هشدار درخصوص حملات با مضمون ویروس‌کرونا که ویندوز را به بدافزار Lokibot آلوده می‌کند.

Coronavirus-themed Attack Delivers Lokibot Malware

خلاصه‌ی خبر:

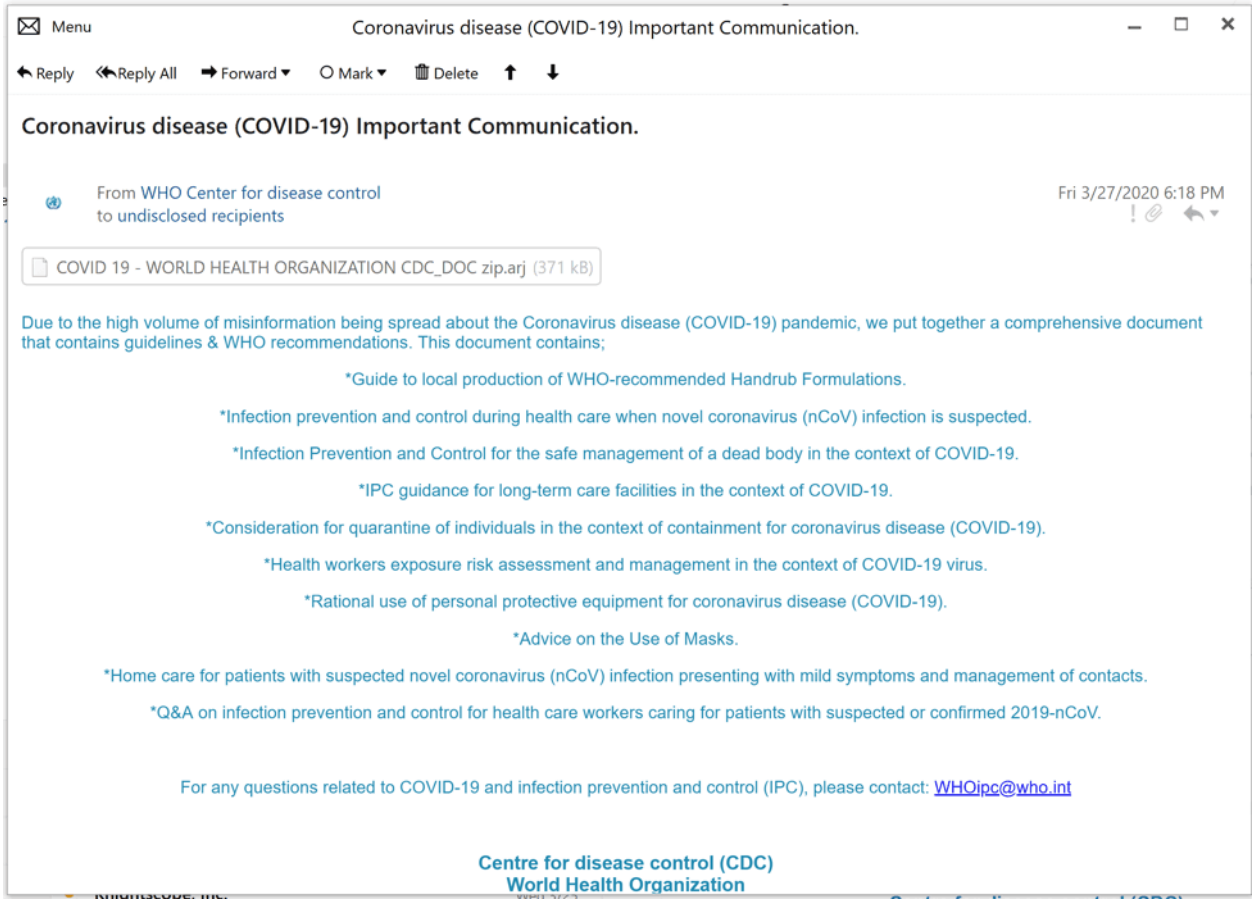
یک کارزار جدید که از ۲۷ مارس فعالیت دارد، از روش‌های مختلفی برای آلوده‌کردن قربانیانش استفاده کرده و کاربران زیادی را در کشورهای مختلفی به‌خصوص ترکیه، پرتغال، آلمان، اتریش و ایالات متحده، فریب داده‌است. این کارزار جدیداً با ارسال یک ایمیل جعلی از طرف سازمان بهداشت جهانی با مضمون و عنوان ویروس‌کرونا و همچنین با داشتن یک فایل با پسوند غیراجرایی در ظاهر، قربانیان را فریب داده و بدافزار Lockibot را بر روی دستگاه‌های آن‌ها نصب می‌کند. این بدافزار که برای سرقت اطلاعات طراحی شده، جدیداً قابلیت‌های بیشتری نیز پیدا کرده است.

اخیراً یک کارزار جدید که با استفاده از ایمیلی با مضمون ویروس‌کرونا/ COVID-19 از طرف سازمان بهداشت جهانی (WHO)، بدافزار مخرب Lokibot را انتشار می‌دهد، مشاهده شده است.

