شیوع باج گیر سایبری جدید در ایران / استفاده از ایمیل جعلی رستاخیز +عکس

مرکز ماهر نسبت به انتشار نوع جدیدی از بدافزار باج گیر در فضای سایبری کشور هشدار داد که این ویروس، برای هدف قراردادن کاربران فارسی زبان طراحی شده است.

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای (ماهر) نسبت به نوع جدیدی از باج افزار خطرناک با زمینه فارسی در فضای سایبری کشور هشدار داد.

بررسی های مرکز ماهر نشان می دهد که باج افزاری موسوم به «TYRANT» با الهام از یک باج افزار متن باز در فضای سایبری منتشر شده است که از صفحه باج خواهی به زبان فارسی استفاده می کند و طبیعتا برای هدف قرار دادن کاربران فارسی زبان طراحی شده است.

نیمی از آنتی ویروس ها قادر به شناسایی «تای رنت» هستند

این باج افزار در محیط سیستم عامل های ویندوزی عمل می کند. تا این لحظه تقریبا فقط نیمی از آنتی ویروس‌های معتبر، قادر به شناسایی این بدافزار هستند.

تای رنت ۱۵ دلار باج می خواهد

باج افزار «TYRANT» با قفل کردن دسترسی به سامانه های قربانی و رمزکردن فایل های سیستم، اقدام به مطالبه ۱۵ دلار باج به شکل ارز الکترونیکی کرده و از بستر غیر قابل پیگیری تلگرام (@Ttypern) و ایمیل (rastakhiz@protonmail.com)برای برقراری ارتباط با قربانی و بررسی پرداخت باج، استفاده می کند.

روش انتشار با فیلترشکن سایفون

در گزارش های واصله، روش انتشار این باج افزار استفاده از پوشش فیلترشکن سایفون بوده و از طریق شبکه های اجتماعی با فریفتن کاربران، آنها را تشویق به دریافت و اجرای فایلی اجرایی با ظاهر سایفون می کند که در حقیقت حاوی بد افزار است.

البته با توجه به ماهیت حمله، استفاده از دیگر روش های مرسوم برای توزیع این بدافزار، از جمله پیوست ایمیل، انتشار از طریق وب سایت آلوده یا RDP حفاظت نشده نیز محتمل است.

روش انتقال باج که این باج افزار از آن استفاده می کند، «Web money»است و سازنده باج افزار، مدت ۲۴ ساعت فرصت برای پرداخت باج، در نظر گرفته است.

همچنین به منظور راهنمایی قربانی، آدرس تعدادی از وب سایت های فارسی ارائه کننده این نوع از ارز الکترونیکی توسط باج افزار معرفی می شوند.

تحلیل‌های اولیه نشان می‌دهد که احتمالا این نسخه اول یا آزمایشی از یک حمله بزرگتر باشد چرا که با وجود مشاهده شدن کدهای مربوط به رمزگذاری فایل ها، گاهی باج افزار موفق به رمزگذاری فایل های قربانی نمی شود و از آن مهمتر اینکه با وجود ایجاد تغییرات بسیار در رجیستری سیستم قربانی، موفق به حفظ قابلیت اجرا در زمان پس از ریستارت کردن سیستم نمی شود. با این وجود به نظر نمی رسد که تاکنون از محل این باج افزار خسارت قابل توجه ای ایجاد شده باشد.

راهکار های پیشگیری را جدی بگیرید:

۱ -از دریافت فایلهای اجرایی در شبکه های اجتماعی و اجرای فایل های ناشناخته و مشکوک پرهیز شود.

۲ -از دانلود و اجرای فایل‌های پیوست ایمیل‌های ناشناس و هرزنامه‌ها خودداری شود.

۳ -دقت ویژه در به روزرسانی دایم سیستم عامل و آنتی ویروس.

۴ -دقت ویژه در پرهیز از استفاده از دسترسی راه دور و در صورت عدم امکان حذف دسترسی راه دور و رعایت دقیق تمهیدات امنیتی

۵ -عدم استفاده از مجوز دسترسی Administratorروی سیستم‌های کاربران سازمانی

اواسط هفته گذشته نیز وزیر ارتباطات اعلام کرد که به تعدادی از وب سایتهای ایرانی حمله ای صورت پذیرفت.

محمدجواد آذری جهرمی با تاکید براینکه دامنه این حمله سایبری شناسایی و کنترل شده است از تربیت ۱۰ هزار نیروی امنیت سایبری طی ۴ سال آینده خبر داده است.