روش جدید سارقان در برداشت غیر قانونی از دستگاههای خود پرداز

به موازات پیشرفت تکنولوژی و توسعه الکترونیکی در ابعاد مختلف، مجرمین نیز از این قاعده مستثنی نبوده و گاهی اوقات برخی قابلیت ها و فناوری پیشرفته الکترونیکی، در مسیر ارتکاب جرم از سوی مجرمین مورد سوءاستفاده قرار می گیرد. در متن حاضر که از سوی دبیرخانه مرکزی سازمان اینترپل دریافت و پس از ترجمه در قالب ویژه نامه اخیر تهیه شده است، یکی از جدیدترین شگردهای مورد استفاده مجرمین در زمینه سرقت اطلاعات و برداشت غیر قانونی پول از دستگاههای خودپرداز معرفی می شود که امیدواریم مورد توجه خوانندگان محترم قرار گیرد.

دبیرخانه مرکزی سازمان بین المللی پلیس جنایی (اینترپل) در ۲۳ مارس ۲۰۰۹ پیام هشداری را از دفتر ملی اداره بررسی اطلاعات جنایی مجارستان بخش OCB دریافت کرد. این پیام که منبع انتشار آن گروه بررسی امکان کلاهبرداری سیتی بانک (Citibank) روسیه است، از روش جدید سارقان در سرقت اطلاعات و برداشت غیر قانونی پول از دستگاه های خودپرداز پرده بر می دارد. این اطلاعات پس از آنکه توسط سیتی بانک در اختیار بانک OTP مجارستان قرار گرفت، به پلیس مجارستان ارجاع شد.

در متن اصلی این پیام فهرستی از دستگاههای خودپردازی که از این پدیده مخرب زیان دیده اند یافت می شود. تمامی این دستگاهها در ۳ کشور عضو یعنی تایلند، کرواسی و بلغارستان بوده اند. اما به نظر می رسد که این شیوه در تعداد زیادتری از کشورها به کار گرفته شده است.

در حالی که کمیته رسیدگی به جرایم مالی و پیشرفته پلیس بین الملل به دنبال تأییدیه و یا دریافت اطلاعات تکمیلی این کشورها در زمینه وجود چنین مشکلی است، اما ماهیت این ویروس به شکلی است که هشدار پیرامون آن بسیار لازم و ضروری می نماید.

در اینجا به منظور جلوگیری از هر گونه دخل و تصرف در متن، محتوای کامل نامه دریافتی سازمان اینترپل به شرح زیر ارایه می شود.

" تیم بررسی مقابله با کلاهبرداری سیتی بانک روسیه به تازگی با شیوه نوینی از کلاهبرداری برخـورد کـرده و معتقد است که به جز کشور اوکراین که با استفاده از این شیوه مورد استراق سمع تلفنی قرار گرفته هیچ کشور دیگری حتی نوع مشابه این موضوع را تجربه نکرده است"

این موضوع در مورد برداشت غیر قانونی پول و یا به شکل دقیق تر سرعت اطلاعات از دستگاه های خودپرداز ساخت شرکت دیبولد است که در این ماجرا افراد کلاهبردار با استفاده از ویروس های پیشرفته این دستگاه ها را مورد حمله قرار دادند.

این ویروس که کد مخربی را در دستگاه قرار می دهد باعث می شود نرم افـزار صـفحه کلیـد دسـتگاه هـای خود پرداز دیبولد از کد امنیتی رمزگشایی کرده و آن را به همراه داده های مربوطـه روی نـوار مغناطیـسی بـر روی سخت دیسک ذخیره نماید. سپس این افراد با استفاده از کارت تراشه مخصوص (کارت ویژه) به دسـتگاه آسیب دیده فرمان می دهند تا داده های خود از قبیل کد امنیتی (pin) را طبق روال دستگاه های خود پـرداز چاپ نماید.

طبق اطلاعات جمع آوری شده توسط بانک های زیان دیده محلی، ویروس در اغلـب مـوارد از طریـق کابـل USB و دقیقاً مانند زمانی که دستگاه با کلید استاندارد خود توسط متصدی باز مـی شـود، وارد دسـتگاه مـی شود که این مسأله به احتمال قریب به یقین همان علت ایجاد اختلال داخلی فرض می شود. در مـواردی نیـز مشاهده شده که سوراخی بر روی سطح دستگاه خودپرداز ایجاد شده اسـت. در تمـامی مـوارد سیـستم عامـل تمامی دستگاهها ویندوز XP بوده است.

