

هشدار در خصوص حملات با مضمون ویروس کرونا که ویندوز را به بدافزار Lokibot آلوده می کند.



Coronavirus-themed Attack Delivers Lokibot Malware

خلاصه‌ی خبر:

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

اخيراً یک کارزار جدید که با استفاده از ایمیلی با مضمون ویروس کرونا/ 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 استفاده شده است که برای ایجاد بایگانی فایل‌های فشرده با راندمان بالا استفاده می‌شود.

حمله با مضمون ویروس کرونا

هنگام باز شدن فایل فشرده در 7-zip، با مشاهده‌ی پسوند “Doc.zip.arj”، روشی ست برای فریب کاربران که امید دارند این یک فایل اجرایی نباشد.

Menu Coronavirus disease (COVID-19) Important Communication.

← Reply ↩ Reply All → Forward ○ Mark 🗑 Delete ↑ ↓

Coronavirus disease (COVID-19) Important Communication.

From WHO Center for disease control to undisclosed recipients Fri 3/27/2020 6:18 PM

COVID 19 - WORLD HEALTH ORGANIZATION CDC_DOC zip.arj (371 kB)

Due to the high volume of misinformation being spread about the Coronavirus disease (COVID-19) pandemic, we put together a comprehensive document that contains guidelines & WHO recommendations. This document contains;

- *Guide to local production of WHO-recommended Handrub Formulations.
- *Infection prevention and control during health care when novel coronavirus (nCoV) infection is suspected.
- *Infection Prevention and Control for the safe management of a dead body in the context of COVID-19.
- *IPC guidance for long-term care facilities in the context of COVID-19.
- *Consideration for quarantine of individuals in the context of containment for coronavirus disease (COVID-19).
- *Health workers exposure risk assessment and management in the context of COVID-19 virus.
- *Rational use of personal protective equipment for coronavirus disease (COVID-19).
- *Advice on the Use of Masks.
- *Home care for patients with suspected novel coronavirus (nCoV) infection presenting with mild symptoms and management of contacts.
- *Q&A on infection prevention and control for health care workers caring for patients with suspected or confirmed 2019-nCoV.

For any questions related to COVID-19 and infection prevention and control (IPC), please contact: WHOipc@who.int

Centre for disease control (CDC)
World Health Organization

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

Name	Date modified	Type	Size
COVID 19 - WORLD HEALTH ORGANIZATION CDC_DOC pdf.exe	3/27/2020 5:16 PM	Application	665 KB

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

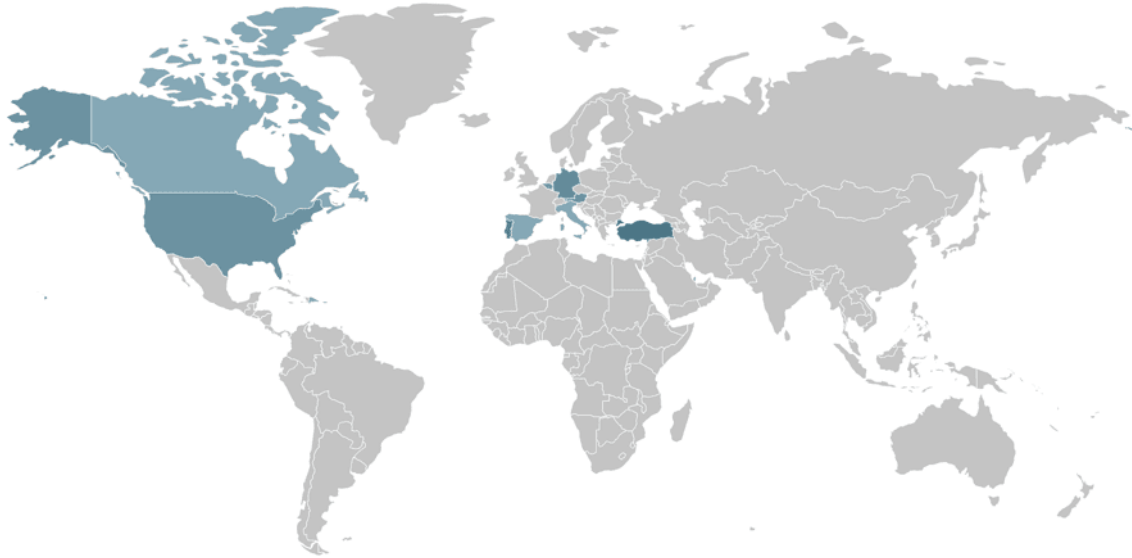
این برنامه اطلاعات و اعتبارنامه‌ها را از برنامه‌های مختلف مانند Google Chrome، Mozilla Firefox، Thunderbird، FTP و SFTP جمع‌آوری می‌کند.

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.

اخيراً 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/>