McAfee

گزارش و آمار فصلی از فعالیت بدافزارها و تهدیدات سایبری

ویژه‌نامه کرونا

شبکه گستر

امنیت شما | وظیفه ما

چکیده مدیریتی

سال ۲۰۲۰ در حالی آغاز شد که بحران همه‌گیری ویروس کووید-۱۹ و ترس عمومی از آن، کاربران نگران و جویای کسب اطلاعات در خصوص این بیماری را به هدفی آسیب‌پذیر برای تبهکاران سایبری و گردانندگان حملات فیشینگ تبدیل کرد.

در این گزارش اختصاصی، شرکت امنیتی مک‌آفی با نگاهی عمیق به بررسی تهدیدات مرتبط با کووید-۱۹ پرداخته است. علاوه بر آن مک‌آفی با راه‌اندازی سامانه‌ای با عنوان McAfee COVID-19 Threats Dashboard[۱] دامنه آگاهی رسانی خود را فراتر از این گزارش برده و با ارائه اطلاعات فوری و لحظه‌ای، راهبران شبکه و مدیران امنیت سازمان‌ها را از آن دسته از تهدیدات فعالی که در حال بهره‌جویی از بحران کرونا هستند هوشیار می‌کند.

سوءاستفاده مهاجمان سایبری از همه‌گیری کووید-۱۹ برای هدف قرار دادن کارکنانی که به دلیل شیوع این ویروس از منزل و خارج از محدوده امن سازمان به دورکاری می پردازند از همان ابتدا دور از انتظار نبود. فراهم کردن بستری امن در زمانی که سازمان‌ها به‌صورت اضطراری و فوری ناچار شدند تا بدون تجربه قبلی اقدام به دورکار کردن عده زیادی از کارکنان خود کنند چالشی جدی برای مراکز عملیات امنیتی[۲] و مدیران ارشد فناوری[۳] بود.

در این دوران فراهم شدن امکان مشارکت و تأمین سیستم‌هایی کارا مستلزم اعتماد به کارکنان برای رسیدگی به کارهایشان در بستر اینترنت است. از سویی دیگر نگرانی از تغییر روال‌ها، رسیدگی به نیازهای جدید خانواده در دوران قرنطینه، لزوم حفظ فاصله‌گذاری اجتماعی، وسایل بهداشتی و حفاظتی مورد نیاز، کمبودها و در عین حال افزایش نیازها، بیکاری روز افزون و حذف برخی مزایا بسیاری را در معرض فشارهای روانی و استرس قرار داده است. در این برهه از زمان، تبهکاران سایبری نیروهای انسانی دورکار، پریشان و آسیب‌پذیر را هدف و ابزاری عالی برای رسیدن به اهداف پلید خود دیدند.

مهاجمان با تکنیک‌های مهندسی اجتماعی و موضوعاتی مرتبط با کووید-۱۹، اقدام به ارسال هرزنامه‌های کلاهبرداری و راه‌اندازی سایت‌های با محتوای جعلی برای به دام انداختن کارکنان دورکار کردند. این افراد کوشیدند تا با سوءاستفاده از آسیب‌پذیری‌های ناشی از این همه‌گیری، کارکنان و به تبع آن سازمان را هدف انباره بدافزارهای خود قرار داده و به شبکه داخلی سازمان‌ها راه پیدا کنند.

از همان گزارش‌های اولیه در خصوص شیوع ویروس کرونا محققان مک‌آفی تاکتیک‌ها و تکنیک‌های مهاجمان سایبری را که از این بحران برای پیش‌برد اهداف پلید خود بهره می‌بردند مورد رصد قرار دادند. ما تلاش کرده‌ایم تا با شناسایی سریع این تهدیدات مشتریان و جامعه امنیت را به سلامت مقصد برسانیم.

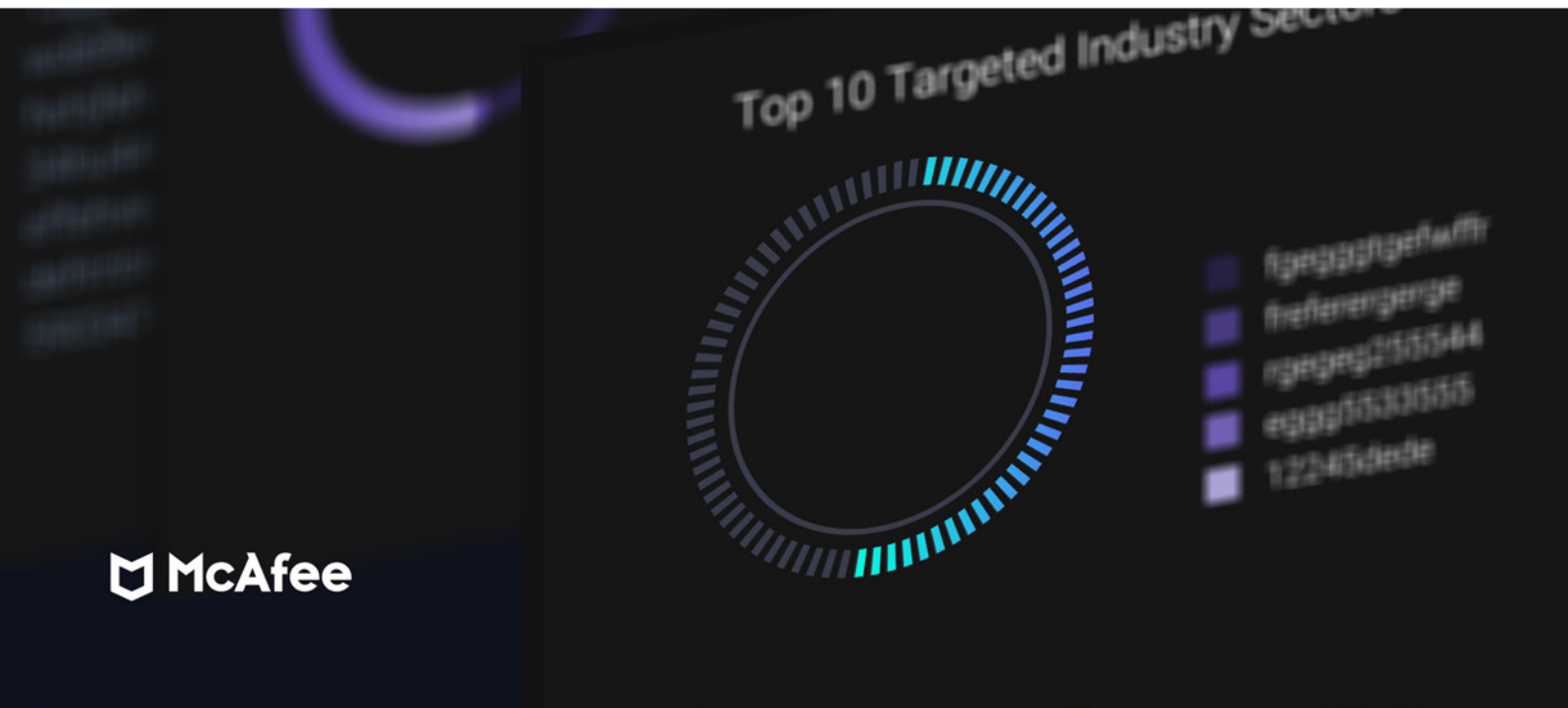
در این گزارش ضمن ارائه آمار تهدیدات سایبری در سه‌ماهه اول سال ۲۰۲۰ برخی نمونه‌ها از تلاش تبهکاران سایبری در سوءاستفاده از بحران کرونا مورد بررسی و تحلیل قرار گرفته است.

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

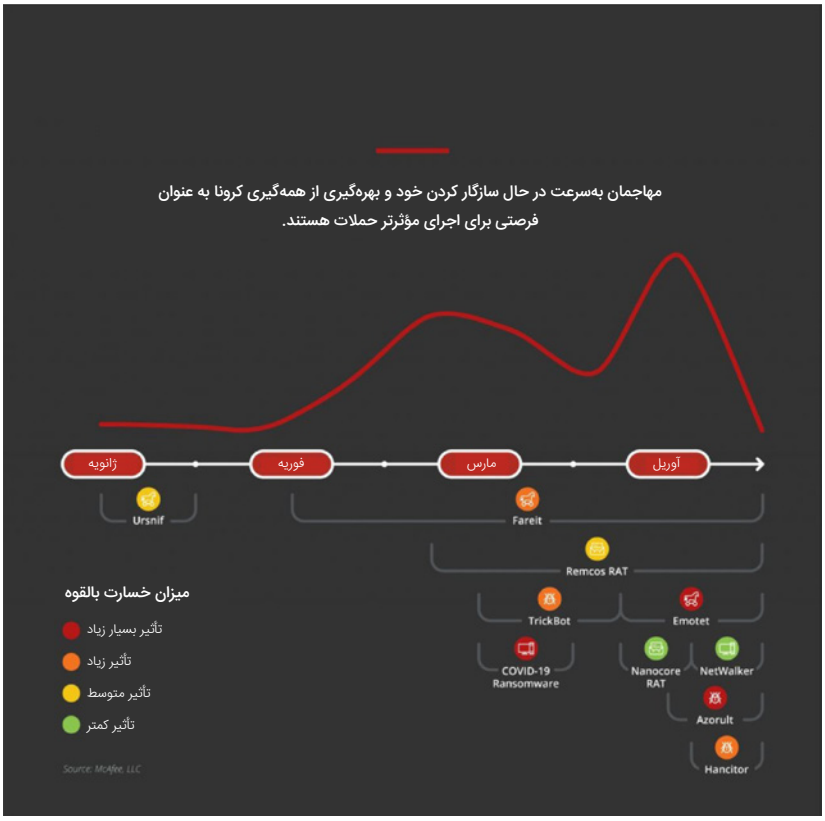
[۲] SOC

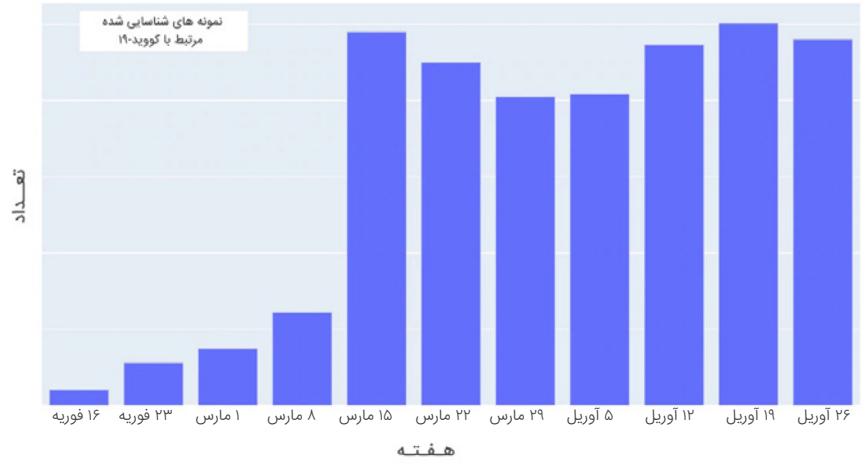
[۲] CTO

فهرست مطالب



جدول زمانی و روش‌های توزیع تهدیدات سایبری مرتبط با کووید-۱۹



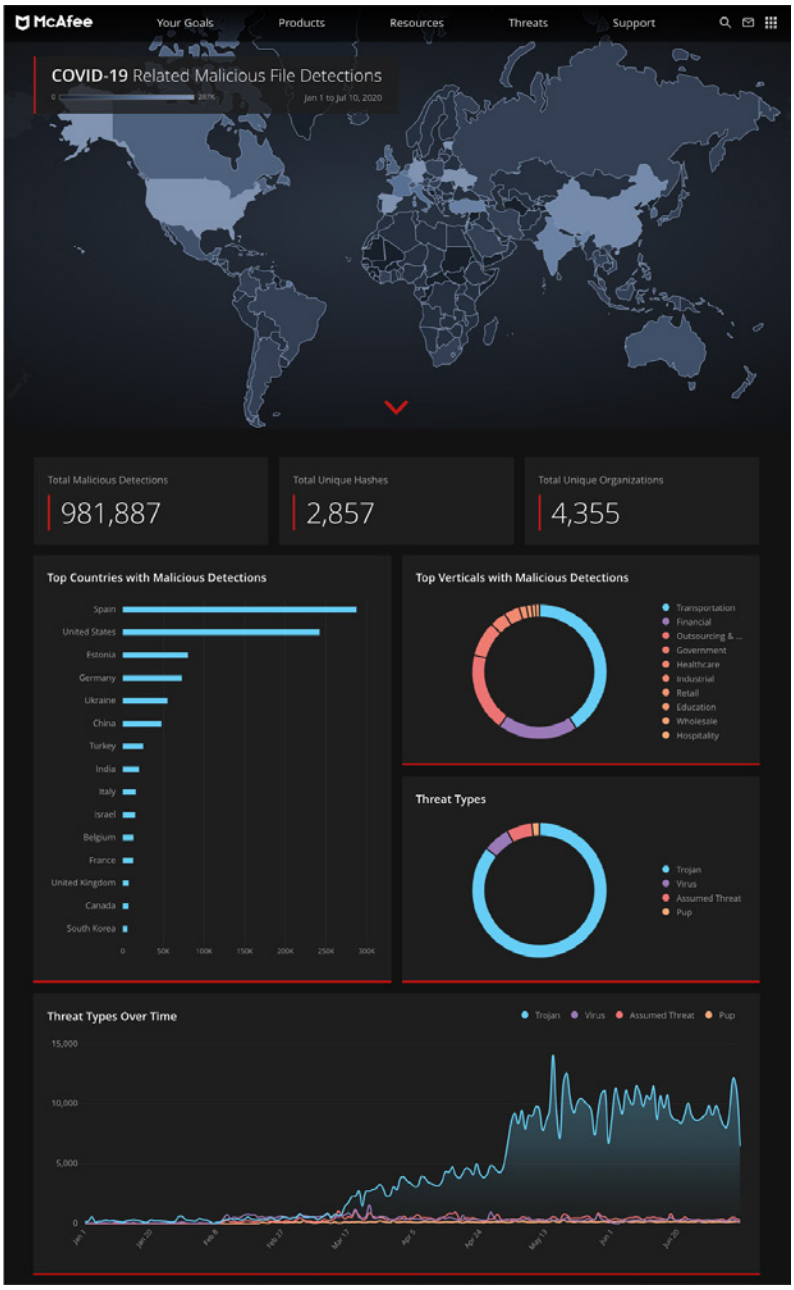


بخش‌های در معرض حمله

تعداد انواع تهدیدات و حملاتی که در آنها موضوعات مرتبط با بیماری کووید-۱۹ به عنوان طعمه استفاده شده قابل توجه است. مک‌آفی فعالیت این نوع تهدیدات مخرب را تقریباً در تمامی کشورهایی که متأثر از شیوع ویروس کووید-۱۹ هستند شاهد بوده است. گرچه تفاوت تعداد در برخی نقاط به‌نحو فاحشی متفاوت از نقاط دیگر بوده است.