بعلاوه طبق اخبار دریافتی از یکی از بانک های محلی در اواخر فوریه ۲۰۰۹ سارقان بـا ارتقـاء ویـروس و وارد کردن آن به یکی از دستگاههای خودپرداز شرکت دیبولد، تمام موجودی این دستگاه را تخلیـه کردنـد. پلـیس فعالانه برای شناسایی رمز این ویروس همکاری میکند. اولین نشانه های ارتکاب این جرم در سن پترزبورگ و مسکو دیده شده است. برخی از سارقان نیز در این ارتباط دستگیر شده اند. طبق گفته پلیس یک گروه تبهکـار با سازماندهی بسیار قوی پشت این ماجرا قرار دارند و در حال حاضر به سختی می توان گفت که افراد دستگیر شده بتوانند پلیس را به سران این باند برسانند.

این تیم متعاقبا" در نشستی با حضور بانک های زیان دیده از این ویروس پیشرفته و نمایندگان شرکت دیبولـد حضور یافت . در این نشست مشخص شد که تعداد بانک های محلی زیـان دیـده ۸ مـورد و تعـداد رخنـه بـه

دستگاه به ۲۴ مورد رسیده است. شرکت دیبولد ضمن تایید آسیب پذیر بودن نرم افزار خود اعلام داشت که پیچ هایی (بسته های ترمیمی جهت رفع نقص) را به همراه برنامه ضد ویروس (Antivirus) در دستگاههای خود نصب کرده است. اما این مشکل با به روز شدن ویروس، دوباره به قوت خود باقی خواهد بود. شرکت دبی متعهد شد که ضمن ادامه تحقیقات در کوتاه ترین زمان راه حل مناسب را رایه می دهد.

در حال حاضر شواهدی مبنی بر آسیب پذیری مشابه سایر مدل های دستگاه های خودپرداز وجود ندارد. اما می توان با بررسی اطلاعات NCR به موارد مشابهی که توسط این ویروس ایجاد شده پی برد. از آنجا که این پدیده به مشکلی جدی برای بازار روسیه تبدیل شده و با توجه به هدایت این ماجرا توسط یک گروه تبهکار کاملاً حرفه ای در حیطه درون و برون مرزی، لزوم تسریع در اعلام این هشدار و نیز توجه تمامی مشاغل به این مسأله امری بسیار ضروری محسوب می شود. همچنین لزوم بازنگری کامل و دقیق روی سیستم امنیتی ماشین های خودپرداز به خصوص خودپردازهای ساخت شرکت دیبولد بشدت احساس می شود. در حال حاضر مشخصات این ویروس در اختیار پلیس قرار دارد و تلاشهای انجام شده در جهت دستیابی به رمز آن تا کنون بی نتیجه مانده است. زیرا در اختیار داشتن این رمز به گروههای مختلفی که مشغول آزمایش و بررسی این ویروس هستند، کمک زیادی خواهد نمود. ما بر این باوریم که این مسأله با توجه به تجربه ما، از حساسیت بالایی برخوردار بوده و به سرعت می تواند به غرب اروپا و ایالات متحده تسری یابد.

در اینجا نکاتی را که می توان در این ارتباط به کار بست به شرح ذیل اعلام می داریم:

۱- تجهیز دستگاه های خودپرداز به حسگر جهت تشخیص هر گونه ورود غیر قانونی خارجی و اعلام خطر سریع، بانک و خاموش کردن دستگاه و در نهایت اعزام مهندسین به محل جهت انجام بازرسی های لازم.

۲- صفحه کلید باید رمز امنیتی(pin code) را بطور رمزی درج کرده و امکان ظهور آشکار آن را فراهم نکند.

در این حالت تمامی داده ها از ابتدا تا انتها باید به صو.رت رمزدر آیند.

۳- خریداران، توزیع کنندگان و سازندگان دستگاههای خودپرداز باید به دقت مراقب هر گونه خط احتمالی بوده و به طور مداوم نرم افزارهای ضد ویروس نصب شده بر روی دستگاه ها را ارتقاء دهند.