ترفند جدید هکرها برای سرقت فایل‌های سیستم: ارسال ایمیل جعلی آزمایش ایدز - دیجیاتو

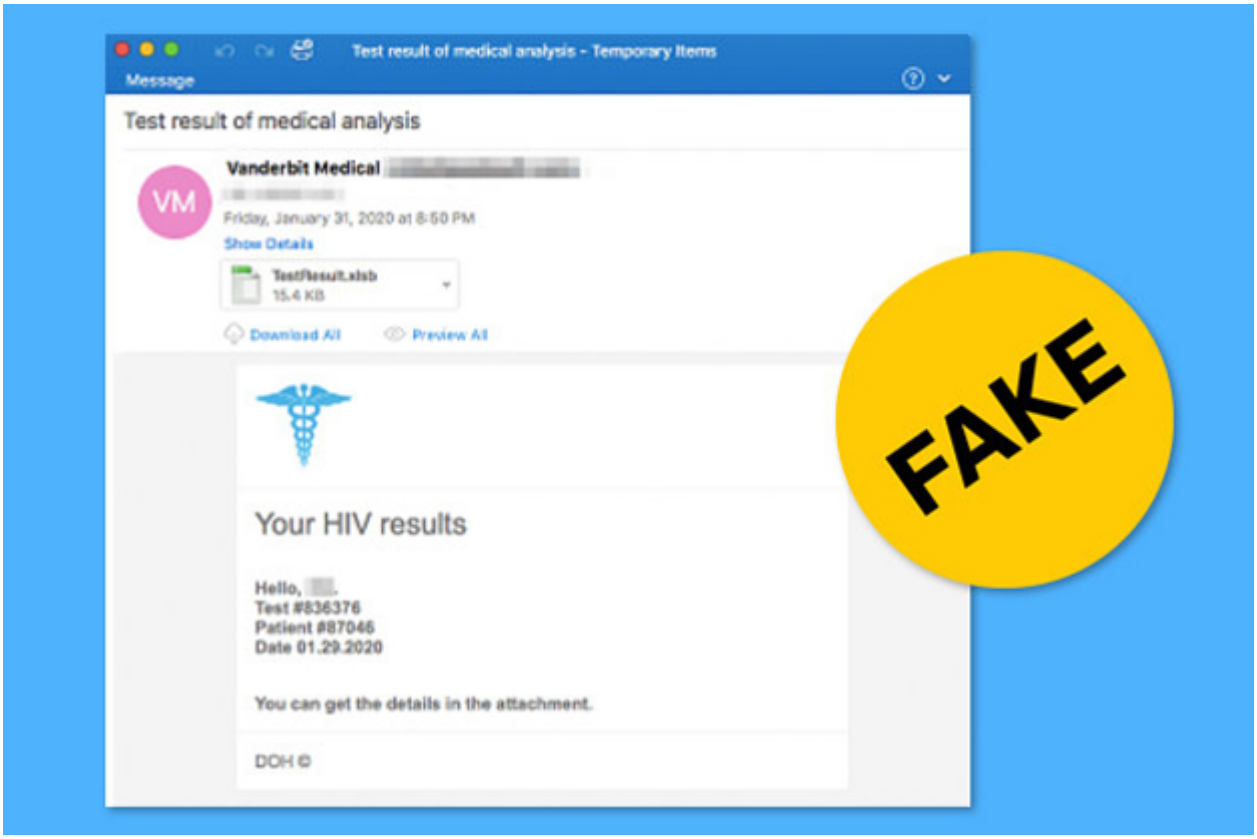
پیمان حسنی | پنجشنبه، ۲۲ اسفند ۱۳۹۸

به گفته محققان امنیتی هکرها با ارسال ایمیل جعلی با عنوان نتایج آزمایش ایدز، کامپیوتر قربانی را به بدافزار آلوده کرده و اطلاعات شخصی آنرا سرقت می کنند.

بر اساس گزارش شرکت تحقیقاتی Proofpoint، هکرها با ارسال ایمیل های فیشینگ و به کمک ابزار مخصوصی که به هکرهای دولتی چین و روسیه ربط داده شده، کامپیوتر قربانی را آلوده می کنند.

هکرها که هویت آنها هنوز مشخص نشده، ایمیل ها را از طرف مرکز پزشکی دانشگاه وندربیلت آمریکا (Vanderbilt University Medical Center) به کاربران ارسال می کنند. ایمیل ها حاوی بدافزاری به نام «Koadic» هستند که قابلیت نفوذ به سیستم کاربر و سرقت فایل های آنرا دارد.

هکرها در قسمت عنوان ایمیل عبارت «نتیجه آزمایش پزشکی» را درج کرده و در متن آن از کاربر می خواهند تا برای مطلع شدن از نتیجه آزمایش ایدز، سریع تر فایل اکسل مخربی که پیوست شده را باز کند. اگر کاربر ماکرو را فعال کند، ابزار Koadic روی سیستم نصب خواهد شد.



به گفته محققان شرکت امنیتی یاد شده، Koadic در واقع یک ابزار منبع باز برای محافظت از شبکه است و به کاربر کنترل کامل به سیستم را می دهد. در سال های اخیر هکرهای وابسته به دولت روسیه و چین از این ابزار برای حمله به کاربران سوءاستفاده کرده اند.

به دام انداختن کاربران از طریق ارسال ایمیل های مربوط به مسائل پزشکی، یکی از روش های مورد علاقه هکرها برای حمله به کاربران است. پیش از این هکرها با سوءاستفاده از بحران کرونا کاربران را با ارسال ایمیل فیشینگ و ساخت سایت های آماری جعلی هدف قرار داده بودند.

محققان شرکت Proofpoint به کاربران توصیه کرده اند تا با ایمیل هایی که مربوط به مسائل پزشکی بوده و ادعا می کنند حاوی اطلاعات مهمی در مورد سلامت کاربر هستند، با احتیاط بسیار بیشتری برخورد کنند. آنها از کاربران خواسته اند تا فایل های پیوست این قبیل ایمیل ها را باز نکرده و شخصاً با پزشک خود صحبت کنند.

دیجیاتو