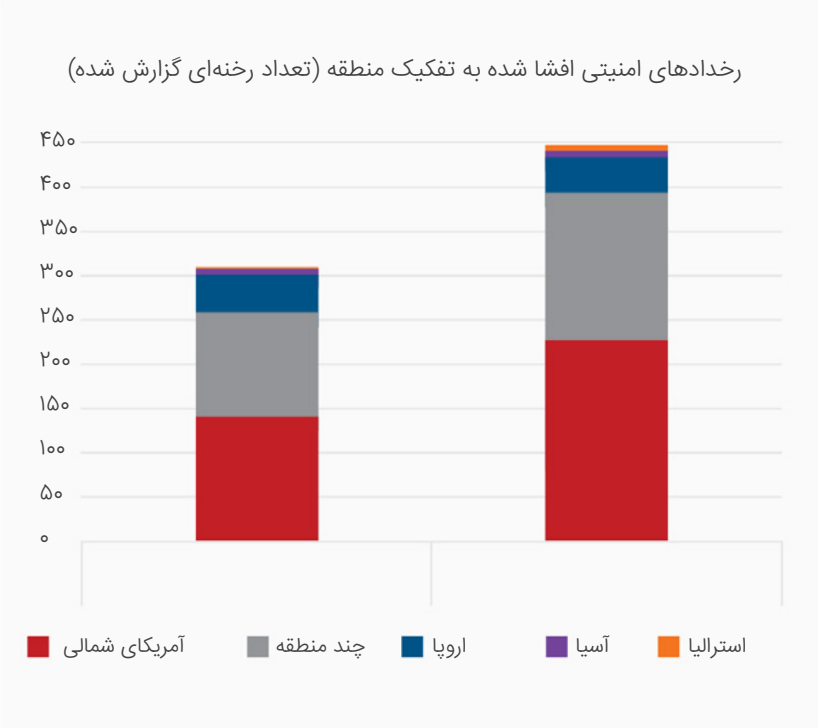
اهداف و روش‌های اجرای این تهدیدات

نخستین نمونه از این تهدیدات در اواسط ژانویه به دست مک‌آفی رسید. سامانه McAfee COVID-19 Threat Dashboard[1] اطلاعات باارزشی را که به‌صورت مستمر توسط گروه برنامه‌های پیشرفته مک‌آفی[2] به‌روزرسانی می‌شود ارائه می‌کند.

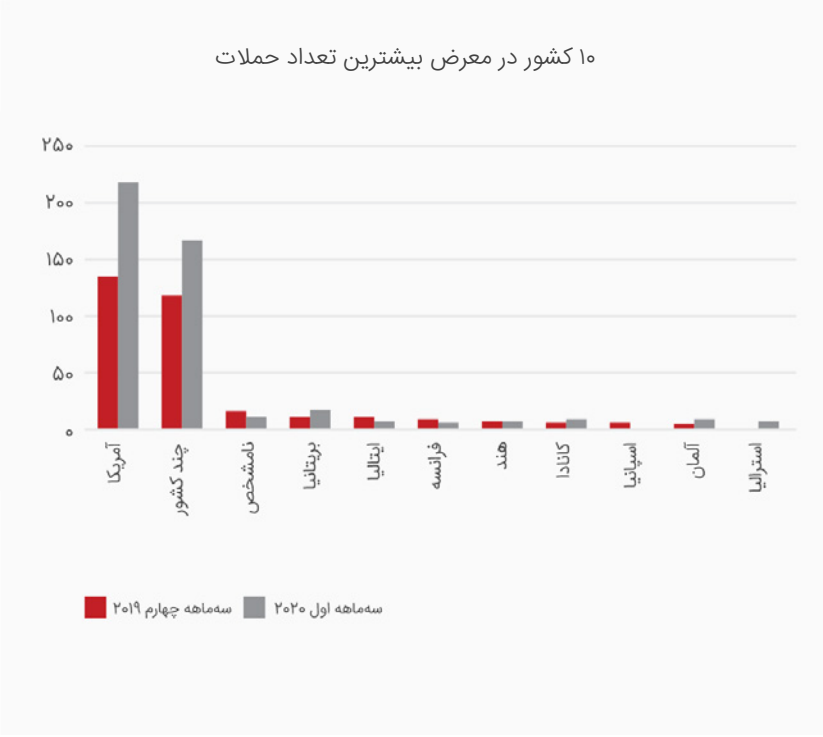


[1] https://www.mcafee.com/enterprise/en-us/lp/covid-19-dashboard.html

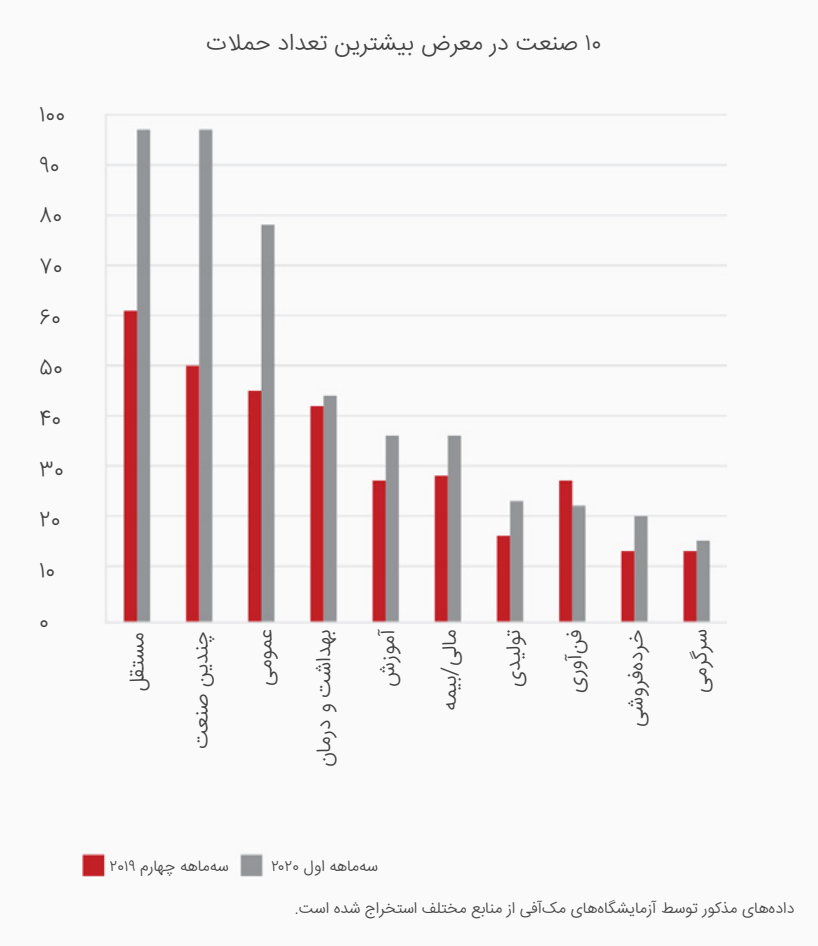
[2] McAfee Adavanced Programs Group



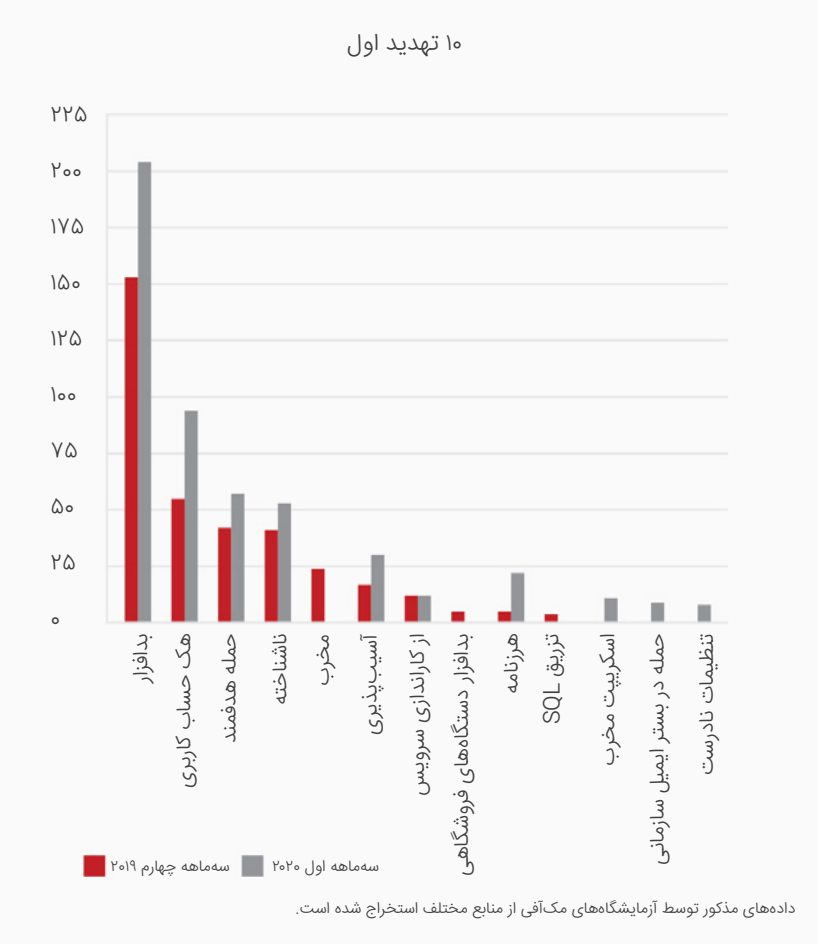
محققان مک‌آفی در سه‌ماهه اول سال ۲۰۲۰، حدود ٤٦۰ رخداد امنیتی را که به‌صورت عمومی افشا شده بودند مورد رصد قرار دادند که افزایشی ٤۱ درصدی نسبت به سه‌ماهه چهارم ۲۰۱۹ را نشان می‌دهد. تعداد رخدادهای افشا شده‌ای که در آنها آمریکای شمالی هدف قرار گرفته افزایشی ٦۰ درصدی را نسبت به سه‌ماهه قبلی نشان می‌دهد؛ در عین حال در منطقه اروپا ۷ درصد کاهش را شاهد بودیم.



در سه‌ماهه اول ۲۰۲۰ تعداد رخدادهای گزارش شده‌ای که آمریکا، بریتانیا و کانادا را هدف قرار دادند به ترتیب ٦۱، ۵۵ و ۵۰ درصد نسبت به دوره پیشین افزایش داشتند.



تعداد رخدادهای افشا شده‌ای که در سه‌ماهه اول ۲۰۲۰ چندین صنعت، حوزه عمومی، صنایع مستقل و بخش‌های تولیدی از آنها تأثیر پذیرفتند به‌ترتیب ۹۴، ۷۳، ۵۹ و ٤٤ در مقایسه با دوره پیشین افزایش داشته است. در عین حال تعداد رخدادها در بخش علوم و فنون کاهشی ۱۹ درصدی داشته است.



داده‌های مذکور توسط آزمایشگاه‌های مک‌آفی از منابع مختلف استخراج شده است.

به‌طور کلی، بدافزارها، هک حساب های کاربری و حملات هدفمند بیشترین سهم از رخدادهای امنیتی گزارش شده در سه‌ماهه اول ۲۰۲۰ را به خود اختصاص دادند. از میان رخدادهای گزارش شده به‌صورت عمومی، بدافزارها ۳۳ درصد، هک حساب‌های کاربری ۷۱ درصد و حملات هدفمند ٦٠ درصد نسبت به دوره قبلی افزایش داشتند.

