificate برای نسخ ۲۶ تا ۲۹ که از طریق ONE Store توزیع شده‌اند یکسان است. هیچ برنامه دیگری که توسط این نویسنده توسعه داده شده باشد بر روی ONE Store شناسایی نشده است. در حال حاضر در ONE Store نسخه ۲۹ را سرویس می‌دهد که حاوی کد مخرب نیست. در Play Store همچنان نسخه ۲۶ توزیع شده است؛ اگر چه نسخه مذکور نیز در Play Store فاقد آلودگی است.

[1] McAfee Mobile Research



جریان کلی این برنامه با تمرکز بر روی تابع مخرب در زیر نمایش داده شده است.



پس از آن که بدافزار نصب می‌شود کد مخرب با تاخیری ۱۰ ساعته - به‌منظور عبور از سد سازوکارهای موسوم به تحلیل پویا - اجرا می‌گردد.

به‌روش‌های مقابله با آسیب‌پذیری Ripple20

۲۷ خرداد ۱۳۹۹ چندین نهاد امنیتی ایالات متحده با انتشار توصیه‌نامه‌ای حیاتی نسبت به اثرگذاری چند آسیب‌پذیری جدید بر روی دستگاه‌های متصل به اینترنت ساخت شرکت‌های مختلف هشدار دادند. این مجموعه ۱۹ عددی از آسیب‌پذیری‌ها که از آنها با عنوان Ripple20 یاد شده کتابخانه نرم‌افزاری سطح پایین TCP/IP را که توسط شرکت Treck توسعه داده شده متأثر می‌کند.

این استک شبکه‌ای، جزیی نرم‌افزاری است که ارتباط شبکه‌ای را در بستر پودمان‌های استاندارد اینترنتی برقرار می‌کند. در این مورد به‌خصوص این پودمان‌ها شامل پودمان‌های ارتباطی ARP، IP[1]، ICMPv4، UDP و TCP و همچنین پودمان‌های برنامه‌ای DNS و DHCP است. استک شبکه‌ای Treck در بسیاری از حوزه‌ها[2] به واسطه بکارگیری آن توسط دستگاه‌های ساخت سازندگان مختلف مورد استفاده قرار می‌گیرد. موضوعی که گسترده بودن دامنه آن و چالش هایی همچون آن که هر سازنده مستقلا نیاز به اعمال به‌روزرسانی بر روی دستگاه‌های ساخت خود هستند. به‌عبارت دیگر تاثیر Ripple20 به دلیل پیچیدگی در زنجیره تأمین و طراحی است.

شناسایی دستگاه‌های آسیب‌پذیر در شبکه سازمان گامی کلیدی در ارزیابی ریسک Ripple20 است. یک جستجوی ساده "treck" در www.shodan.io حدود ۱۰۰۰ دستگاه را که به احتمال زیاد دستگاه‌های آسیب‌پذیر قابل دسترس بر روی اینترنت هستند استخراج می‌کند. این تنها بخشی از دستگاه‌های متأثر است.

شناسایی استک شبکه‌ای Treck در مقایسه با سایر استک‌های شبکه‌ای[3] نیازمند انجام تحلیل با جزییات و انگشت‌نگاری تکنیک‌ها بر اساس نتایج پویش‌های شبکه‌ای دستگاه‌های موضوع بحث است.

تأثیر این آسیب‌پذیری‌ها متعدد بوده و از از کاراندازی سرویس[4] تا اجرای کامل کد به‌صورت از راه دور بر روی اینترنت را شامل می‌شود که حداقل در یک مورد[5] بهره‌جویی از آسیب‌پذیری مستلزم اصالت‌سنجی نیست. بررسی محققان نشان می‌دهد که این آسیب‌پذیری‌ها ترکیبی از دستگاه‌های سنتی و اینترنت اشیاء را متأثر می‌کنند. از آنجا که دستگاه‌های غیر اینترنت اشیاء نیز ممکن است ثابت‌افزاری[6] را اجرا کنند که در آن استک شبکه‌ای Treck مورد استفاده قرار گرفته مشتریان باید توصیه‌نامه سازندگانی همچون اینتل[7] و اچ‌پی[8] را بررسی کنند.

