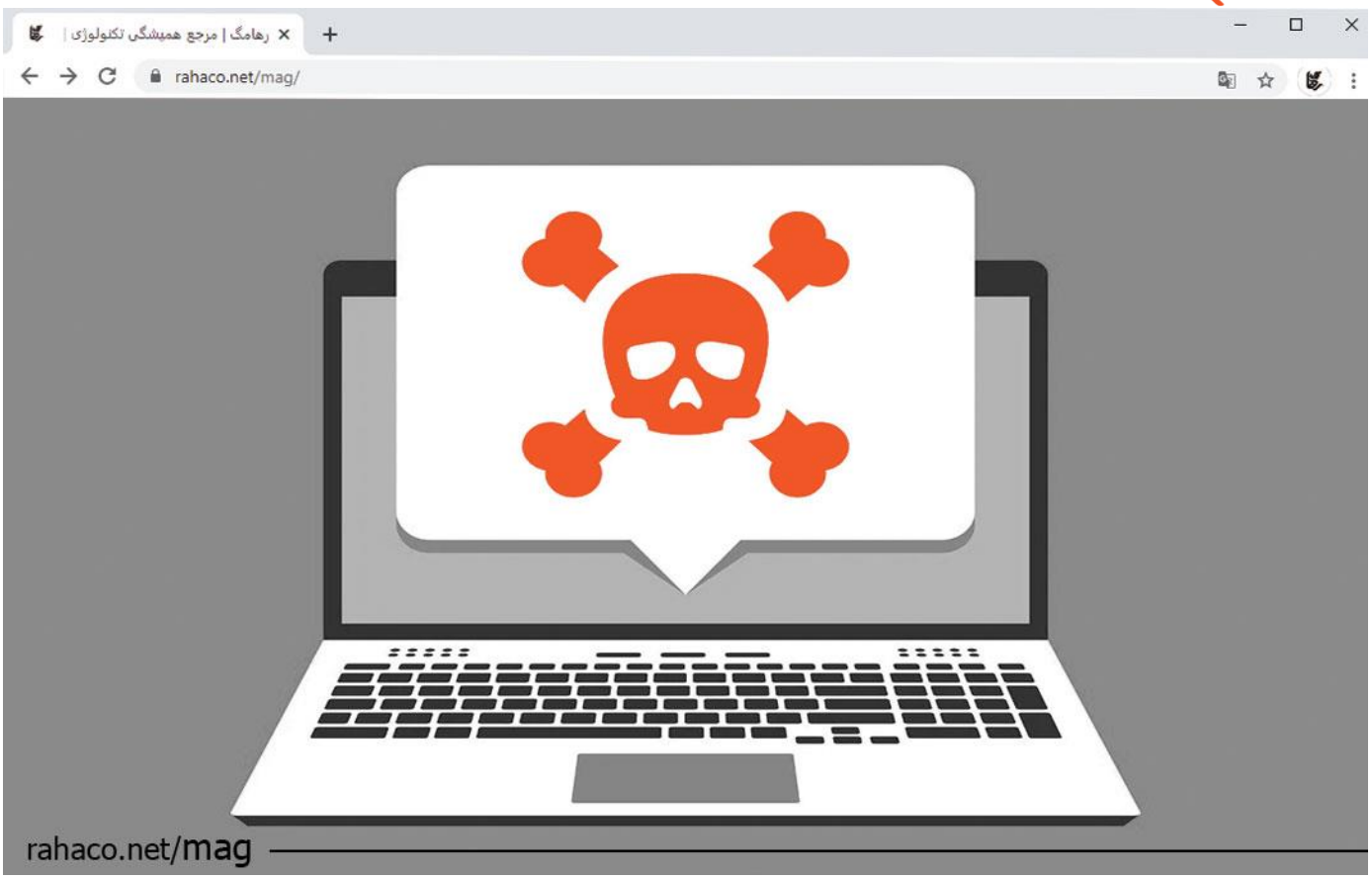
هشدار جدی، بدافزار Dolphin اطلاعات مهمتان را هک می‌کند!