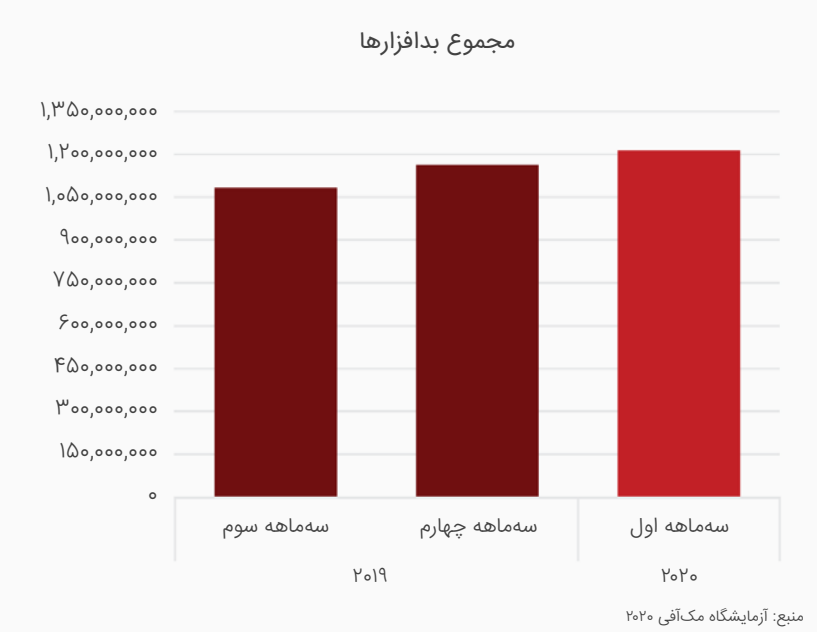
آمار تهدیدات بدافزاری

در سه‌ماهه اول ۲۰۲۰ شاهد افزایش قابل توجه در چندین دسته از این تهدیدات بودیم:

- در این دوره آزمایشگاه‌های مک‌آفی ۳۷۵ تهدید را در هر دقیقه شناسایی کردند.
- بدافزارهای جدید مبتنی بر PowerShell در سه‌ماهه اول ۲۰۲۰ در مقایسه با دوره قبل افزایشی ۶۸۹ درصدی داشتند. از جمله دلیل این افزایش قابل توجه ظهور خانواده بدافزاری Donoff بوده است. این اسب تروای دانلودکننده در افزایش ۴۱۲ درصدی بدافزارهای مبتنی بر ماکرو نیز نقش داشته است.
- مجموع بدافزارهای PowerShell در مقایسه با چهار دوره قبل ۱۹۰۲ درصد افزایش یافتند.
- بدافزارهای جدید دستگاه‌های همراه در سه‌ماهه اول ۲۰۲۰ نسبت به دوره قبل، عمدتاً به دلیل ظهور اسب‌های تروای جدید ۷۱ درصد افزایش داشتند.
- مجموع کل بدافزارهای دستگاه‌های همراه نزدیک به ۱۲ درصد افزایش را نسبت به چهار دوره قبل نشان می‌دهد.
- بدافزارهای جدید موسوم به اینترنت اشیاء ۵۸ درصد و بدافزارهای جدید MacOS ۵۱ درصد افزایش داشتند.
- نمونه‌های جدید از بدافزارهای موسوم به استخراج‌کننده ارز رمز[1] ۲۶ درصد بیشتر از دوره قبل بودند.
- بدافزارهای جدید مبتنی بر Linux ۸ درصد افزایش یافتند.

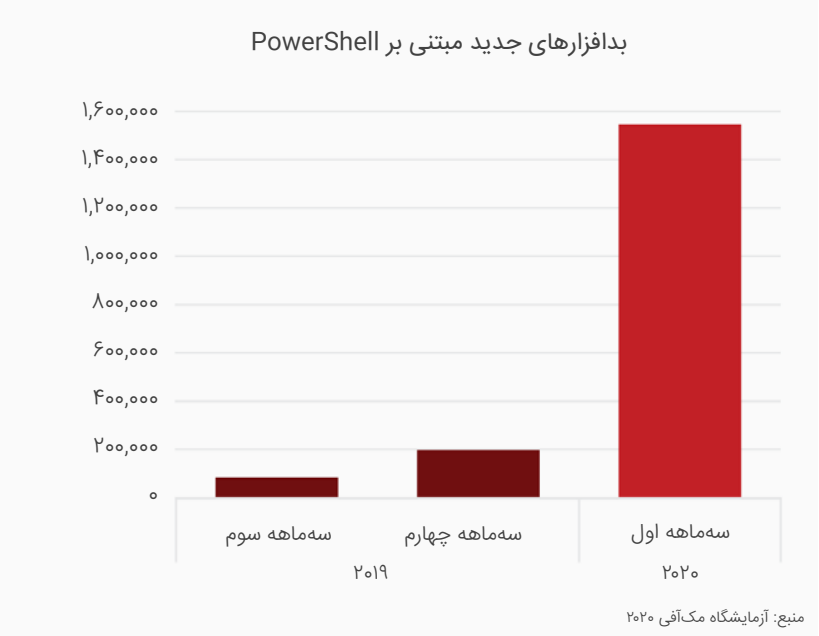
در عین حال در این دوره شاهد کاهش تهدیدات زیر بوده‌ایم:

- تعداد بدافزارهای جدید بهره‌جو[2] ۵۶ درصد کاهش را نشان می‌دهد.
- بدافزارهای جدید JavaScript کاهشی ۳۸ درصدی داشتند.
- تعداد کل بدافزارهای جدید ۳۵ درصد کاهش را نشان می‌دهد.
- باج‌افزارهای جدید کاهشی ۱۲ درصدی داشتند.
- کدهای موسوم به دودویی امضا شده[3] ۱۱ درصد کاهش داشتند.

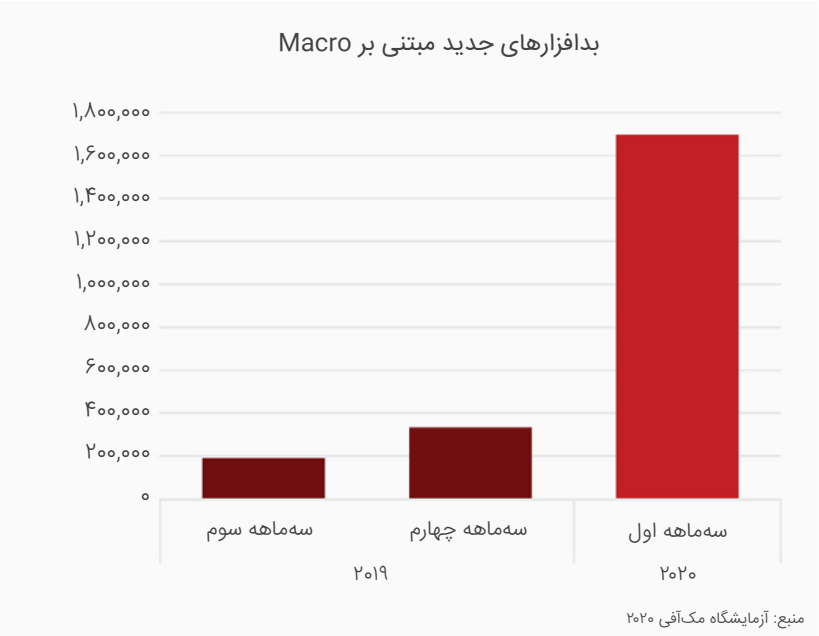


منبع: آزمایشگاه مک‌آفی ۲۰۲۰

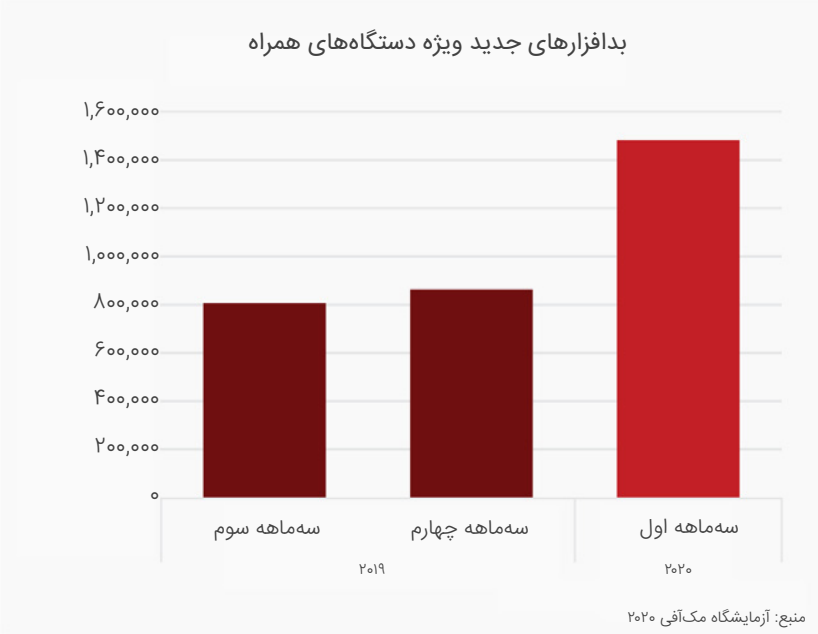
[1] Coin Miner
[2] Exploit
[3] Signed Binary