خطر Ripple20 بیش از همه متوجه دستگاه‌هایی که استک شبکه آنها تأثیرپذیر از آسیب‌پذیری‌های مذکور است[9] - در مقایسه با دستگاه‌هایی که استک آنها تنها در دسترس دستگاه محلی است - می‌باشد. مک‌آفی به راهبران توصیه می‌کند که با ممیزی تمامی دستگاه‌های با ارتباط شبکه‌ای فعال، آسیب‌پذیر بودن آنها به ضعف‌های امنیتی مذکور را بررسی کنند.

به‌طور بالقوه ده‌ها میلیون دستگاه حداقل به یکی از ضعف‌های Ripple20 آسیب‌پذیر هستند. کاهش شدت خطر نیازمند انجام اقداماتی توسط صاحبان دستگاه‌ها و در عین حال سازندگان دستگاه‌هاست. در خصوص صاحبان دستگاه‌ها می‌توان به اقدامات زیر اشاره کرد:

- ترمیم هر دستگاهی که سازنده آن برای آن به‌روزرسانی عرضه کرده است.
- حداقل دسترسی به تمامی کاربران و دستگاه‌ها[1] تخصیص داده شود؛ در این مورد به‌خصوص در معرض شبکه قرار داشتن و قابل دسترس بودن بر روی اینترنت برای همه دستگاه‌های کنترل سیستم[2] باید به حداقل برسد.
- شبکه‌های سیستم کنترلی و دستگاه‌های از راه دور در پشت دیواره آتش را شناسایی کرده و آنها را از شبکه سازمان قرنطینه کنید.
- زمانی که دسترسی از راه دور نیاز است از روش‌های امن، نظیر Virtual Private Networks - به اختصار VPN - استفاده شود. با این توضیح که ابزارهای VPN خود نیز ممکن است آسیب‌پذیری داشته باشند و باید از آخرین نسخه آنها بهره گرفته شود. همچنین باید توجه داشت که یک VPN به امنی دستگاه‌های متصل است. در راهکارهای VPN باید از اصالت‌سنجی چندعاملی[3] استفاده شود.
- از سرورهای DNS با قابلیت Caching در سازمان استفاده شده و پرس‌وجوهای DNS مستقیم به سمت اینترنت مسدود شوند. ایده‌آل آن است که سرورهای Caching DNS از DNS-over-HTTPS برای جستجوها استفاده کنند.
- ترافیک IP غیرعادی با ترکیب دیواره آتش و سیستم‌های نفوذیاب مسدود شود.

[1] نسخ ۴ و ۶
[2] پرشکی، دولتی، دانشگاهی، خدمات رفاهی و غیره
[3] نظیر استک‌های بومی لینوکس یا استک‌های ویندوز
[4] Denial of Server
[5] CVE-2020-11901
[6] Firmware
[7] https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html
[8] https://support.hp.com/in-en/document/c06640149
[9] به‌طور کلی دستگاه‌های اینترنت اشیاء که از استک شبکه‌ای Treck بهره می‌گیرند.

فیشینگ OneDrive

کلاهبرداران سایبری با روش‌های مختلف اطلاعات شخصی کاربران را هدف قرار می‌دهند. در یکی از نمونه‌های اخیر، این افراد با سوءاستفاده از ترس ناشی از همه‌گیری کرونا اقدام به ارسال ایمیل‌های فیشینگ و کلاهبرداری از کاربران OneDrive کرده‌اند. در ایمیل‌های ارسالی وانمود می‌شود که فرستنده دولت، شرکت‌های مشاوره یا سازمان‌های خیریه است. اما در واقعیت هدف آنها سرقت اطلاعات حساس حساب کاربری نظیر نام‌های کاربری و رمزهای عبور است.

در مواردی نیز تظاهر می‌شود که ایمیل‌ها از سوی دفاتر دولتی ارسال شده‌اند و شامل اسنادی شامل آخرین نظرسنجی‌های مرتبط با کووید-۱۹ هستند. با نگاهی دقیق به نشانی ایمیل ارسالی و موقعیتی که در سرآیند ایمیل به آن اشاره شده و همچنین با مراجعه به سایت معتبر دولتی در خصوص اطلاعاتی که در ایمیل به آنها اشاره شده می‌توان به جعلی بودن ایمیل پی برد.

در نمونه مذکور هدف از نمایش پیام هشدار "Hmm... looks like this file doesn't have a preview we can show you" فریب کاربر در کلیک بر روی دگمه Open است که در صورت به دام افتادن قربانی در مرحله بعد از او درخواست می‌شود که اطلاعات شخصی خود را وارد کند.

