اداره کل ارتباطات و فناوری اطلاعات استان همدان

اطلاع رسانی در خصوص بدافزار رجین – Regin

تاریخ: ۹۳/۹/۸

تاریخچه ویروس:

نام Regin در حقیقت معکوس شده In Reg و یا به طور کامل‌تر In Registry است. چرا که ماژول‌های آن در رجیستری ذخیره می‌گردد.این بدافزار یک تروجان back-door است که بسته به هدف، با گستره متنوعی از قابلیت‌ها سفارشی‌سازی می‌شود. به گفته سیمانتک، تولید این بدافزار ماه‌ها و حتی سال‌ها زمان برده است و نویسندگان آن تمام سعی خود را برای پوشاندن ردپای این بدافزار کرده‌اند. این بدافزار با ماژول‌های متفاوت سفارشی سازی شده برای سرقت انواع خاص اطلاعات، غالباً شرکت‌های مخابراتی، سازمان های دولتی و دستگاه های اجرایی، بنگاه های اقتصادی بزرگ ، موسسات پژوهشی و افراد شخصی که در مورد موضوعات خاصی (که مدیران بدافزار رجین تعریف کرده اند) پژوهش و تحقیق می کرده اند را هدف قرار داده است. به نظر می‌رسد که مهاجمان به دنبال اطلاعات لاگین برای ایستگاه‌های پایه (BTS) شبکه GSM نیز بوده‌اند. به طور مختصر، Regin یک حمله سایبری است که مهاجمان را قادر می‌سازد تا در کل شبکه قربانی بتوانند دسترسی را در تمام سطوح به دست آورند و کنترل از راه دور داشته باشند. این پلتفرم به صورت ماژولار بوده و دارای مراحل (Stage) مختلف است.. تا کنون، دو هدف اصلی حملات ناشی از این بدافزار مشاهده شده است:

۱- جمع آوری اطلاعات هوشمند افراد یا سازمان ها

۲- تسهیل سایر حملات با حمله به اپراتورهای مخابراتی و باز کردن راههای اضافی

نحوه شناسایی سیستم های آلوده به این بدافزار:

در صورتی که فایل‌های زیر در مسیرهای گفته شده در سیستم شما وجود دارد به رجین آلوده شده‌اید.

C:\Windows\system32\nsreg1.dat

C:\Windows\system32\bssec3.dat

C:\Windows\system32\msrdc64.dat

فایل‌های یاد شده معمولا به عنوان نشانه‌های باقی مانده از رجین در سیستم‌های آلوده به این بدافزار (حتی پس از پاک شدن خود بدافزار) یافت می‌شوند.

اقدامات پیشگیرانه برای جلوگیری از آلوده شدن به این بدافزار:

استفاده از آنتی ویروس دارای حق امتیاز (قویا از استفاده از آنتی ویروس های کرک شده اجتناب کنید) و بروز رسانی آن

به روز رسانی نرم افزارهای کاربردی سازمان و مدیریت دائم اصلاحیه ها

مدیریت مناسب رمزهای عبور

تعریف دقیق و سخت گیرانه دسترسی کارکنان سازمانی در شبکه

تعریف دقیق قوانین مربوط به امنیت پست الکترونیک و استفاده از ابزارهای مانیتورینگ شبکه

آموزش کارکنان سازمانی و اطلاع رسانی های دوره ای در حوزه امنیت شبکه

استفاده از ابزار های مکمل مانند ابزارهای مدیریت یکپارچه تهدیدها (UTM) بر روی درگاه های اصلی اینترنت شبکه

منبع: www. securelist.com