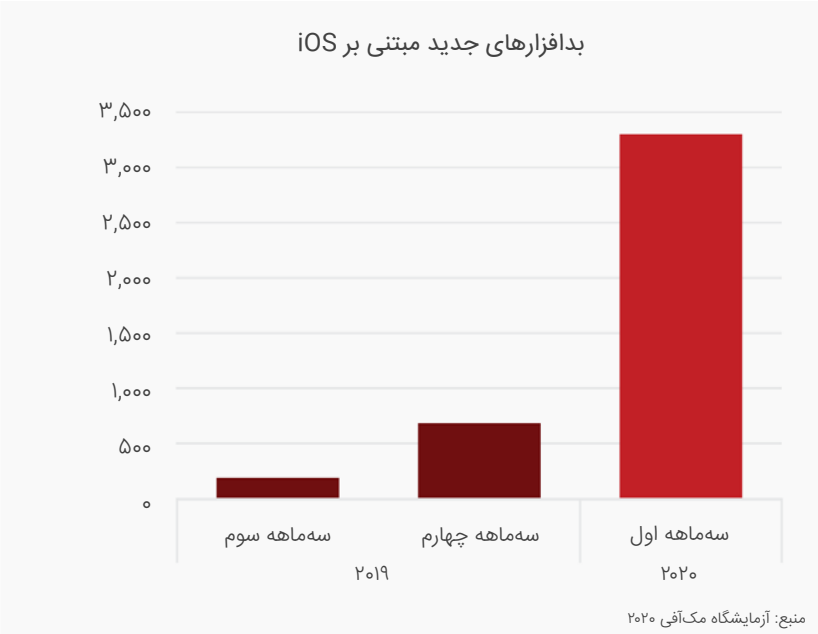
منبع: آزمایشگاه مک‌آفی ۲۰۲۰



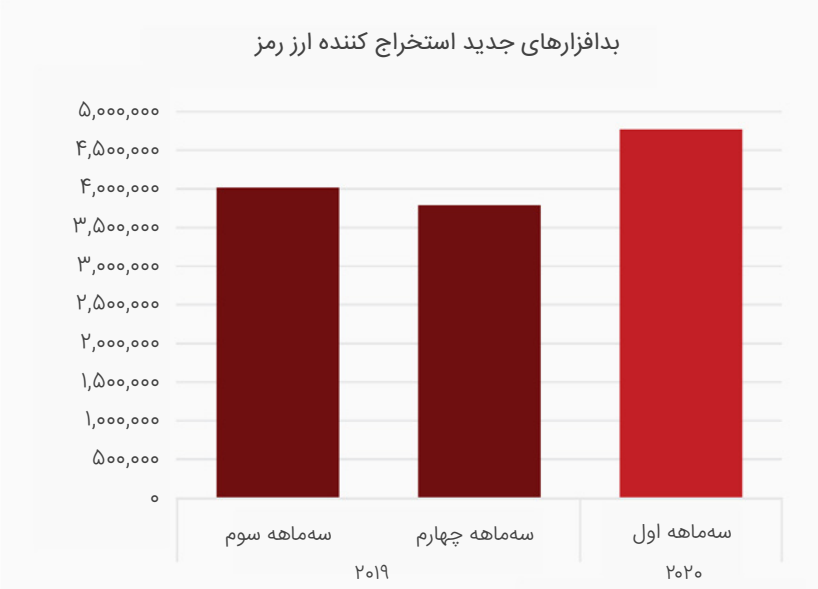
منبع: آزمایشگاه مک‌آفی ۲۰۲۰



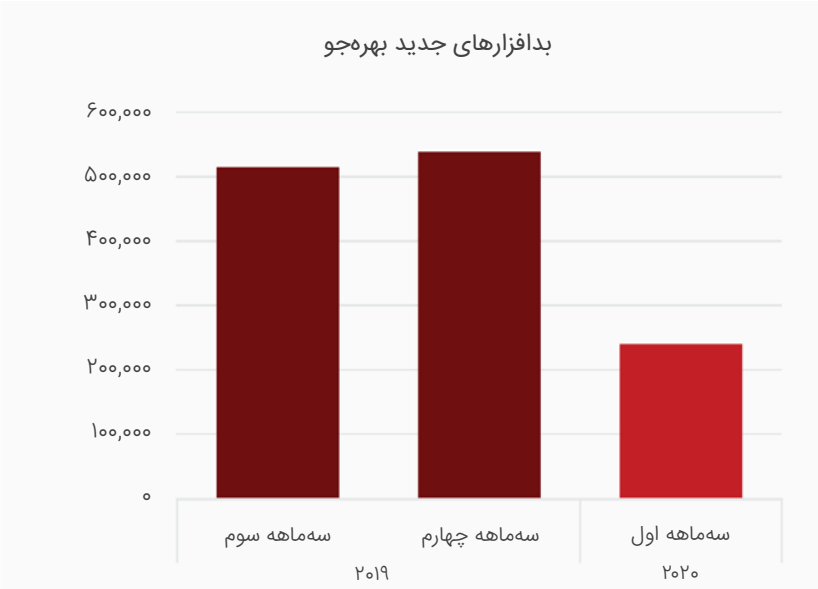
منبع: آزمایشگاه مک‌آفی ۲۰۲۰



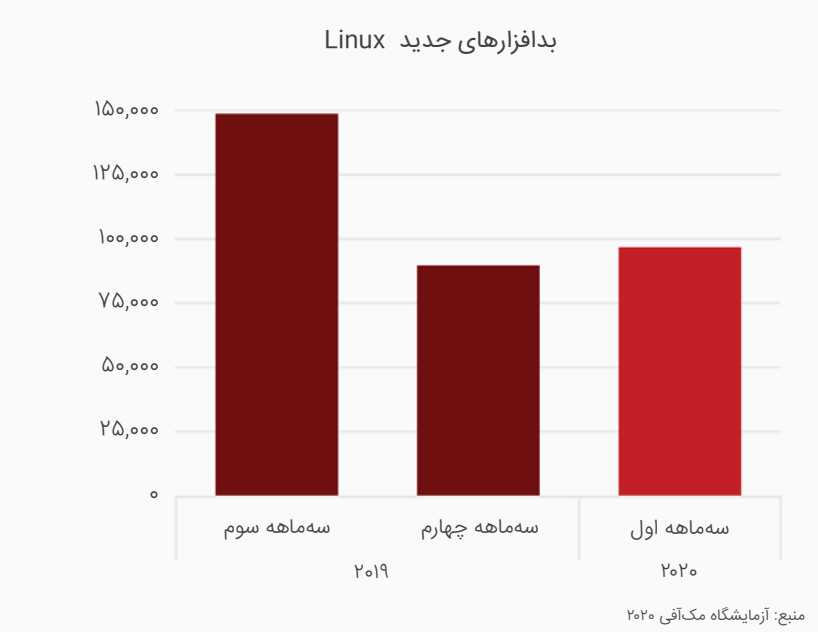
منبع: آزمایشگاه مک‌آفی ۲۰۲۰



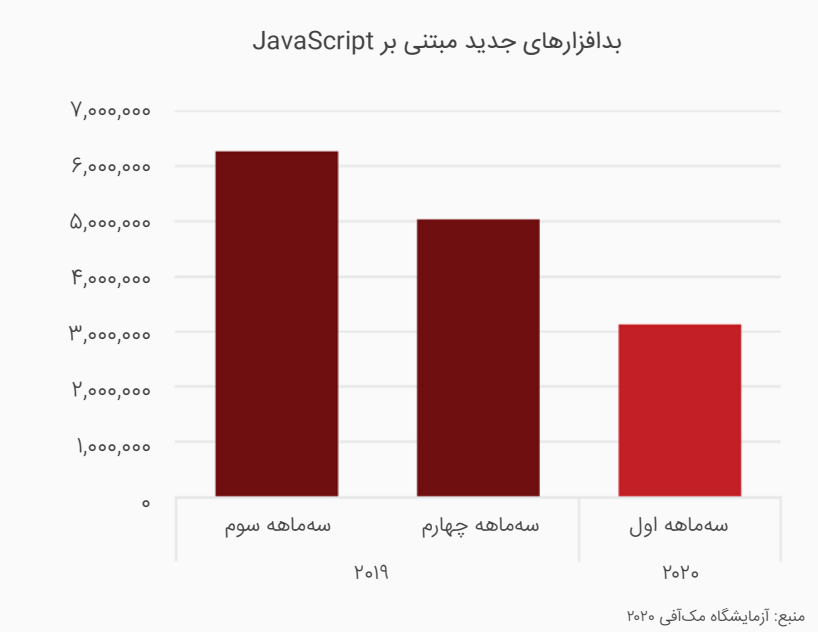
منبع: آزمایشگاه مک‌آفی ۲۰۲۰



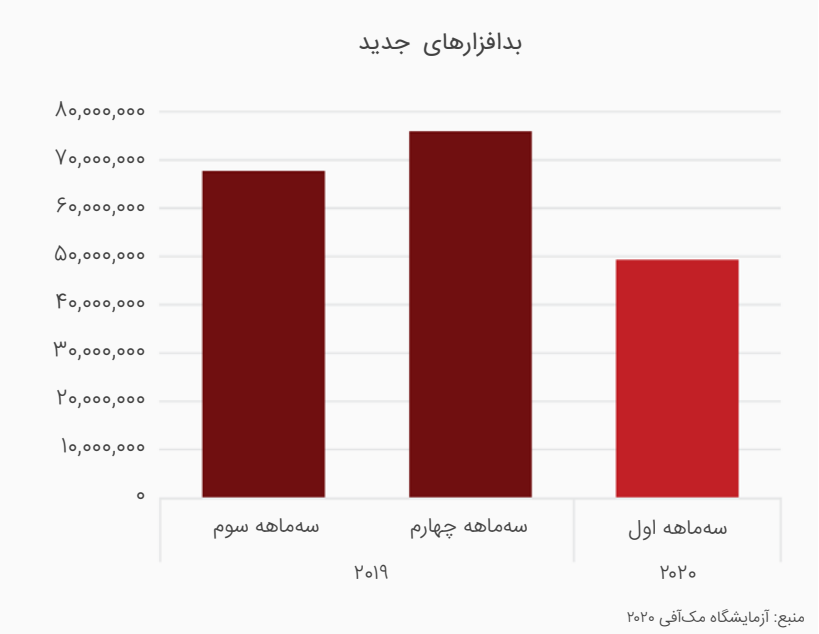
منبع: آزمایشگاه مک‌آفی ۲۰۲۰



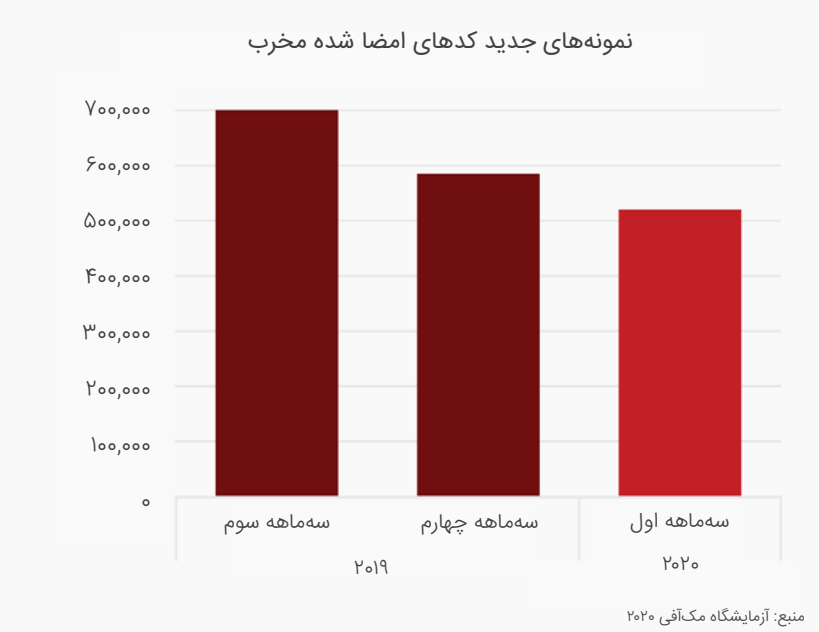
منبع: آزمایشگاه مک‌آفی ۲۰۲۰



منبع: آزمایشگاه مک‌آفی ۲۰۲۰



منبع: آزمایشگاه مک‌آفی ۲۰۲۰



منبع: آزمایشگاه مک‌آفی ۲۰۲۰

رایانش ابری، هدف مهاجمان

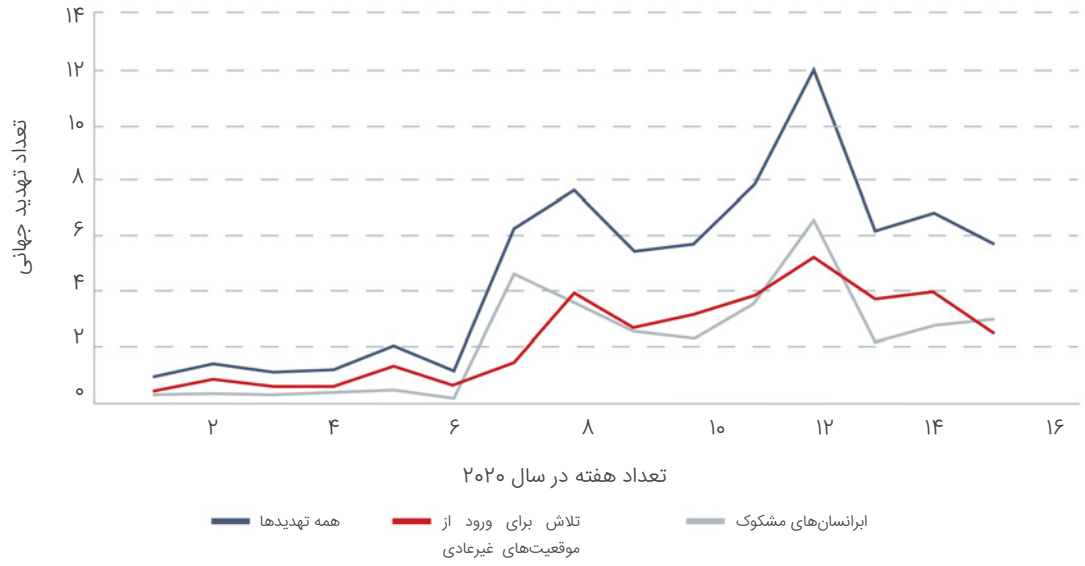
شرکت مایکروسافت برآورد کرده است که در نتیجه اعمال تغییرات ناگهانی و عظیم در سبک کار کارکنان به دلیل شیوع ویروس کووید-۱۹ میزان استفاده از سرویس‌های رایانش ابری در سطح جهانی افزایشی ۷۷۵ درصدی داشته است[۱]. همچنین بر اساس گزارش Cloud Adoption and Risk Report: Work From Home Edition[۲] که داده‌های آن در فاصله ژانویه و آوریل ۲۰۲۰ به‌صورت ناشناس از بیش از ۳۰ میلیون کاربر McAfee MVISION Cloud در سرتاسر جهان استخراج شده است تعداد کل تهدیدات از سوی مهاجمان خارجی که سرویس های رایانش ابری نظیر Microsoft 365 را هدف قرار می‌دهند ۶۳۰ درصد افزایش داشته است. مک‌آفی تهدیدات خارجی را به دو دسته تقسیم کرده که در هر دوی آنها سرقت اطلاعات اصالت‌سنجی دخیل بوده است:

تلاش برای ورود از موقعیت‌های غیرعادی - حمله با ورود از موقعیتی که تا پیش از آن شناخته نشده بود و از دید سازمان موقعیتی غیرعادی است آغاز می‌شود. مهاجم در ادامه تلاش می‌کند که بیش از حد معمول با سطح دسترسی فراتر از انتظار به داده‌ها دست پیدا کند.

ابرانسان‌های مشکوک - این تلاشی برای احراز هویت شدن از نقاط مختلف جهان است که سفر به آنها در فاصله زمانی میان هر یک از ثبت‌های ورود عملاً غیرممکن است. برای مثال پنج دقیقه پس از تلاش برای ورود به Microsoft 365 از سنگاپور با همان نام کاربری یک تلاش برای ورود در کالیفرنیای آمریکا ثبت می‌شود.

در این حملات کارکنان گرداننده حمله و سوءاستفاده‌کننده از موقعیت دورکار شدن نبوده‌اند. اکثر حملاتی که مک‌آفی شاهد آنها بوده تهدیدات متداول خارجی علیه بسترهای رایانش ابری هستند که به طور مستقیم حساب‌های کاربری ابری را هدف قرار داده‌اند.

درصد افزایش در تهدیدات مبتنی بر رایانش ابری: ژانویه تا آوریل ۲۰۲۰



منبع: آزمایشگاه مک‌آفی ۲۰۲۰

[۱] https://azure.microsoft.com/en-us/blog/update-2-on-microsoft-cloud-services-continuity

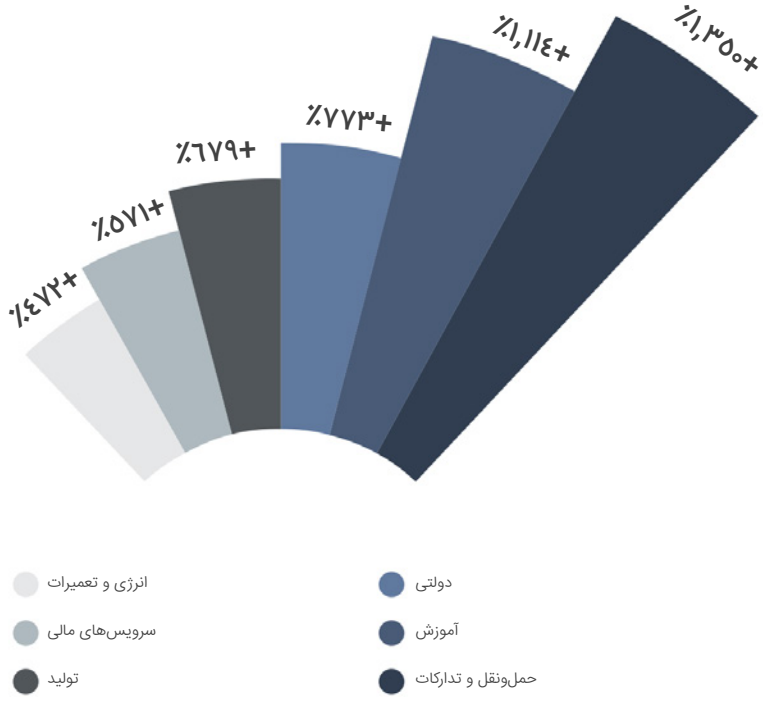
[۲] https://www.mcafee.com/enterprise/en-us/forms/gated-form.html?docID=3804edf6-fe75-427e-a4fd-4eee7d189265

تمرکز بر افزایش: تهدیدات مبتنی بر رایانش ابری

حمل‌ونقل و تدارکات، آموزش و سازمان‌های دولتی شاهد بیشترین افزایش را در آمار رخدادهای تهدیدات داخلی و خارجی در حساب‌های کاربری ابری خود بودند. وابستگی این حوزه‌ها به سرویس‌های رایانش ابری به‌صورت روزافزون در حال افزایش بوده و به تبع آن مهاجمان نیز تمرکز خاصی بر روی هک حساب کاربری آنها و در ادامه سرقت داده‌های قابل دسترس در این بسترها دارند.

