با توجه به اینکه چند روزی است باج‌افزاری موسوم به TYRANT با الهام از یک باج‌افزار متن باز در فضای سایبری منتشر شده و به کاربران ایرانی حمله نموده و از صفحه باج‌خواهی به زبان فارسی استفاده می‌کند به آنها ۲۴ ساعت فرصت داده تا ۱۵ دلار بابت دریافت کلید رمزگشایی بپردازند، این باج افزار بومی توضیحات کاملی در خصوص نحوه پرداخت باج به کاربران آلوده شده می دهد و با توجه به مبلغ کم درخواستی و احتمال زیاد پرداخت آن توسط قربانیان، احتمال حملات و شیوع بیشتر این نوع باج افزار ها در ایران شدت می یابد،

معرفی باج افزار فارسی Tyrant

این باج افزار در محیط سیستم عامل‌های ویندوزی عمل می‌کند؛ و تقریبا فقط نیمی از آنتی ویروس‌های معتبر، قادر به شناسایی این بدافزار هستند.

این باج‌افزار دسترسی به سامانه های قربانی را با قفل کردن آنها مسدود می نماید و فایلهای سیستم های آنان را رمز گذاری می کند و در نهایت با نمایش یک صفحه درخواست باج فارسی اقدام به مطالبه ۱۵ دلار باج به شکل ارز الکترونیکی می نماید، به طوریکه برای برقراری ارتباط با قربانیان از بستر غیرقابل پیگیری تلگرام(@Ttypern) و ایمیل(rastakhiz@protonmail.com) و بررسی پرداخت باج، استفاده می‌کند، روش انتقال این باج افزار فارسی زبان Web money و فیلترشکن سایفون می باشد به طوریکه از طریق شبکه‌های اجتماعی با فریب قربانیان، آنها را تشویق به دریافت و اجرای فایلی اجرایی با ظاهر سایفون می‌کند که در حقیقت حاوی بدافزار است، لازم به ذکر است که احتمالا از دیگر روشهای مرسوم برای توزیع این بدافزار نیز استفاده می شود نظیر دریافت و نمایش پیوست ایمیل، انتشار از طریق وب سایت های آلوده یا RDP حفاظت نشده.

راهکارهای پیشگیری از حمله باج افزار Tyrant

- از اطلاعات سازمانی به‌صورت منظم و مستمر نسخه پشتیبان تهیه کنید.
- بروز رسانی کامل سیستم عامل و Patch های امنیتی
- بروزرسانی مستمر آنتی ویروس سیستم ها و اسکن کامل سیستم ها
- با توجه به انتشار بخش قابل توجهی از باج‌افزارها از طریق فایل‌های نرم‌افزار Office حاوی ماکروی مخرب، بخش ماکرو را برای کاربرانی که به این قابلیت نیاز کاری ندارند با انتخاب گزینه "Disable all macros without notification" غیرفعال کنید.