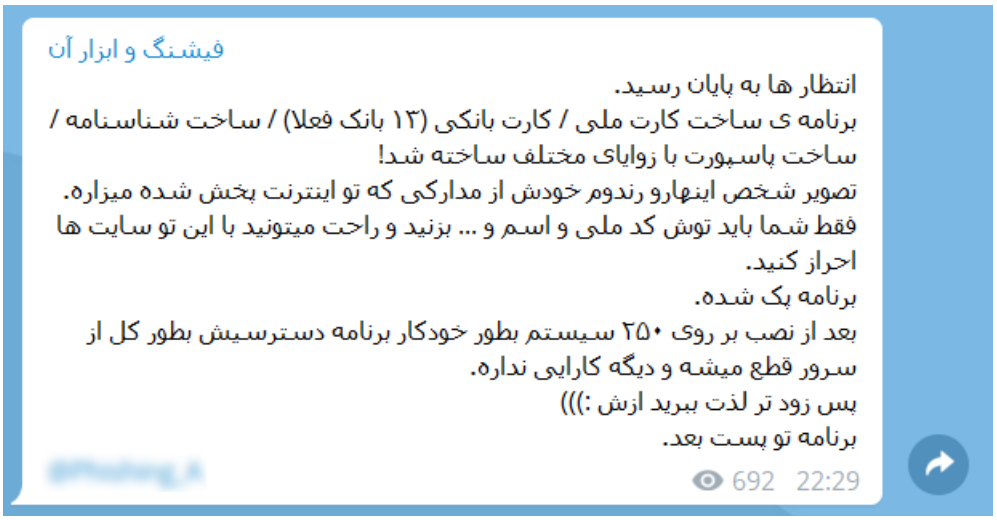
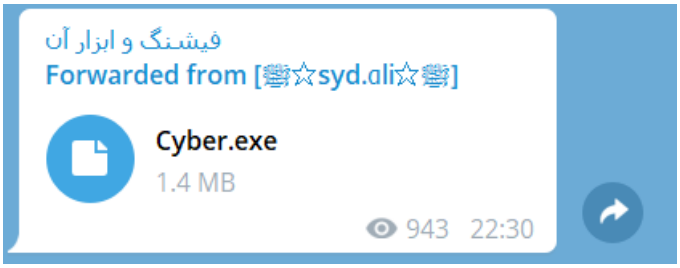
هشدار در خصوص انتشار باج افزار Cybersccp در کانال های تلگرامی فارسی زبان

مشاهدات اخیر در فضای سایبری کشور مخصوصاً در پیام‌رسان تلگرام حاکی از آن است که یک باج‌افزار از خانواده خطرناک شناخته شده HiddenTear با نام Cyber.exe در پوشش برنامه‌ای کاربردی با ادعای ساخت تصویر جعلی کارت ملی، کارت بانکی، شناسنامه و پاسپورت با پیامی به شرح زیر در حال انتشار است:





قربانیان که عموماً افراد مبتدی و با انگیزه جعل هویت هستند، پس از دریافت فایل Cyber.exe با حجم ۱,۴۲ مگابایت و اجرای آن بر روی رایانه خود در محیط سیستم عامل ویندوز در معرض حمله باج‌افزاری قرار می‌گیرند. آیکن فایل اجرایی این باج‌افزار به شکل زیر می‌باشد:

بررسی‌ها نشان می دهد که باج‌افزار مورد اشاره، تمام فایل‌های موجود بر روی دسکتاپ قربانی را رمزگذاری کرده و پس از رمزگذاری، به ابتدای فایل‌ها، عبارت .Lock اضافه می‌کند. حتی میانبرهای نرم‌افزارها نیز پس از حمله باج افزار، قابل اجرا نخواهند بود. سپس با تغییر پس‌زمینه دسکتاپ به شکل زیر، دو فایل به نام‌های Lock.Cyber.exe و Lock.desktop.ini نیز بر روی دسکتاپ ایجاد می‌کند.

همانطور که در تصویر مشخص است، باج‌افزار برای رمزگشایی فایل‌ها، از قربانیان طلب ۰٫۰۳ بیت کوین باج می‌کند.

مرکز ماهر موکداً به کاربران در فضای مجازی متذکر می‌شود که از دریافت و اجرای فایل‌های اجرایی از منابع ناشناخته پرهیز نمایند.

همچنین یادآور می‌شود که بر اساس قانون جرایم رایانه‌ای مصوب در تاریخ ۱۱ بهمن ۱۳۸۹ مجلس شورای اسلامی، هریک از فعالیت‌های مورد ادعا در پوشش انگیزشی این بدافزار، جرایمی جدی بوده و مورد تعقیب قضایی قرار خواهد گرفت.

در انتها و به عنوان یک توصیه کلی خاطر نشان می‌گردد که ساختار حملات باج‌افزاری به گونه‌ای است که با وجود رعایت تمام تمهیدات، در حال حاضر موثرترین راهکار پیشگیری، تهیه منظم نسخ پشتیبان از اطلاعات و نگهداری آن‌ها بصورت آفلاین می‌باشد.