درصد افزایش در تهدیدات مبتنی بر رایانش ابری

ژانویه تا آوریل ۲۰۲۰

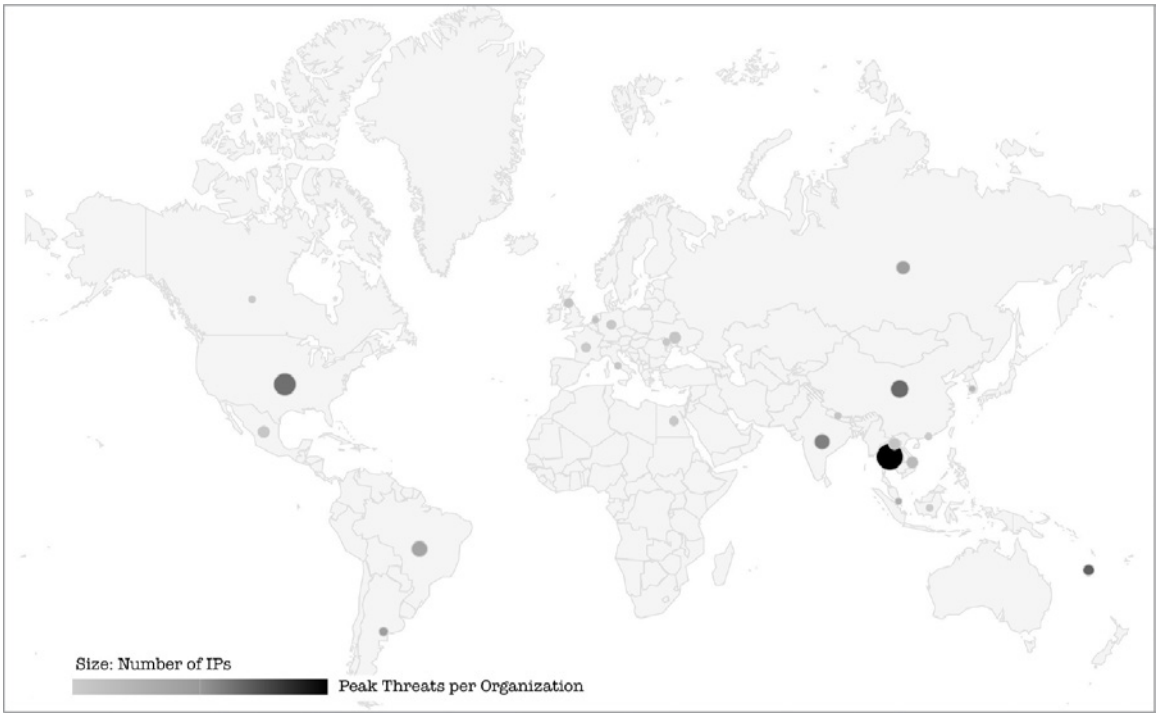


میزان افزایش رویدادهای مربوط به تهدیدات ابری به تفکیک هر صنعت

مک‌آفی با تحلیل نشانی‌های IP استفاده شده توسط مهاجمان خارجی در جریان حملات آنها اقدام به شناسایی موقعیت آنها کرده است. اگر چه نمی‌توان با قطعیت از نشانی IP برای انتساب حمله استفاده کرد اما در عین حال نمایی از داده های حمله ارائه می‌کند که از آنها برای پیاده‌سازی کنترل‌های امنیتی می‌توان بهره برد. نشانی‌های IP رصد شده نه فقط برای حمله به حساب‌های کاربری که در سایر فعالیت‌های مخرب در زیرساخت تبهکاران و اجرای حملات دیگر نیز مورد استفاده قرار گرفته بودند.

در نمودار اندازه دایره‌ها نمایانگر تعداد نشانی‌های IP استفاده شده و میزان تیرگی رنگ معرف تعداد رخدادهای شناسایی شده سازمان‌های مستقل است.

موقعیت جغرافیایی نشانی‌های IP که در فاصله بین ژانویه و فوریه ۲۰۲۰ مبداء اجرای حملات خارجی تهدیدات مبتنی بر رایانش ابری بوده است



نمای جهانی از مبادی حملات خارجی بر ضد حساب‌های کاربری رایانش ابری بر اساس نشانی IP

۱۰ کشور اول با بیشترین تعداد نشانی IP دخیل در اجرای حملات خارجی به حساب‌های کاربری ابری از ژانویه تا آوریل ۲۰۲۰ که بر اساس تعداد مرتب شده به‌شرح زیر است:

۱- تایلند
۲- آمریکا
۳- چین
۴- هند
۵- برزیل
۶- فدراسیون روسیه
۷- لائوس
۸- مکزیک
۹- کالدونیای جدید
۱۰- ویتنام

توجه! هیچ کدام از کشورهای مذکور در اروپا که درگیر برخی از سخت‌گیرانه‌ترین قواعد حفاظت از داده‌ها در جهان هستند قرار ندارند. اکثر آنها از کشورهایی هستند که به‌صورت تاریخی در جرایم سایبری نقش داشته‌اند و قوانین و نهادهای قانونی آنها در حوزه جرایم سایبری کم‌رنگ عمل می‌کنند.

فیشینگ و اسب‌های تروا

در زمانی که سازمان‌ها درگیر چالش‌های امنیتی جدید و نیروی کار در حال سازگار کردن خود با دورکاری ناشی از شیوع ویروس کووید-۱۹ بود مهاجمان فرصت‌طلب از این دغدغه‌ها برای پیش‌برد اهداف خود بهره بردند.

تبهکاران سایبری با ارسال ایمیل فیشینگ با عناوین و محتوای مرتبط با همه‌گیری کرونا، کارکنان و خانواده آنها را به عاملی برای رخنه به سیستم‌های آنها تبدیل کردند.

نمونه‌هایی از کارزارهایی که در جریان اجرای آنها ایمیل‌های حاوی اطلاعات دروغین در خصوص وام، آزمایشات کووید-۱۹ و درمان‌های موسوم به آنتی‌بادی بود مشاهده شدند.

بدافزار Ursnif

در ژانویه، مک‌آفی شاهد ظهور کارزار فیشینگی بود که گردانندگان آن اقدام به انتشار گونه‌ای از بدافزار Ursnif می‌کردند. Ursnif یک اسب تروای بانکی است که امکان سرقت اطلاعات اصالت‌سنجی بانکی را از طریق رصد فعالیت‌های کاربر، ضبط کلیدهای فشرده شده و ردیابی ترافیک شبکه و فعالیت مرورگر فراهم می‌کند.

با اجرای فایل VBS یک فایل DLL در مسیر C:\Programdata\FxrPLxT.dll ایجاد شده و در ادامه از طریق پروسه معتبر rundll32.exe فراخوانی می‌شود. DLL پس از تزریق شدن به iexplorer.exe اقدام به برقراری ارتباط با سرور فرماندهی[1] خود با استفاده از درخواست‌های HTTP GET می‌کند.

نشانه‌های آلودگی:

نوع	نشانه آلودگی	توضیحات
Sha256	e82d49c11057f5c222a440f05daf9a53e860455d-c01b141e072de525c2c74fb3	Filename: Coronavirus_disease_COVID-19__194778526200471.vbs
Sha256	8bcdf1fbc8cee1058ccb5510df49b268dbfce541cfc-4c83e135b41e7dd150e8d	Ursnif dll

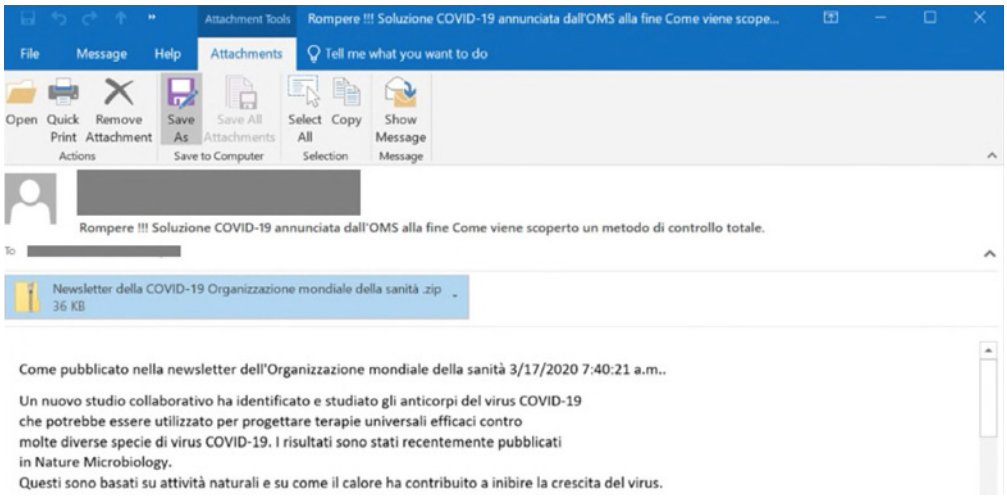
ماتریس MITRE ATT&CK:

شناسه تکنیک	تاکتیک	جزییات تکنیک
T1059	اجرا	رابط کاربری خط فرمان
T1129	اجرا	اجرا از طریق فراخوانی ماژول
T1085	عبور از سد سازوکار دفاعی، اجرا	Rundll32
T1060	ماندگاری	کلیدهای Run در محضرخانه (Registry) / پوشه Startup
T1055	عبور از سد سازوکار دفاعی، ترفیع سطح دسترسی	تزریق پروسه

[1] C&C

اسب تروای Fareit

از ابتدای فوریه، مک‌آفی کارزار دیگری را رصد کرد که در آن با استفاده از ایمیل‌های فیشینگ با عناوین فریبنده‌ای همچون COVID-19 و Coronavirus کاربر ناآگاه متقاعد به کلیک بر روی لینک‌ها یا باز کردن پیوست‌هایی می‌شد که در نهایت منجر به دریافت و اجرای یک اسب تروای سارق اطلاعات با عنوان Fareit می‌گردید.



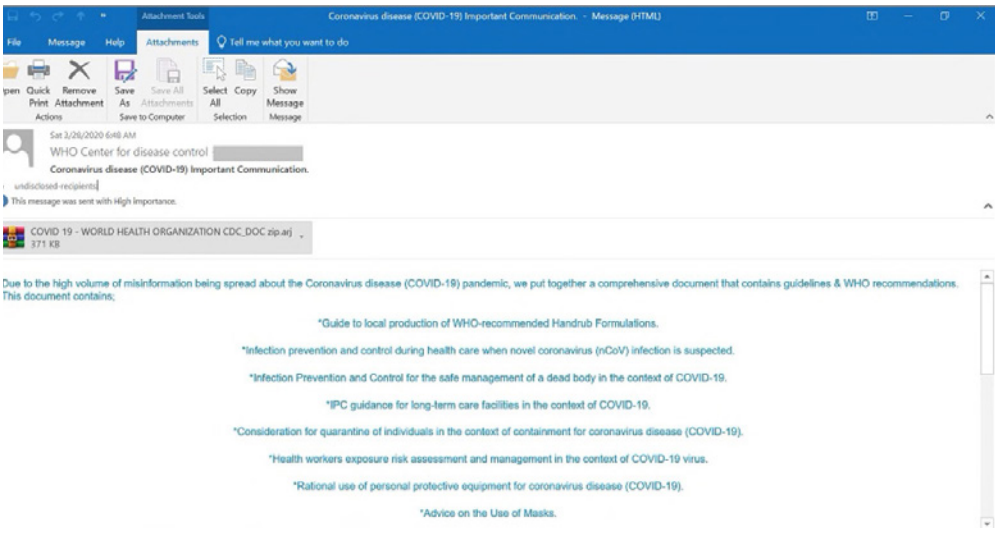
نشانه‌های آلودگی:

نوع	نشانه آلودگی	توضیحات
Sha256	2faf0ef9901b80a05ed77fc20b55e89dc0e1a23ae86d-c19966881a00704e5846	پیوست
Sha256	38a511b9224705bfea131c1f77b3bb233478e2a1d9bd3bf99a7933dbe11d-be3c	ایمیل

ماتریس MITRE ATT&CK:

شناسه تکنیک	تاکتیک	جزییات تکنیک
T1193	اجرا	پیوست فیشینگ هدفمند
T1106	اجرا	اجرا از طریق API
T1130	عبور از سد سازوکار دفاعی، اجرا	نصب گواهینامه موسوم به Root Certificate
T1081	ماندگاری	اصالت‌سنجی‌های درون فایل
T1012	عبور از سد سازوکار دفاعی، ترفیع سطح دسترسی	پرس‌وجو از محضرخانه
T1071	سرور فرماندهی	استفاده از پودمان استاندارد Application Layer Protocol

نمونه ای دیگر از هرزنامه Fareit



نشانه‌های آلودگی:

نوع	نشانه آلودگی	توضیحات
Sha256	2faf0ef9901b80a05ed77fc20b55e89dc0e1a23ae86d-c19966881a00704e5846	دودویی دانلود شده
Sha256	38a511b9224705bfea131c1f77b3bb233478e2a1d9bd3bf99a7933dbe11d-be3c	پیوست
Sha256	ada05f3f0a00dd2acac91e24eb46a1e719fb08838145d9ae7209b5b7b-ba52c67	ایمیل

ماتریس MITRE ATT&CK:

شناسه تکنیک	تاکتیک	جزییات تکنیک
T1193	دسترسی اولیه	پیوست فیشینگ هدفمند
T1204	اجرا	اجرا توسط کاربر
T1071	سرور فرماندهی	استفاده از پودمان استاندارد Application Layer Protocol

