کشف باج افزار PureLocker که سرورهای سازمانی را هدف گرفته است - دیجیاتو

حمید مقدسی | چهارشنبه، ۲۲ آبان ۱۳۹۸

محققین امنیتی به باج افزار PureLocker برخورده اند که مستقیماً با هدف آلوده کردن سرورهای سازمانی طراحی شده و احتمالاً به یکی از خطرناک ترین گروه های هک دنیا تعلق دارد.

باج افزار جدید که اطلاعات سرورها را رمزنگاری می کند، توسط تحلیلگران امنیتی شرکت Intezer و IBM X-Force شناسایی شده است. این باج افزار به خاطر استفاده از زبان برنامه نویسی PureBasic با نام PureLocker شناخته می شود.

نوشتن باج افزار با استفاده از زبان PureBasic چندان مرسوم نیست، ولی مزایایی را در اختیار هکرها قرار می دهد. اکثر سامانه های امنیتی نمی توانند وجود کد مخرب را در این زبان تشخیص دهند. همچنین برنامه ای که به زبان PureBasic نوشته شود، در هر سه سیستم عامل ویندوز، لینوکس و OS-X قابل استفاده است.

هکرها فعلاً سرورهای سازمانی را با باج افزار PureLlocker هدف گرفته اند و اطلاعات شرکت ها را

رمزنگاری می کنند. واضح است که اگر درخواست چند ده هزار دلاری هکرها را پرداخت نکنید، احتمالاً هیچگاه به اطلاعات دست پیدا نخواهید کرد. هدف قرار دادن سرورها بیشترین آسیب را به کسب و کارها می زند، چون اطلاعات حیاتی و حساس شرکت ها را از دسترس خارج می کند.

در حال حاضر هیچ آماری از تعداد قربانیان باج افزار PureLocker وجود ندارد، ولی محققین امنیتی می گویند این باج افزار در حال حاضر در فروم های زیرزمینی در قالب خدمت (aaS) عرضه شده است. بدین ترتیب فقط گروه های هکری قدرتمند با پرداخت هزینه اولیه نسبتاً زیادی قادر به استفاده از آن هستند.

در کد منبع باج افزار PureLocker نشانه هایی از دیگر بدافزارها دیده می شود که توسط گروه های خطرناکی مثل Cobalt Gang یا FIN6 استفاده شده اند. به همین دلیل کارشناسان معتقدند حملات با این باج افزار به شکل هدفمند و سازمان یافته انجام خواهد شد. احتمالاً روش انتقال این باج افزار هم از طریق ایمیل های فیشینگ خواهد بود.

دیجیاتو