چهار شنبه 27 اردیبهشت 1396 - 06:26

تلاش جهانی برای شکار خالقان باج‌افزار

همزمان با آغاز عملیات پاکسازی سازمان‌های مختلف در سرتاسر جهان که به بدافزار باج‌خواهی سایبری آلوده شده‌اند، توجه‌ها متوجه افرادی شده که این حملات وسیع را مدیریت کرده‌اند.

همزمان با آغاز عملیات پاکسازی سازمان‌های مختلف در سرتاسر جهان که به بدافزار باج‌خواهی سایبری آلوده شده‌اند،‌ توجه‌ها متوجه افرادی شده که این حملات وسیع را مدیریت کرده‌اند.
براساس گزارش BBC، این بدافزار از آسیب‌پذیري استفاده کرده که توسط آژانس امنیت ملي آمریکا ایجاد شده‌است،‌ اما استفاده ابزاري از این نقص امنیتي و به کارگیري آن به عنوان يك سلاح توسط فرد و یا افرادي کاملا متفاوت انجام گرفته‌است، افرادي که تا به امروز هویت آنها آشکار نشده‌است.
میکو هیپونن رئیس شرکت امنیني اف-سکیور مي‌گوید بررسي بدافزار هیچ ردپایي از مجرمي را آشکار نکرده‌است. به گفته وي درحال حاضر بیش از 100 گروه مختلف باج‌خواهي سایبري را تحت نظر دارند اما مشخص نیست باج‌افزار WannaCry توسط کدامیك مورد استفاده قرار گرفته‌است زیرا نشانه‌ها و ردپاهاي به جا مانده بسیار محدود و گنگ هستند.
اولین نسخه از این باج‌افزار در 10 فوریه 2017 در يك حمله کوتاه‌مدت باج‌‌خواهي مورد استفاده قرار گرفت، اما هیچ‌فردي به عنوان عامل این حمله دستگیر نشد. نسخه بعدي باج‌افزار که طي روزهاي گذشته در سرتاسر جهان فاجعه به بار آورده‌است، تفاوتي کوچك نسبت به نسخه اول داشت و مي‌توانست به صورت مستقل منتشر شود.
بررسي کد‌هاي باج‌افزار گاه مي‌تواند اطلاعاتي قابل ردیابي از عامل منتشر‌کننده بدافزار در اختیار متخصصان قرار دهد اما در این مورد خاص هیچ اطلاعاتي به دست نیامده‌است. با این‌همه گروهي از متخصصان باور دارند از آنجایي که این بد‌افزار بیشتر به سیستم‌هایي که تحت الفباي سیریلیك فعالند تمایل دارد، گروهي کاملا جدید هدایت آن را به عهده داشته‌است. از سویي دیگر بیشتر بدافزارهایي که از روسیه نشات مي‌گیرند تلاش دارند تا از آلوده ساختن کاربران روسي خودداري کنند.
همچنین بررسي‌ها نشان داده که کدهاي بدافزار توسط سیستم سرهم‌بندي شده که زمان آن 9 ساعت جلوتر از زمان گرینویچ بوده‌است و این یعني مکاني در ژاپن،‌ فیلیپین، اندونزي یا بخش‌هایي دورافتاده در چین یا روسیه.
موفقیت بالاي این باج‌افزار در آلوده کردن بیش از 200 هزار رایانه، ثبت نکردن نام دامنه‌اي که در کد‌هاي باج‌افزار دیده مي‌شود و استفاده از سه آدرس کد‌دار بیتکویني براي پرداخت باج‌ها که ردیابي فرد پرداخت‌کننده و دریافت‌کننده را دشوار ساخته‌است، همگي از نشانه‌هایي هستند که خبر از جدید بودن فرد یا افراد مسئول این حمله سایبري مي‌دهند.
با این‌همه ازآنجایي که بیت‌کوین به اندازه دلخواه سارقان سایبري ناشناخته نیست، و هر تراکنش مالي در آن ثبت مي‌شود، محققان مي‌توانند از این اطلاعات براي ایجاد تصویري از مسیر جریان پول‌ها استفاده کرده و در نهایت منجر به کشف ردپایي از آنها شود. درحال حاضر بیش از 50 هزار دلار پول باج به آدرس‌هاي بیت‌کویني پرداخت شده‌است.