اسب تروای Emotet

در اواخر ماه مارس مک‌آفی کارزار فیشینگی را شناسایی کرد که در آن مهاجمان با سوءاستفاده از موضوعات مرتبط با کووید-۱۹ دستگاه قربانیان را آلوده به گونه‌ای از اسب تروای Emotet می‌کردند. در یکی از نمونه ایمیل‌های ارسالی تظاهر می‌شد که حاوی اطلاعاتی در مورد تحقیقات در خصوص آنتی‌بادی کرونا و درمان‌های جدید برای کووید-۱۹ است. اگر چه به محض آلودگی، Emotet قادر به انجام اقدامات مختلفی بر روی سیستم است اما همیشه اینطور برنامه‌نویسی شده بود که ایمیل‌هایی انبوه به زبان اسپانیایی را به سایر کاربران ارسال کند. نمونه‌ای از این ایمیل ها که توسط مک‌آفی به انگلیسی برگردان شده در تصویر زیر قابل مشاهده است:

Subject:

Break !!! COVID-19 solution announced by WHO at the end How a total control method is discovered

Email Body:

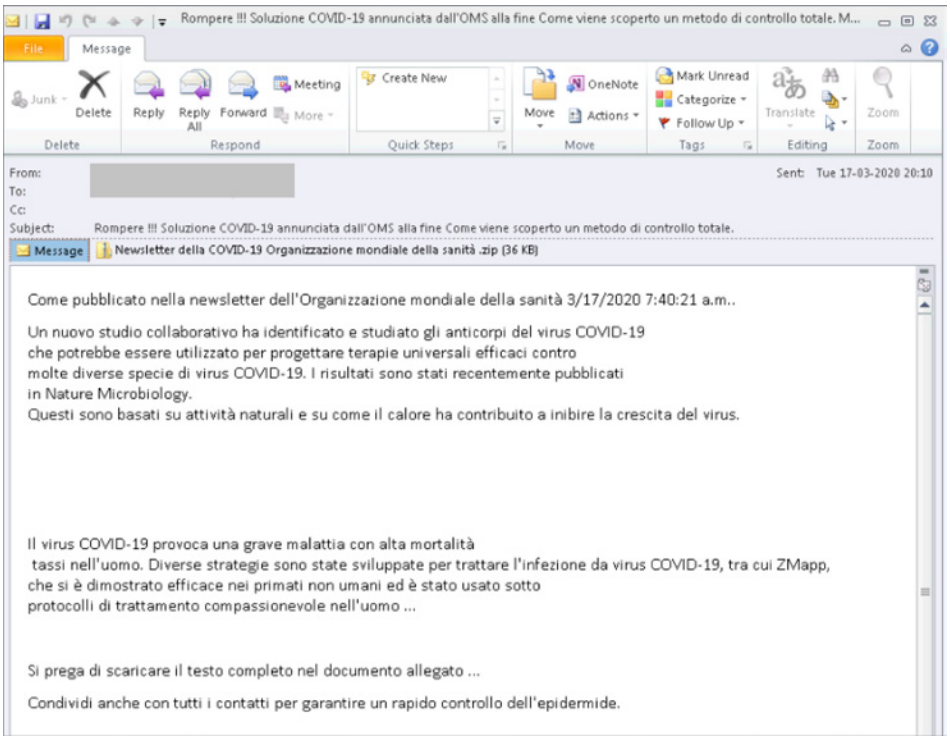
As published in the newsletter of the World Health Organization 3/17/2020 7:40:21 a.m. A new collaborative study identified and studied antibodies to the COVID-19 virus which could be used to design effective universal therapies against many different species of COVID-19 viruses. The results have recently been published in Nature Microbiology.

These are based on natural activities and how heat helped inhibit the virus from growing.

The COVID-19 virus causes a serious disease with high mortality badgers in humans. Several strategies have been developed to treat COVID-19 virus infection, including ZMapp, which has proven effective in non-human primates and has been used below compassionate treatment protocols in humans ...

Please download the full text in the attached document ...

Also share with all contacts to ensure quick epidermal control.



پیوست ایمیل فایلی ZIP حاوی فایل اجرایی Emotet است که پس از اجرا، خود را با بهره‌گیری از تکنیک موسوم به Hollowing به پروسه‌ای با عنوان regasm.exe تزریق می‌کند. در ادامه نیز با سرور فرماندهی ارتباط برقرار کرده و به ابزاری برای ارسال هرزنامه‌های مورد نظر مهاجمان تبدیل می‌شود.

نشانه‌های آلودگی:

نوع	نشانه آلودگی	توضیحات
Sha256	ca70837758e2d70a91fae20396dfd80f93597d4e606758a02642a-c784324eee6	پیوست
Sha256	702feb680c17b00111c037191f51b9dad1b55db006d9337e-883ca48a839e8775	ایمیل

ماتریس MITRE ATT&CK:

شناسه تکنیک	تاکتیک	جزییات تکنیک
T1121	عبور از سد سازوکار دفاعی، اجرا	Regsvcs/Regasm
T1093	عبور از سد سازوکار دفاعی	Process Hollowing

بدافزار Azorult

Azorult بدافزار جدیدی است که در بیشتر مواقع برای سرقت نام‌های کاربری، رمزهای عبور، استخراج‌کنندگان ارز رمز، سوابق سایت‌های مرور شده و کوکی‌ها مورد استفاده مهاجمان قرار می‌گیرد. این اطلاعات در بازارهای زیرزمینی تبهکاران به گردانندگان باج‌افزار فروخته شده و آنها نیز از آن به‌منظور رخنه به اهداف خود بهره می‌گیرند. گروه برنامه‌های پیشرفته مک‌آفی نمونه‌هایی را مشاهده کرده که آلودگی به Azorult منجر به انتشار گسترده باج‌افزار در عرض چند ساعت یا نهایت چند روز شده است. جالب آن‌که سازندگان Azorult اقدام به راه‌اندازی سایتی به نشانی corona-virus-map[.]com کرده‌اند که در آن اطلاعاتی جعلی در خصوص میزان شیوع ویروس کرونا در نقاط مختلف جهان ارائه می‌شود.

نشانه‌های آلودگی:

نوع	نشانه آلودگی	توضیحات
SHA256	c40a712cf1eec59efac42daada5d79c7c3a1e8ed5fbb9315bfb26b-58c79bb7a2	از دامنه Jar دریافت فایل
URL	H**p://corona-virus-map.net/map.jar	
Sha256	63fcf6b19ac3a6a232075f65b4b58d69cfd4e7f396f573d-4da46aaf210f82564	فایل دودویی دریافت‌شده

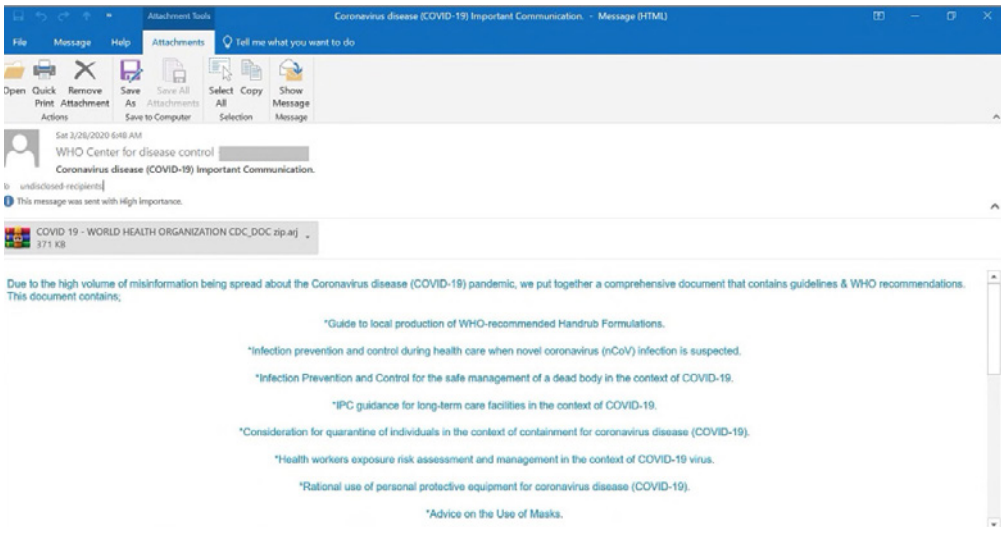
ماتریس MITRE ATT&CK:

شناسه تکنیک	تاکتیک	جزییات تکنیک
T1059	اجرا	رابط خط-فرمان
T1012	کشف	پرس‌وجو در محضرخانه

ابزار دسترسی از راه دور NanoCore

NanoCore یک اسب تروای دسترسی از راه دور[1] مجهز به افزونه‌های به‌شدت سفارشی‌سازی شده است که قابلیت‌های مختلفی را در اختیار مهاجمان قرار می‌دهد. نمونه‌هایی از این RAT در قالب ایمیل‌هایی با عناوینی مرتبط با موضوع شیوع کرونا نظیر Covid-19 Urgent Precaution Measures منتشر شدند.

[1] Remote Access Trojan - به اختصار RAT



نشانه‌های آلودگی:

نوع	نشانه آلودگی	توضیحات
SHA256	ca93f60e6d39a91381b26c1dd4d81b7e352aa3712a965a15f0d5edd-b565a4730	فایل دودویی دریافت‌شده
SHA256	89b2324756b04df27036c59d7aaaeef384c5bfc98ec-7141ce01a1309129cdf9f	پیوست Iso
Sha256	4b523168b86eafe41acf65834c1287677e15fd04f77fea3d-0b662183ecee8fd0	ایمیل

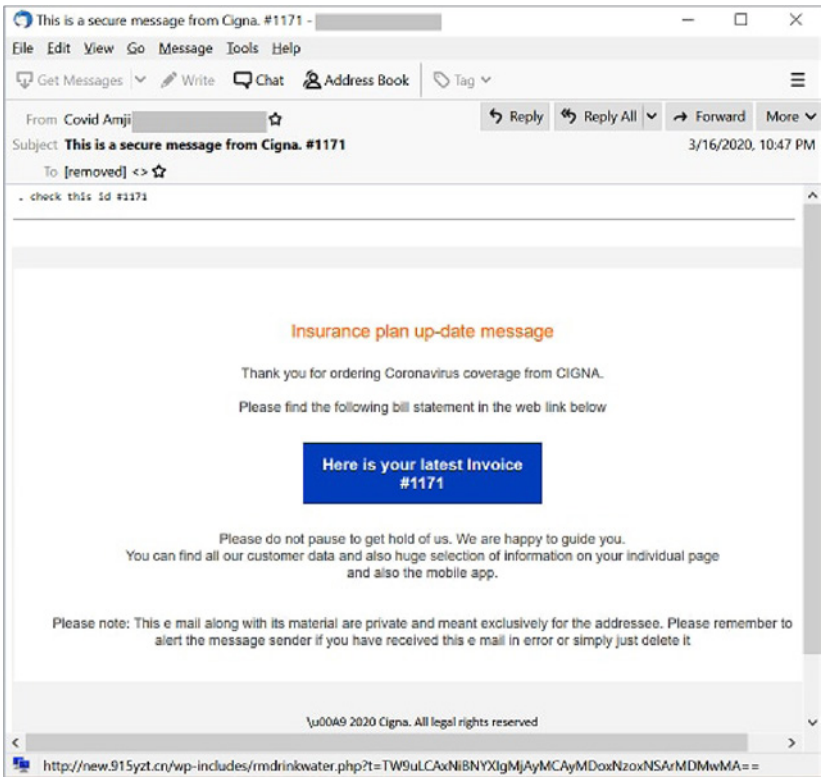
ماتریس MITRE ATT&CK:

شناسه تکنیک	تاکتیک	جزییات تکنیک
T1193	دسترسی اولیه	پیوست فیشینگ هدفمند
T1053	اجرا	فرامین زمان‌بندی‌شده در Scheduled Task
T1060	ماندگاری	کلیدهای Run در محضرخانه (Registry) / پوشه Startup
T1143	عبور از سد سازوکار دفاعی	پنجره مخفی
T1036	عبور از سد سازوکار دفاعی	جعل
T1497	عبور از سد سازوکار دفاعی	مجازی‌سازی / عبور از سد قرنطینه امن
T1012	کشف	پرس‌وجو در محضرخانه
T1124	کشف	کشف زمان سیستم
T1065	سرور فرماندهی	درگاه‌های غیرمتداول

اسب تروای Hancitor

اسب تروای Hancitor از طریق هرزنامه‌هایی با الگوی کووید-۱۹ که در ظاهر از سوی یک شرکت بیمه‌ای ارسال شده بودند منتشر شد. ایمیل حاوی لینکی است که با کلیک بر روی آن یک صورتحساب جعلی که وظیفه آن دریافت اسکریپت مخرب VBS است اجرا می‌شود.

با اجرای VBS فایل DLL مخرب Hancitor تحت نام temp_adobe_123452643.txt در مسیر %AppData%Local/Temp ایجاد می‌شود. در ادامه فایل DLL با استفاده از Regsvr32.exe اجرا شده و با سرور فرماندهی ارتباط برقرار می‌کند.