شرکت رهاکو

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

شرکت ESET به عنوان یک شرکت فعال در حوزه امنیت سایبری به تازگی بدافزار خطرناکی را تحت عنوان Dolphin کشف کرده است که تحت حمایت دولت کره شمالی می‌باشد. این گروه هکری مدت‌هاست که در حال فعالیت است. به گفته محققان این بدافزار پس از نصب شدن بر روی رایانه‌های شخصی و آلوده کردن سیستم عامل ویندوز می‌تواند تمام دستگاه‌های متصل به رایانه را برای سرقت اطلاعات بیشتر و ویروسی کردن مورد بررسی قرار دهد. شاید برخی از آن ها ساده به نظر برسند اما با گذشت زمان نسخه‌های پیشرفته‌تر و پیچیده‌تری از بدافزارها طراحی می‌شوند؛ درست مانند بدافزار.Dolphin

انواع بد افزارها

بدافزار یکی از ابزارهای اقدامات ضد امنیتی است و به برنامه هایی گفته می شود که بدون اجازه صاحب سیستم قصد انجام کارهای ناخواسته یا خرابکارانه در سیستم دارند. انواع متنوعی از بد افزار وجود دارد که شامل: ویروس‌های کامپیوتری، تروجان‌ها، باج افزارها، نرم افزارهای جاسوسی، کرم‌ها و بات نت‌ها می‌شود.

ویروس‌های کامپیوتری

ویروس کامپیوتری برنامه مخربی است که خود را با کپی در برنامه‌های دیگر تکثیر می‌کند. به عبارت دیگر ویروس‌های کامپیوتری خود به خود درون سایر کدهای اجرایی و برنامه‌ها گسترش می‌یابند. هدف از ایجاد ویروس کامپیوتری این است که سیستم‌ها را آلوده کرده و کنترل سیستم را بدست آورد. هکرها این ویروس‌ها را با هدف تخریب کاربران آنلاین طراحی می‌کنند.

تروجان‌ها

این نوع بد افزار به شکل‌های مختلف برای فریب کاربران وارد کامپیوتر می‌شود و به قسمت‌هایی از کامپیوتر که برای آن برنامه ریزی شده است، حمله می‌کند. تروجان‌ها می‌توانند با ورود به سیستم کاربران به صورت یک نرم افزار یا یک برنامه قانونی علاوه بر دسترسی به پرونده‌ها و فایل‌های کاربران، آن‌ها را به سیستم‌های دیگر نیز ارسال کند.

باج افزارها

باج افزارها نوع خطرناکی از بد افزارها هستند که به سیستم‌های افراد، شرکت‌های شخصی و دولتی نفوذ کرده و دسترسی به سامانه یا فایل‌هایی مانند اطلاعات مالی را محدود می‌کنند. محدود کردن دسترسی توسط باج افزار معمولا از طریق رمزگذاری یا قفل کردن روی فایل‌ها و داده‌ها صورت می‌گیرد. باج افزار می‌تواند از طریق لینک‌های فریبنده مانند: ایمیل، پیامک، وب سایت و غیره به سیستم نفوذ کند. مهاجم در ازای ارسال کلید رمز گشایی برای کاربر، از او باج درخواست می‌کند. این اتفاق در دنیای خرید و فروش ارز دیجیتال نیز زیاد اتفاق می افتد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

نرم افزارهای جاسوسی

این نوع از بد افزارها به صورتی طراحی شده‌اند که مخفیانه فعالیت‌های یک سیستم را زیر نظر بگیرند. این اطلاعات ممکن است برای ردیابی فعالیت آنلاین کاربر مورد استفاده قرار بگیرد یا به رقیبان فروخته شود. به همین ترتیب، گاها از نرم افزارهای جاسوسی برای دزدیدن اطلاعات شخصی استفاده می‌شود. یعنی اطلاعاتی مانند: گذرواژه‌ها یا شماره کارت اعتباری ممکن است منجر به سرقت هویت شود.

بات نت‌ها

بات نت‌ها شبکه‌هایی هستند که با در اختیار گرفتن مجموعه‌ای از کامپیوترها به نام بات (bot) تشکیل می‌شوند. این شبکه‌ها توسط یک یا چند مهاجم که botmasters نامیده می‌شوند، با هدف انجام فعالیت‌های مخرب طراحی شده است. به عبارت ساده‌تر، هکرها با انتشار ویروس‌ها و برنامه‌های مخرب به صورت غیر قانونی و بدون اطلاع صاحب کامپیوتر کنترل آن را در دست می‌گیرند. سپس درخواست‌های جعلی زیادی را به سمت سرور یا سایت قربانی ارسال می‌کنند که منجر به انجام یک حمله DDoS می‌شود.

کرم‌ها

کرم‌ها نوع متفاوتی از بدافزارها هستند که مانند ویروس بعد از ورود به محیط شبکه یا یک کامپیوتر به سرعت تکثیر می‌شوند. برخلاف ویروس‌ها، کرم‌ها به برنامه یا فایل میزبان برای اجرا شدن در محیط باینری نیاز ندارند. بلکه با دانلود یک نرم افزار آلوده از سطح اینترنت و سایتی نامعتبر یا حتی از طریق پلاگ کردن یک فلش آلوده، کرم به همراه فایل‌ها وارد سیستم می‌شود.