در حقیقت کلیک بر روی لینک کاربر را به یک سایت مبتنی بر نسخه آسیب‌پذیر WordPress هدایت می‌کند که به اصطلاح نقش صفحه فرود[۵] فیشینگ اطلاعات اصالت‌سنجی را بر عهده دارد. بدیهی است که صفحه ثبت ورود[۶] سرویس OneDrive نمی‌تواند بر روی دامنه‌ای به غیر از دامنه‌های متعلق به شرکت مایکروسافت - به‌عنوان صاحب OneDrive - میزبانی شده باشد. این باید هشدار برای کاربری باشد که هدف چنین حمله کلاهبرداری یا فیشینگ قرار گرفته است.

همان‌طور که کلاهبرداران قصد دارند کاربر نمی‌تواند به سند OneDrive که در ظاهر حاوی جدیدترین پرسشنامه دولتی است دسترسی داشته باشد؛ در عوض پیام خطایی در خصوص تلاش مجدد را مشاهده می‌کند.

در این مرحله، دیگر کلاهبرداران اطلاعات شخصی قربانی را سرقت کرده‌اند.

همچنین کلاهبرداران تلاش می‌کنند تا داوطلبان و علاقمندان به کمک به دیگران را از طریق اسناد امن شده و ایمیل‌های سازمان‌های خیریه جعلی فریب دهند.

اطلاعات بیشتر در خصوص تحقیقات مک‌آفی در مورد فیشینگ مبتنی بر OneDrive را به همراه بهترین راهکارهای مقابله با آنها در لینک زیر بخوانید:

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/onedrive-phishing-awareness/

[۱] دستگاه‌ها و کاربران باید تنها به مجموعه‌ای از قابلیت‌های مورد نیاز برای انجام وظایفشان داشته باشند.
[۲] Control System
[۳] Multi-factor Authentication
[۴] Denial of Service
[۵] Landing Page
[۶] Login

شرکت McAfee در سال ۱۹۸۷ توسط بنیانگذار آن، John McAfee، تأسیس شد. بعدها، وی سهام خود را به‌طور کامل فروخت و از شرکت کناره‌گیری کرد ولی نام McAfee همچنان با این شرکت باقی ماند. البته برای مدت کوتاهی از اواخر دهه ۱۹۹۰ میلادی تا سال ۲۰۰٤، نام شرکت به Network Associates تغییر یافت ولی دوباره با تصمیم مدیران شرکت، نام McAfee انتخاب شد. در سال ۱۹۹۸ این شرکت اقدام به خرید شرکت Dr. Solomons که شرکت مهندسی شبکه گستر نمایندگی انحصاری آن را در ایران داشت، نمود. در سال ۲۰۱۰، شرکت Intel با پرداخت ۷/۷ میلیارد دلار، McAfee را به‌طور کامل خرید و در اختیار گرفت. در پی آن شرکت McAfee با حفظ ساختار، به‌عنوان یک شرکت تابعه متعلق به اینتل تحت مجموعه بزرگ Intel Security به فعالیت خود ادامه داد. در اواخر سال ۲۰۱٦ شرکت سرمایه‌گذاری TPG Capital اقدام به خرید ۵۱ درصد از سهام Intel Security از Intel نمود و این شرکت از اوایل سال ۲۰۱۷ فعالیت رسمی خود را با منابع و سرمایه‌ای بیشتر اما به‌صورت مستقل از دو شرکت صاحب سهام خود - Intel و TPG Capital - با همان نام قدیمی McAfee و با شعار جدید "قدرت در با همدیگر بودن است" (Together is power.) آغاز کرد. McAfee با بیش از ۷ هزار متخصص و اختراع بیش از ۱۵۵۰ فناوری ثبت شده یکی از بزرگترین و اصلی‌ترین تأمین‌کنندگان امنیت نقاط پایانی در جهان است. در حال حاضر ٦۲۲ میلیون نقطه پایانی در سرتاسر جهان تحت پوشش محصولات McAfee قرار دارند. ۸۷ درصد از بزرگترین بانک‌های جهان و ۸۰ درصد از یکصد شرکت برتر (موسوم به Fortune 100) از محصولات شرکت McAfee برای حفاظت از سیستم‌های خود استفاده می‌کنند.

شبکه گستر

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.

شبکه گستر
امنیت شما | وظیفه ما

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳
تلفن / دورنگار ۴۲۰۵۲-۰۲۱
www.shabakeh.net info@shabakeh.net