نشانه‌های آلودگی:

نوع	نشانه آلودگی	توضیحات
SHA256	2f87dd075fc12c2b6b15a1eb5ca209ba056bb6aa-2feaf3518163192a17a7a3	فایل دودویی دریافت‌شده
SHA256	0caef2718bc7130314b7f08559beba53ccf00e5ee5aba49523fb83e-1d6a2a347	فایل دودویی دریافت‌شده
Sha256	375d196227d62a95f82cf9c20657449ebea1b512d4cb19cd-fe9eb8f102dd9fa	فایل دودویی دریافت‌شده
Sha256	0b8800734669aa7dbc6e67f93e268d827b5e67d4f30e33734169d-dc93a026	فایل دودویی دریافت‌شده
Sha256	9c40426f157a4b684047a428428f882618d07dc5154cf1bf-89da5875a00d69c	ایمیل

ماتریس MITRE ATT&CK:

شناسه تکنیک	تاکتیک	جزییات تکنیک
T1192	دسترسی اولیه	لینک فیشینگ هدفمند
T1064	اجرا	اسکریپت‌نویسی
T1117	اجرا	Regsvr32
T1071	سرور فرماندهی	استفاده از پودمان استاندارد Application Layer Protocol

باج‌افزارها

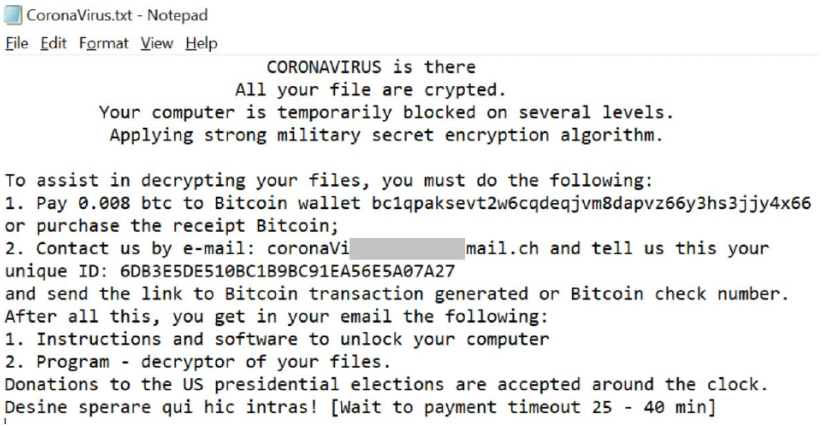
در سال ۲۰۱۹ کارزارهای باج‌افزاری سرخط بسیاری از اخبار در بخش‌های مختلف بودند. گردانندگان خدمات معروف به "باج‌افزار به‌عنوان سرویس"[۱] تمرکز ویژه‌ای بر روی هدف قرار دادن شهرداری‌ها و سازمان‌های فعال در حوزه هایی همچون بهداشت و درمان و امور مالی داشتند. گروه برنامه‌های پیشرفته مک‌آفی کارزارهای باج‌افزاری متعددی را از جمله Sodinokibi - که با نام REvil نیز شناخته می‌شود[۲] - که با بهره‌گیری از دغدغه کووید-۱۹ سرتاسر جهان را هدف قرار دادند تحلیل کردند.

حتی تا قبل از چالش دورکاری کارکنان نیز مهندسان امنیت، بخش‌های فناوری اطلاعات و تحلیلگران درگیر یافتن راهکارهای مؤثر برای مقابله با تهدیدات مخرب باج‌افزاری بودند. اما چطور می‌توان اطمینان یافت که حفاظت در برابر بدافزارها در خارج از شبکه نیز همچون داخل شبکه مدیریت شده است؟

همانطور که کارکنان دور کار و مهندسان فناوری اطلاعات به طور روزافزون از پودمان RDP جهت دسترسی اولیه به شبکه سازمان استفاده می‌کنند مهاجمان ضعف‌های بیشتری برای بهره‌جویی از آنها کشف می‌کنند. این آسیب‌پذیری‌ها شامل سوءاستفاده از مکانیزم‌های اصالت‌سنجی یا کنترل‌های امنیتی یا حتی خرید رمزهای عبور هک شده RDP ر بازارهای زیرزمینی است. بهره‌جویی از این آسیب‌پذیری‌ها مهاجم را قادر می‌کند تا با سطح دسترسی Admin به سادگی باج‌افزار یا سایر بدافزارها را نصب کرده و سپس به شبکه سازمان راه پیدا کند.

باج‌افزار GVZ

باج‌افزار GVZ در کارزارهای با الگوی کرونا در ماه مارس پدیدار شد. این باج‌افزار در اطلاعیه باج‌گیری[۳] خود در ازای آن‌چه که بازگرداندن اطلاعات به حالت اولیه می‌خواند مبلغی را اخاذی می‌کند. به‌محض اجرا، GVZ از طریق پروسه معتبر vssadmin اقدام به حذف نسخه‌های موسوم به Shadow Copy کرده و سپس تمامی انواع فایل‌های غیراجرایی را رمزگذاری می‌کند. با تکمیل رمزگذاری فایل‌های درون پوشه اطلاعیه باج‌گیری که نمونه‌ای از آن در زیر قابل مشاهده است در آن کپی می‌شود.


CoronaVirus.txt - Notepad

File Edit Format View Help

CORONAVIRUS is there
All your file are crypted.
Your computer is temporarily blocked on several levels.
Applying strong military secret encryption algorithm.

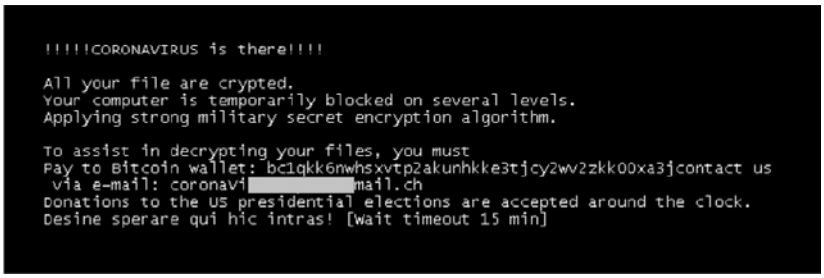
To assist in decrypting your files, you must do the following:
1. Pay 0.008 btc to Bitcoin wallet bc1qpaksevt2w6cqdeqjvm8dapvz66y3hs3jjy4x66
or purchase the receipt Bitcoin;
2. Contact us by e-mail: coronaVi[redacted]mail.ch and tell us this your
unique ID: 6DB3E5DE510BC1B9BC91EA56E5A07A27
and send the link to Bitcoin transaction generated or Bitcoin check number.
After all this, you get in your email the following:
1. Instructions and software to unlock your computer
2. Program - decryptor of your files.
Donations to the US presidential elections are accepted around the clock.
Desine sperare qui hic intras! [Wait to payment timeout 25 - 40 min]

[۱] Ransomware-as-a-Service

[۲] https://www.mcafee.com/blogs/other-blogs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/

[۳] Ransom Note

GVZ همچنین با ایجاد یک صفحه موسوم به Lock Screen در هنگام راه‌اندازی شدن سیستم پیامی مشابه با شکل زیر را نمایش می‌دهد.



نشانه‌های آلودگی:

نوع	نشانه آلودگی	توضیحات
SHA256	3299f07bc0711b3587fe8a1c6bf3ee6bcbc14cb775f64b28a61d72eb-cb8968d3	فایل دودویی

ماتریس MITRE ATT&CK:

شناسه تکنیک	تاکتیک	جزییات تکنیک
T1486	تأثیر	رمزگذاری داده‌ها
T1083	کشف	کشف فایل و پوشه
T1490	تأثیر	غیرفعال کردن امکان بازگردانی سیستم به حالت اولیه

هرزنامه‌ها و کلاهبرداری‌ها

تهدیدات موبایلی

تنها در مارس ۲۰۲۰ آزمایشگاه‌های مک‌آفی چندین برنامه مخرب Android را که در آنها با بهره‌گیری از بحران شیوع ویروس کووید-۱۹ و استفاده از کلیدواژه‌های مرتبط دستگاه همراه کاربران را هدف قرار می‌دادند شناسایی کردند. این برنامه‌های مخرب عملکردهای متفاوتی نظیر باج‌افزار یا جاسوس‌افزار داشتند. برای مثال می‌توان به برنامه Corona Safety Mask اشاره کرد که مجوزهای مشکوک زیر را از قربانی اخذ می‌کند:

- دسترسی کامل به اینترنت به‌نحوی که برنامه را قادر به ایجاد سوکت‌های شبکه ای می‌کند
- دسترسی به اطلاعات فهرست تماس‌ها از روی دستگاه قربانی
- ارسال پیامک

زمانی که کاربر برنامه را دریافت می‌کند برای خرید ماسک به سایت جعلی coronasafetymask[.]tk هدایت شده و در آنجا قربانی ناآگاه اقدام به ثبت سفارش می‌کند. نویسندگان این برنامه‌ها از دسترسی ارسال پیامک برای کلاهبرداری از افرادی که شماره آنها در فهرست تماس‌های دستگاه قربانی است بهره می‌گیرند.

مک‌آفی تمرکز ویژه‌ای نیز بر شناسایی گردانندگان موسوم به تهدیدات پیشرفته و مستمر[۱] که الگوی کووید-۱۹ را در کارزارهایشان لحاظ کرده‌اند داشته است. برای مثال، توزیع اسنادی که در ظاهر محتوای آنها در مورد همه‌گیری کرونا است اما در عمل حاوی ماکروی مخرب برای دریافت بدافزار و اجرا بر روی سیستم قربانی هستند.

ایمیل‌های وام دروغین

از اواخر ماه مارس یک کارزار فیشینگ از ایمیل هایی بهره برد که در آنها ادعا می‌شد که از سوی اداره کسب‌وکارهای کوچک ایالات متحده[۲] ارسال شده‌اند. فرستندگان این‌طور القا می کردند که ایمیل حاوی اطلاعات و راهنمایی‌های لازم برای دریافت وام از این اداره است. اما در حقیقت سازوکاری برای آلوده‌سازی سیستم دارندگان کسب‌وکارهای کوچک با ابزار دسترسی از راه دور Remcos بودند.

کلاهبرداری آزمایش کووید-۱۹

در مارس تبهکاران سایبری با توزیع ایمیل‌های فیشینگی که در ظاهر از سوی سازمان‌های مسئول انجام آزمایش‌های کووید-۱۹ ارسال شده بودند کاربران را تشویق به باز کردن سند پیوست می‌کردند که در نتیجه آن دستگاه به بدافزار سارق اطلاعات Trickbot آلوده می‌شد.

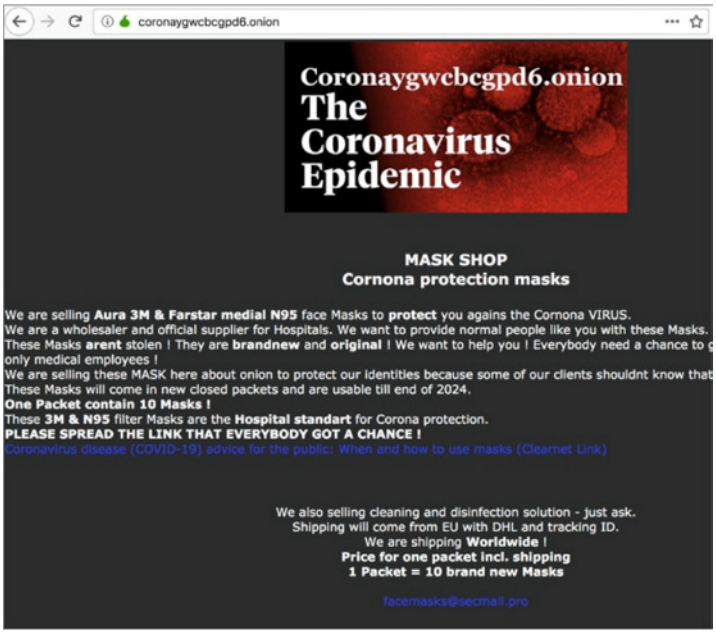
[۱] Advanced Persistent Threat
[۲] Small Business Administration

کلاهبرداری در خصوص اقدامات پیشگیرانه کووید-۱۹

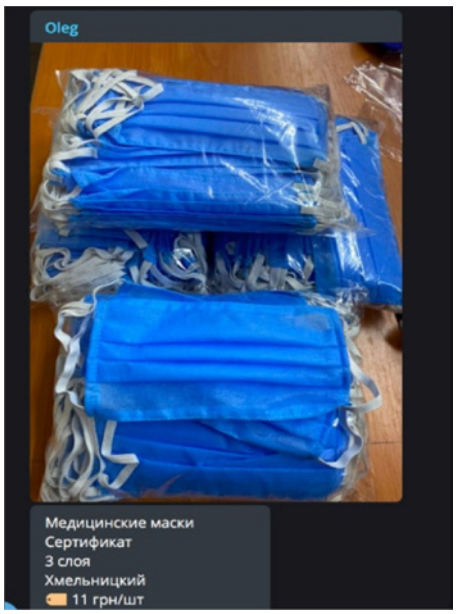
در ماه آوریل شاهد ظهور کارزارهای ایمیل فیشینگ با عنوان COVID-19 Urgent Precaution Measures بودیم که اقدام به توزیع ابزار دسترسی از راه دور NanoCore به منظور استخراج اطلاعات بااهمیت می‌کرد.

بازارهای زیرزمینی

ما همواره شاهد نمونه‌های متعددی از سوءاستفاده افرادی با گرایش‌های فقط مالی از رخدادهای مهم بوده‌ایم و بحران کرونا نیز از چشم این افراد دور نمانده است. تصاویر زیر نمونه‌هایی از فروش ماسک در بازارها و کانال‌های زیر زمینی نمایش می‌دهند.