بدافزار Dolphinچیست و چگونه کار می‌کند؟

بد افزار Dolphin یک جاسوس افزار و گروه هکری دولت کره شمالی است که هدف آن جمع آوری دیتا و آسیب رساندن به ارگان‌های خاص می‌باشد. تا کنون چهار نسخه مختلف از این بدافزار کشف شد. نکته قابل توجه این است که بد افزار Dolphin می‌تواند تمام اطلاعات حساس موجود در تمام درایوهای محلی و خارجی از جمله اطلاعات گوشی موبایل را اسکن کند. به گفته ESET ، تروجان این کار را از طریق Windows Portable Device API انجام می‌دهد Dolphin .دستورات خود را از Google Drive دریافت و اطلاعات سرقتی را نیز به آن ارسال می‌کند. علاوه بر این، بدافزار Dolphin اطلاعاتی مانند نام کامپیوتر و آدرسIP ، مشخصات سخت افزاری و نسخه سیستم عامل را هم می‌تواند استخراج کند.

بدافزار Dolphin از روش‌های استاندارد مبتنی بر پایتون برای پیدا کردن دستگاه‌های مختلف و نفوذ به آن‌ها استفاده می‌کند. در مرحله بعد، اطلاعات حساسی مانند رمز عبور و مدارک امنیتی را در حساب Google Drive یک گروه

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

هکری آپلود کرده و هکرها می‌توانند به راحتی به آن‌ها دسترسی داشته باشند. محققان شرکت ESET همچنان دریافتند که بدافزار Dolphin به راحتی می‌تواند به افزونه‌های نصب شده روی سیستم، تصاویر ذخیره شده و اسکرین شات‌ها دسترسی داشته باشند.

هدف هکرهای کره شمالی از ایجاد بدافزار Dolphinچیست؟

گزارش‌های منتشر شده نشان می‌دهد بد افزار Dolphin تا به امروز تنها در حملات watering hole مورد استفاده قرار گرفته است. این حملات اغلب افراد رده بالای دولتی مانند: رئیس بانک‌ها، نظامیان و غیره را مورد هدف قرار می‌دهند. بنابراین، می‌توان گفت که هکرهای کره شمالی با انتشار بدافزار Dolphin به دنبال هدف قرار دادن کاربران یا گروه‌های خاص با دسترسی به داده‌ها یا سیستم‌های ارزشمند هستند نه کاربران عادی.

کره شمالی یک از فعال‌ترین کشورها در زمینه جرایم سایبری محسوب می‌شود که در چند سال گذشته حملات زیادی را به دولت خود داشته است. شاید مهم‌ترین حمله هکرهای کره شمالی در سال‌های گذشته به گروه Lazarus مربوط می‌شود که در جریان آن تقریبا 625 میلیون دلار رمز ارز از شبکه بلاکچین Ronin سرقت شد.

تعریف بد افزار به صورت کلی

بد افزار همان نرم افزار است که از عمد برای خراب کردن رایانه، سرور و شبکه کامپیوتری طراحی می‌شود. بدافزارها توسط هکرهای کلاه سیاه برای سرقت اطلاعات شخصی، مالی یا تجاری مورد استفاده قرار می‌گیرند. این تروجان‌ها به طور گسترده علیه شرکت‌ها برای سرقت دیتاهای حساس یا مختل کردن عملکرد وبسایت‌ها استفاده می‌شود. از زمان دسترسی گسترده به اینترنت نرم افزارهای مخرب بیشتری طراحی و مورد استفاده قرار گرفتند. بد افزارها می‌توانند انواع کارهای مخرب را از سرقت اطلاعات حساس گرفته تا از بین بردن کل سیستم‌ها و دستگاه‌ها انجام دهند. در بیشتر حملات سایبری نفوذ بد افزارها از طریق سرقت اطلاعات گاهی منجر به سرقت هویت هم می‌شود.

نتیجه گیری

گروه‌های هکر تحت حمایت دولت کره شمالی به تازگی بدافزار Dolphin را در فضای مجازی منتشر کرده‌اند که سیستم‌های کامپیوتری را آلوده می‌کند. این بدافزار به راحتی می‌تواند تمام دستگاه‌های متصل به سیستم مانند: فلش USB و گوشی‌های هوشمند را شناسایی کرده و اطلاعات موجود در حافظه را به سرقت می‌برد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net