دوشنبه 13 تیر 1390 - 10:23

گسترش کلاهبرداری آلمان‌ها در فضای مجازی

ارتکاب جرم در فضای مجازی، روز به روز افزایش می‌یابد. اداره‌ی جنایی آلمان تنها در سال ۲۰۱۰، بیش از ۶۰ هزار مورد کلاهبرداری اینترنتی را به ثبت رسانده است

ارتکاب جرم در فضای مجازی، روز به روز افزایش می‌یابد. اداره‌ی جنایی آلمان تنها در سال ۲۰۱۰، بیش از ۶۰ هزار مورد کلاهبرداری اینترنتی را به ثبت رسانده است.

این رقم نسبت به موارد تقلب در سال ۲۰۰۹، ۲۰ درصد افزایش داشته است.

به گزارش رادیو دولتی آلمان، بنابر گزارش رئیس اداره جنایی آلمان، یورگ تسیرکه، زیان‌های ناشی از جرائم ارتکابی در اینترنت که در سال ۲۰۰۹ بر ۳۷ میلیون یورو بالغ می‌شده، در سال ۲۰۱۰ به حدود ۶۱ و نیم میلیون یورو رسیده است. تسیرکه تأکید می‌کند که این زیان‌ها تنها محدوده‌های روشن، یعنی مواردی که کشف شده را شامل می‌شود. به نظر وی، زیان‌های ناشی از خلافکاری‌ها در محدوده‌های تاریک، یعنی مواردی که به دلایل مختلف کشف و ثبت نشده، تقریباً دو برابر جرائم محدوده‌های روشن است.

•کاربر بی‌اطلاع
رایج‌ترین شیوه‌ای که کلاهبرداران اینترنتی از آن استفاده می‌کنند، روش بات نتسه (Bot-Netze)، یعنی وصل تعداد زیادی رایانه ویروس‌دار به یکدیگر است، بدون این که کاربر از آن اطلاع داشته باشد.

خلافکاران اینترنتی با بکارگیری روش بات نتسه به کامپیوترهای ادارات و سازمان‌های دولتی، شرکت‌های بزرگ و بین‌المللی حمله می‌برند و کار و فعالیت آن‌ها را متوقف می‌سازند، تا به اهداف خود (اغلب اخاذی یا اعمال فشار سیاسی) برسند. یورگ تسیرکه در این رابطه می‌گوید: روزانه بیش از ۷۰۰ هزار کامپیوتر برای این نوع کلاهبرداری‌ها مورد استفاده قرار می‌گیرند. کارشناسان امور فنی ادارات دولتی و نهادهای مبارزه با جرائم اینترنتی، از سوی دیگر، پیوسته در حال کشف راه‌ها و شیوه‌های مقابله با شگردهای خلافکاران اینترنتی هستند.

دیتر کرمپ، رئیس اتحادیه‌ی اطلاعات، ارتباطات و رسانه‌ها در این مورد می‌گوید: وقتی بانک‌های بزرگ سیستم جدیدی را بکار می‌گیرند، از شمار حمله‌های خلافکاران اینترنتی کاسته می‌شود، تا این که کاربران به استفاده از آن سیستم عادت کنند و خلافکاران روش‌های تازه‌ای را برای دستیابی به داده‌های شخصی کاربران بیابند. در این مرحله باز بر شمار حمله‌های متقلبان افزوده می‌شود.

•سهل‌انگاری کاربران
یکی از عواملی که موجب موفقیت خلافکاران در فضای مجازی شده، بی‌توجهی و عدم دقت کاربران رایانه‌های خانگی و دستی است. بر اساس جدیدترین آمار اتحادیه‌ی اطلاعات، ارتباطات و رسانه‌ها، با این که بیش از ۸۵ درصد کاربران احساس خطر می‌کنند از اینکه هدف حمله‌های اینترنتی قرار بگیرند، تنها یک تن از چهار نفری که تلفن دستی اینترنت‌دار در اختیار دارد، مجهز به برنامه‌های ضدویروس است و تنها یک تن از هر پنج نفر از سد ایمنی شبکه‌ی رایانه‌ای دیوار آتش استفاده می‌کند.

یورگ تسیرکه، یکی از راه‌های مبارزه با خلافکاران را ضبط آدرس‌های رمز رایانه‌ها، به‌طور کلی، می‌داند. این کار ولی در آلمان ممنوع است. او می‌گوید: از آن‌جا که خطر مجازات شدن، به دلیل وجود محدودیت‌های تحقیق و یافتن خاطی، اندک است، شمار حمله‌های اینترنتی روز به روز افزایش می‌یابد.

چطور کلمه عبور خود را حفظ کنیم؟

با وجود این، شرکت‌هایی که کالاهای خود را از طریق اینترنت به فروش می‌رسانند، چندی است که مرکز مبارزه با روش بات نتسه را دایر کرده‌اند. کارکنان این مرکز، به محض آن که از حمله‌ای اینترنتی به یک شرکت ارائه‌ی خدمات باخبر شوند، بلافاصله به کاربران رایانه‌های شخصی‌ای که در ارتباط با شرکت مربوط قرار داشته‌اند، اطلاع می‌دهند تا اقدامات لازم را برای حفظ داده‌های شخصی خود به عمل آورند.

این مرکز هم‌چنین یک خط تلفنی راهنما به‌راه انداخته که به مشتریان خود در این زمینه کمک می‌کند. نتیجه‌ی نهایی فعالیت‌های

این مرکز در پائیز امسال منتشر می‌شود. با این حال،دیتر کرمپ از نتایج بررسی موقت این فعالیت‌ها راضی است. او می‌گوید: تا چندی پیش آلمان در صدر جدول کشورهایی قرار داشت که از حمله‌هایی به روش بات نتسه بیش از کشورهای دیگر زیان می‌دید. حالا مدت‌هاست که آلمان دیگر صدرنشین نیست.

•به‌کارگیری تجربه‌های دیگران
نمایندگان سیاست، اقتصاد و اداره‌ی جنایی آلمان، از این رو و با استفاده از این تجربه‌ها در صدد برآمده‌اند به‌طور هماهنگ با خلافکاران اینترنتی در زمینه‌های دیگر نیز مبارزه کنند. گشایش نهاد مرکز دفاع ملی در فضای مجازی در ماه ژوئن در شهر ُبن، گامی در این جهت است. این مرکز در گردآوری داده‌ها و پیاده‌کردن طرح‌های مبارزه با کلاهبرداران اینترنتی نقش اصلی را بازی می‌کند.

به نظر یورگ تسیرکه، گام بعدی باید در جهت تشکیل شبکه‌ای از نمایندگان شرکت‌های تلفن و ارتباطات، نهادهای بازرسی و تحقیق و نمایندگان اقتصاد برداشته شود. چندی پیش شبکه‌ی مشابهی برای مبارزه با خلافکارانی که با روش فیشینگ (Phishing) به شکار داده‌های کاربران می‌روند، نیز تشکیل شده است. این کلاهبردان اینترنتی می‌کوشند، با استفاده از پیچینگ، یعنی جعل آدرس‌های اینترنتی، پست الکتریکی یا ارسال پیامک با نام‌های مستعار، به داده‌های بانکی کاربران دست یابند.

یورگ تسیرکه امیدوار است با اعمال مجموعه‌ای از این روش‌های دفاعی، فضای مجازی را از وجود خطاکاران اینترنتی پاک کند.