فروش ماسک در سایتی در شبکه ناشناس TOR



کانال تلگرامی با چندین فروشنده ماسک

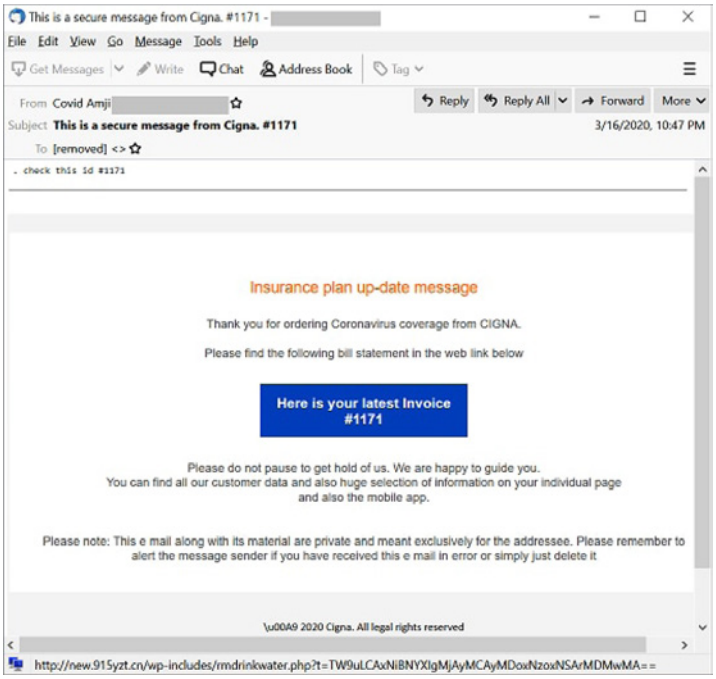
نقشه جعلی آلودگی "جانز هاپکینز"

در ماه آوریل، تبهکاران سایبری با استفاده از ایمیل‌های فیشینگ کاربران را به سایتی هدایت می کردند که در آن به دروغ ادعا می‌شد که آمار نمایش داده شده در آن بر اساس اطلاعات مرکز Johns Hopkins Center for Health Security استخراج شده است. از همان ایمیل‌ها جهت برای آلوده‌سازی سیستم کاربران کنجکاو به بدافزار سارق اطلاعات Azorult استفاده شده بود.

نقشه آلودگی جانز هاپکینز

صورتحساب‌های جعلی بیمه

در اواسط ماه آوریل تبهکاران سایبری با استفاده از ایمیل‌های با الگوی کووید-۱۹ با پیوست صورتحساب‌های جعلی بیمه اقدام به آلوده کردن سیستم‌های کاربران به بدافزار Hancitor کردند.

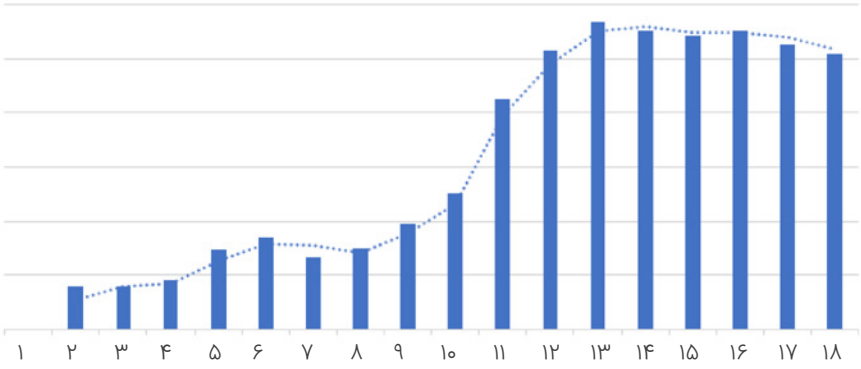


صورتحساب جعلی بیمه

کلاهبرداری از طریق نشانی‌های URL

مک آفی هزاران ایمیل هرزنامه با الگوی کووید-۱۹ و سایت‌های دروغینی که در ظاهر فروشنده کیت‌های آزمایش بیماری، ماسک و سایر وسایل حفاظتی هستند را شناسایی کرده است. طی ۱۳ هفته از شروع همه‌گیری کرونا، سایت‌های جعلی و نشانی‌های URL مخرب از ۱۶۰۰ مورد به ۳۹ هزار مورد افزایش پیدا کرد. آماری که اهمیت دقت و حساسیت در زمان کلیک بر روی لینک‌ها و مراجعه به سایت‌ها را پررنگ می‌کند.

تعداد نشانی‌های URL مخرب مرتبط با کووید-۱۹ به تفکیک هفته‌های سال ۲۰۲۰



در اینجا نمونه‌هایی از سایت‌های مخرب نشان داده شده است. تبلیغ نادرست[1] روشی مشترک میان کلاهبرداران سایبری در این دوران همه‌گیری است. تصویر زیر نمونه‌ای از سایت‌های کلاهبرداری را نمایش می‌دهد که در آن به دروغ آزمایش کرونا به کاربران پیشنهاد می‌شود.

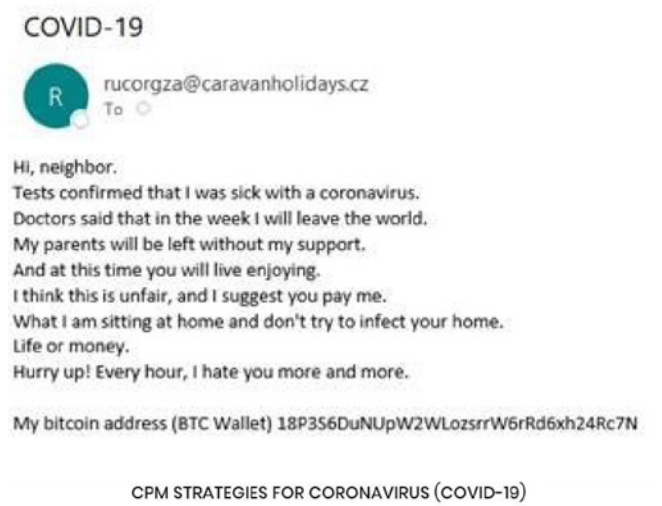
[1] False advertising

با توجه به تقاضای بالا برای ماسک و کمبود آن در مقاطعی حتی برای جامعه بهداشت و درمان ارسال‌کنندگان هرزنامه نیز از این موضوع بهره‌جویی کردند. نمونه‌ای از ایمیل‌ها و سایت‌هایی که در آنها کاربر برای خرید ماسک به فروشگاه‌های آنلاین جعلی هدایت می‌شود در زیر قابل مشاهده است.

Subject: Re: Disposable Surgical Mask Sale
From: sales <sales@xprotecting.com>
Date: Tue, 24 Mar 2020 19:02:43 +0800 (CST)
To: highway
Content-Type: text/html
Attachments No attachments
Message Structure: text/html

Hello,
Medical Surgical Mask Supplier in China. COVID-19 almost gone in our country. We start to support other country now. If you need purchase face musk, please contact with us.

Have a nice day!
Mike
Tel: +86 755 88860096
WhatsApp: +86 137 2876 8866

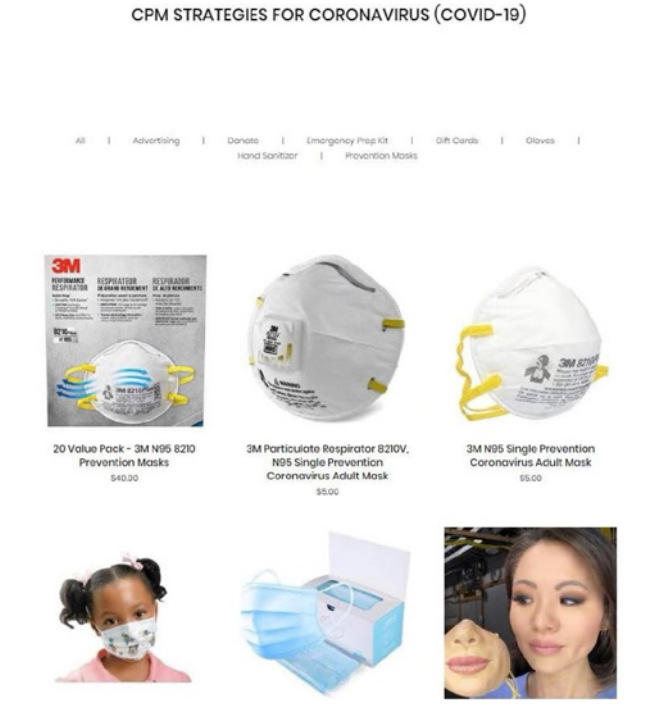


COVID-19

R rucorgza@caravanholidays.cz
To

Hi, neighbor.
Tests confirmed that I was sick with a coronavirus.
Doctors said that in the week I will leave the world.
My parents will be left without my support.
And at this time you will live enjoying.
I think this is unfair, and I suggest you pay me.
What I am sitting at home and don't try to infect your home.
Life or money.
Hurry up! Every hour, I hate you more and more.

My bitcoin address (BTC Wallet) 18P3S6DuNUpW2WLozsrrW6rRd6xh24Rc7N



CPM STRATEGIES FOR CORONAVIRUS (COVID-19)

All | Advertising | Donate | Emergency Prep Kit | Gift Cards | Gloves | Hand Sanitizer | Prevention Masks

20 Value Pack - 3M N95 8210 Prevention Masks $40.00

3M Particulate Respirator 8210V, N95 Single Prevention Coronavirus Adult Mask $5.00

3M N95 Single Prevention Coronavirus Adult Mask $5.00

مقاله‌ای جالب در این خصوص را در لینک زیر بخوانید:

https://www.mcafee.com/blogs/other-blogs/life-at-mcafee/how-one-mcafee-advanced-threat-researcher-is-giving-back-during-covid-19/

جدول زیر بخشی از فهرست نمونه‌هایی است که مک‌آفی آنها در جریان کارزارهای بهره جویی از کووید-۱۹ رصد کرده است. دامنه گسترده‌تری از این تهدیدات توسط راهکارهای مختلف این شرکت نظیر McAfee Global Threat Intelligence و McAfee Adaptive Threat Protection پوشش داده شده است.

نشانه‌های آلودگی:

نشانه آلودگی	نوع
2ec4d4c384fe93bbe24f9a6e2451ba7f9c179ff8d18494c35ed1e92fe129e7fa	SHA256
7e52f7a7645ea5495196d482f7630e5b3cd277576d0faf1447d130224f937b05	SHA256
69724a9bd8033bd16647bc9aea41d5fe9fb7f7a83c5d6fbfb439d21b7b9f53f6	SHA256
f92fecc6e4656652d66d1e63f29de8bfc09ea6537cf2c4dd01579dc909ba0113	SHA256
a5ab358d5ab14b81df2d37aedf52716b5020ab45da472dedc8b8330d129d70bf	SHA256
8028f988c145b98ddd4663d3b5ec00435327026a8533924f7b8320c32737acf4	SHA256
aab93bf5bb0e89a96f93a5340808a7fa2cebf4756bd45d4ff5d1e6c8bdccf75d	SHA256
2e93fe77fafd705e6ca2f61f24e24a224af2490e0a3640ed53a17ea4bf993ec8	SHA256
f850f746f1a5f52d3de1cbbc510b578899fc8f9db17df7b30e1f9967beb0cf71	SHA256
dd78b0ecc659c4a8baf4ea81e676b1175f609f8a7bba7b2d09b69d1843c182cb	SHA256
e352c07b12ef694b97a4a8dbef754fc38e9a528d581b9c37eabe43f384a8a519	SHA256
e82d49c11057f5c222a440f05daf9a53e860455dc01b141e072de525c2c74fb3	SHA256
8bcdf1fbc8cee1058ccb5510df49b268dbfce541cfc4c83e135b41e7dd150e8d	SHA256

فهرست کامل این نشانه‌های آلودگی در لینک زیر قابل دریافت است:

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/covid-19-malware-makes-hay-during-a-pandemic/

توصیه‌ها

تبهکاران سایبری همواره در پی اجرای حملات پیچیده‌تر و بهره‌گیری از هر فرصت ممکن هستند. دورکاری فرصت‌های جدیدی را در اختیار این مهاجمان قرار داده و لازم است که سازوکارها و سیاست‌های دفاعی نیز بر اساس آنها تکامل داده شود. رویدادهای روایت شده در این گزارش اهمیت بکارگیری راهکارهای قدرتمند امنیت سایبری صرف‌نظر از محل حضور کارکنان یادآوری می‌کند. ما باید ترکیب صحیحی از فن‌آوری و آموزش را برنامه‌ریزی و پیاده‌سازی کنیم.

سازمان‌ها نیاز دارند تا در زمان حضور کارکنان در منزل با بکارگیری راهکارهای امنیتی مناسب از اطلاعات حساس و دارایی‌های دیجیتال در برابر سرقت شدن توسط تبهکاران سایبری محافظت کنند.

آینده نامشخص است، تغییر و اختلال قابل پیشگیری نیست و مهاجمان در اقصی نقاط جهان مصمم به بهره‌جویی از آسیب‌پذیری‌های امنیتی هستند. اطمینان از فراهم بودن سازوکارهای دفاعی مؤثر و ابزارهای شناسایی زودهنگام مستلزم تلاشی مستمر و آگاهی از تهدیدات دائماً در حال تغییر و تکامل است.

برای اطلاع بیشتر در مورد تهدیدات مبتنی بر کووید-۱۹ مطالعه گزارش‌های زیر نیز توصیه می‌شود:

سازگاری با رایانش ابری و ریسک آن - نسخه کار از خانه

سیاست‌های اخیر در خصوص کار از منزل تغییرات اساسی در سبک زندگی و کاری ما ایجاد کرده است. گردانندگان تهدید با دنبال کردن این تغییرات، سرویس‌های ابری را بیش از قبل مورد هدف قرار داده‌اند. مشروح گزارش در لینک زیر:

https://www.mcafee.com/enterprise/en-us/forms/gated-form.html?docID=3804edf6-fe75-427e-a4fd-4eee7d189265

قابلیت بازگردانی در ENS 10.7، حفاظی مؤثر در برابر باج‌افزارها

در پی دورکار شدن کارکنان، مهاجمان با بهره‌جویی از چالش‌های تأمین امنیت سیستم‌ها و کشف درگاه‌های آسیب‌پذیر RDP اقدام به توزیع باج‌افزار و انواع دیگر بدافزارها بر روی سیستم‌های کلیدی می‌کنند. مشروح گزارش در لینک زیر:

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ens-10-7-rolls-back-the-curtain-on-ransomware/

آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

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 ۱۰۰) 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