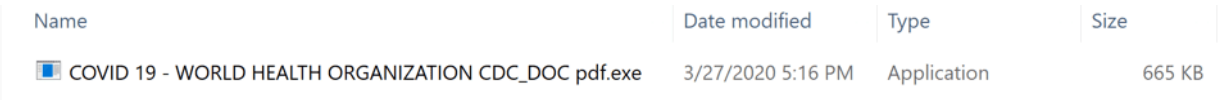
این ایمیل‌ها حاوی یک فایل فشرده هستند که برای فشرده‌سازی از ARJ استفاده‌شده است که برای ایجاد بایگانی فایل‌های فشرده با راندمان بالا استفاده می‌شود.

حمله با مضمون ویروس‌کرونا

هنگام بازشدن فایل فشرده در 7-zip، با مشاهده‌ی پسوند "*Doc.zip.arj*"، روشی‌ست برای فریب کاربران که امید دارند این یک فایل اجرایی نباشد.



این کارزار که توسط Fortinet مشاهده شد، به‌محض باز شدن فایل اجرایی ("COVID_19-WORLD HEALTH ORGANIZATION CDC_DOC.pdf.ece") سیستم قربانی را به بدافزار Lokibot آلوده می‌کند.



بدافزار Lokibot که برای اولین بار در سال ۲۰۱۵ مشاهده شد، به منظور سرقت اطلاعات از دستگاه آلوده طراحی شده است.

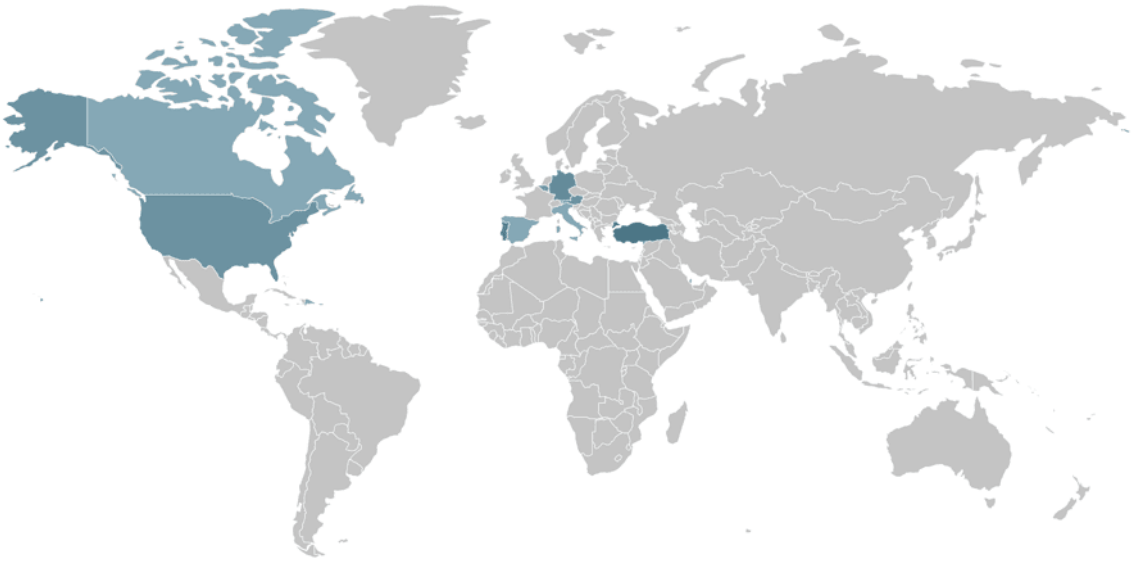
این برنامه اطلاعات و اعتبارنامه‌ها را از برنامه‌های مختلف مانند Mozilla Firefox، Google Chrome، Thunderbird، FTP و SFTP جمع‌آوری می‌کند.

این بدافزار همچنین در بازارهای هک زیرزمینی فروخته شد و در ابتدا به عنوان یک سارق اطلاعات و keylogger معرفی شده بود که بعداً به پیشرفت قابلیت‌های خود ادامه داد.

اخیراً در این بدافزار یک تکنیک قدرتمند در کد آن تزریق شد تا با استفاده از آن شناسایی شدن و تکنیک‌های آنالیز فرار کند و اصطلاحاً این روش‌ها را دور زده و همچنین ابزارهای امنیتی موجود در رایانه‌ی قربانیان هدف، غیر فعال شود.

به گفته Fortiguard، این کمپین از ۲۷ مارس فعال است و به کشورهای زیادی حمله می‌کند.

وی افزود: "۱۰ مکان برتر هدف این کمپین: ترکیه (۲۹٪)، پرتغال (۱۹٪)، آلمان (۱۲٪)، اتریش (۱۰٪) و ایالات متحده (۱۰٪) در صدر این فهرست قرار دارند که بلژیک، پورتو ریکو، ایتالیا، کانادا و اسپانیا با کسب کمتر از یک درصد از این فهرست خارج شدند. "



در یک حمله‌ی اخیر این کازار، بدافزار تروجان Lokibot به عنوان راه‌انداز یک بازی محبوب خود را جا زده و کاربران را برای اجرای بدافزار روی دستگاه‌های خود فریب داده بود.

منبع:

https://gbhackers.com/coronavirus-themed-attack/