

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 باج‌افزار بومی توضیحات کاملی در خصوص نحوه پرداخت باج به کاربران آلوده شده می‌دهد و با توجه به مبلغ کم درخواستی و احتمال زیاد پرداخت آن توسط قربانیان، احتمال حملات و شیوع بیشتر این نوع باج‌افزارها در ایران شدت می‌یابد،

Crypto Tyrant

TYRANT

اگر در حال دیدن این پیام هستید، این بدان معنی است که سیستم شما به باج‌افزار تایرنت آلوده شده و تمام فایل‌ها پوشه‌ها و درایوهای سیستم شما درگیر و توسط الگوریتم‌های بسیار پیچیده (ای بی اس آی و ای ای اس) رمزنگاری شده و کلید رمزگشایی فایل‌های شما به صورت خودکار برای ما ارسال گردیده است. وقت تعیین شده برای پرداخت مبلغ 15 دلار و دریافت ابزار و کلید رمزگشایی فایل‌های شما 24 ساعت تعیین شده است. این بدان معنی است که شما 24 ساعت وقت دارید تا مبلغ 15 دلار را به صورت ویمانی برای ما ارسال نمایید تا کلید رمزگشایی فایل‌هایتان جهت بازگردانی آن‌ها به شما داده شود. در غیر اینصورت و در صورت پرداخت نکردن مبلغ تعیین شده، کلید رمزگشایی فایل‌هایتان به صورت خودکار پس از گذشت 24 ساعت از آلودگی سیستم‌تان از بین خواهد رفت و تمام فایل‌های شما برای همیشه نابود خواهند گردید.

WARNING توجه:

بازگردانی فایل‌هایتان زمانی امکان‌پذیر خواهد بود که تا قبل از اتمام 24 ساعت زمان تعیین شده مبلغ درخواستی را برای ما ارسال نمایید و سپس با کلید رمزگشایی دریافت شده از طرف ما فایل‌هایتان را بازگردانید! در غیر اینصورت هیچ روشی برای بازیابی اطلاعات خود نداشته و فایل‌هایتان را برای همیشه از دست خواهید داد. انتخاب از دست دادن و یا بازگردانی فایل‌هایتان با خود شماست!

WARNING اخطار:

در صورت گذشت مدت 24 ساعت و پرداخت نکردن مبلغ درخواست شده، کلید رمزگشایی فایل‌های سیستم شما به صورت خودکار از سرور حذف خواهد شد و نه تنها هیچ‌کس، بلکه بازگردانی فایل‌هایتان توسط ما هم دیگر امکان‌پذیر نخواهد بود.

23h 59m 52s 
زمان باقی مانده تا نابودی
کلید رمزگشایی

نحوه پرداخت و دریافت کلید رمزگشایی

نحوه پرداخت به چه صورت است؟ از طریق خرید دلار الکترونیک و ارسال آن به ما (یا کارت شارژ دلار وبمانی و یا انتقال وجه به صورت مستقیم به حساب وبمانی ما از طریق صرافی های آنلاین)

در حال حاضر تنها و تنها کارت شارژ وبمانی پذیرفته میشود

وبمانی چیست؟ وبمانی یک واحد ارزی پول الکترونیک میباشد

نحوه خرید وبمانی و ارسال آن به ما- با مراجعه به وبسایت فروشگاه های ارز های الکترونیک و ثبت نام در وبسایت و سپس درخواست انتقال وجه 15 دلار وبمانی به حساب ما و سپس ارسال رسید پرداختی شما به فروشگاه برای ما و یا درخواست خرید کارت شارژ وبمانی به مبلغ 15 دلار از همان وبسایت و ارسال شماره کارت شارژ وبمانی برای ما

پس از ارسال وبمانی به ما و دریافت کلید رمزگشایی پس از انتقال مستقیم وبمانی از طریق وبسایت های فروش ارز الکترونیک به حساب ما و یا ارسال کارت شارژ وبمانی به ما و سپس تایید صحت تراکنش از طرف ما، همان لحظه برنامه ای همراه با کلید رمزگشایی سیستم شما برای شما ارسال خواهد گردید که به وسیله آن میتوانید تمام فایل های رمز نگاری شده خود را به حالت اول برگردانید

در صورت وجود هرگونه سوال و یا مشکل به صورت شبانه روزی میتوانید با آی دی تلگرام @TtypeRns در ارتباط باشید

شماره حساب ما در وبمانی _____

ایمیل rastakhiz@protonmail.com

تلگرام @TtypeRns

نمونه ای از فروشگاه های ارز الکترونیک

exchanging.ir webmoney724.ir

webmoneybuy.com

ثبت

معرفی باج افزار فارسی Tyrant

این باج افزار در محیط سیستم عامل های ویندوزی عمل می کند؛ و تقریباً فقط نیمی از آنتی ویروس های معتبر، قادر به شناسایی این بدافزار هستند.

این باج افزار دسترسی به سامانه های قربانی را با قفل کردن آنها مسدود می نماید و فایل های 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 می کند، روش انتقال این باج افزار فارسی زبان Web money و فیلترشکن سایفون می باشد به طوریکه از طریق شبکه های اجتماعی با فریب قربانیان، آنها را تشویق به دریافت و اجرای فایلی اجرایی با ظاهر سایفون می کند که در حقیقت حاوی بدافزار است، لازم به ذکر است که احتمالاً از دیگر روش های 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 به صورت منظم و مستمر نسخه پشتیبان تهیه کنید.
- بروز رسانی کامل سیستم عامل و Patch های امنیتی
- بروز رسانی مستمر آنتی ویروس سیستم ها و اسکن کامل سیستم ها
- با توجه به انتشار بخش قابل توجهی از باج افزارها از طریق فایل های نرم افزار 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.