Bitdefender

مشخصات گروه باج‌افزاری REvil

REvil اولین بار پس از توقف فعالیت GandCrab شناسایی شد. درواقع، نویسندگان REvil عنوان نمودند که آن را از پایه ایجاد نکرده‌اند، بلکه آن را از کدهای GandCrab که اکنون متوقف شده، ایجاد کرده‌اند.

REvil که برگرفته از Ransomware Evil می‌باشد، به Sodinokibi و BlueCrab نیز معروف است و در قالب خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware as a Service - به اختصار RaaS) عرضه شد.

در خدمات RaaS، نویسندگان بدافزار آن را ایجاد کرده و به سایر مهاجمان سایبری واگذار می‌کنند تا سیستم‌ها را آلوده کرده و باج مطالبه کنند. در عوض، نویسندگان بدافزار، ۲۰-۳۰ درصد از باج مطالبه شده را دریافت می‌کنند.

۱۰۰ میلیون دلار
میانگین درآمد سالانه

۱۹ روز
میانگین مدت زمان هر رویداد

بیش از ۱۲۴ هزار دلار
میانگین باج پرداختی به REvil

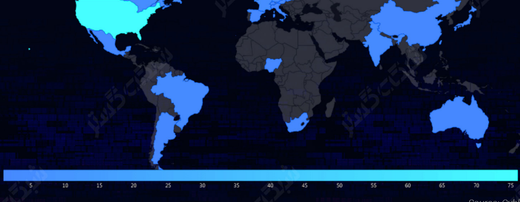
۱۶/۵% از سهم بازار
متداول‌ترین گونه باج‌افزاری در سال ۲۰۲۱

روش‌های متداول آلوده‌سازی

۹% آلودگی از طریق ضعف‌های امنیتی
۹% موارد دیگر

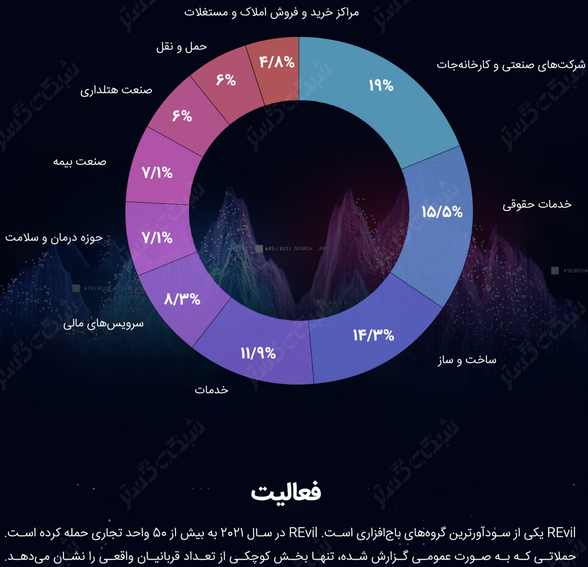
۶۴% آلودگی از طریق RDP
۱۸% آلودگی از طریق فیشینگ

نقشه حملات باج‌افزاری REvil



Source: Cyble Vision

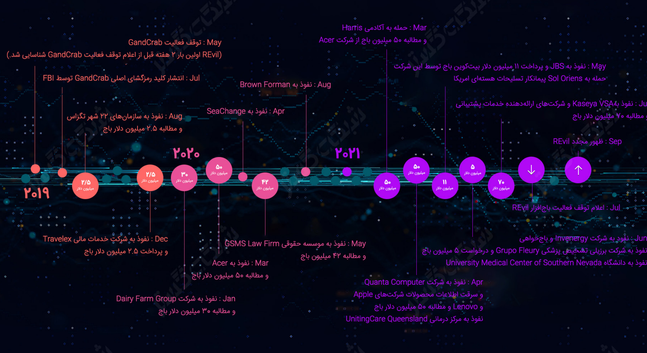
صنایعی که توسط باج‌افزار REvil مورد هدف قرار گرفته‌اند



فعالیت

REvil یکی از سودآورترین گروه‌های باج‌افزاری است. REvil در سال ۲۰۲۱ به بیش از ۵۰ واحد تجاری حمله کرده است. حملاتی که به صورت عمومی گزارش شده، تنها بخش کوچکی از تعداد قربانیان واقعی را نشان می‌دهد. اکثر حملات باج‌افزاری هرگز گزارش نمی‌شوند.

محدوده زمانی برخی از حملات اخیر و شناخته شده باج‌افزار REvil به شرح زیر است.



پیشگیری و کاهش همه‌جانبه حملات باج‌افزاری مستلزم رصد مستمر در تمامی بخش‌های سازمان به‌صورت همزمان است، که هر یک باید توسط راهکارهای امنیتی مربوطه پوشش داده شوند.

فناوری‌های حفاظتی و پیشگیری بیت‌دیفندر، سیستم دفاعی سازمان‌ها را در برابر باج‌افزارها مقاوم می‌کند و حملات موفق را در همان مراحل اولیه شناسایی نموده و اقدامات مخرب و اثرات اولیه یک حمله باج‌افزاری موفق را به حالت قبل برمی‌گرداند.

اطلاعات بیشتر را در این صفحه کسب نمایید.