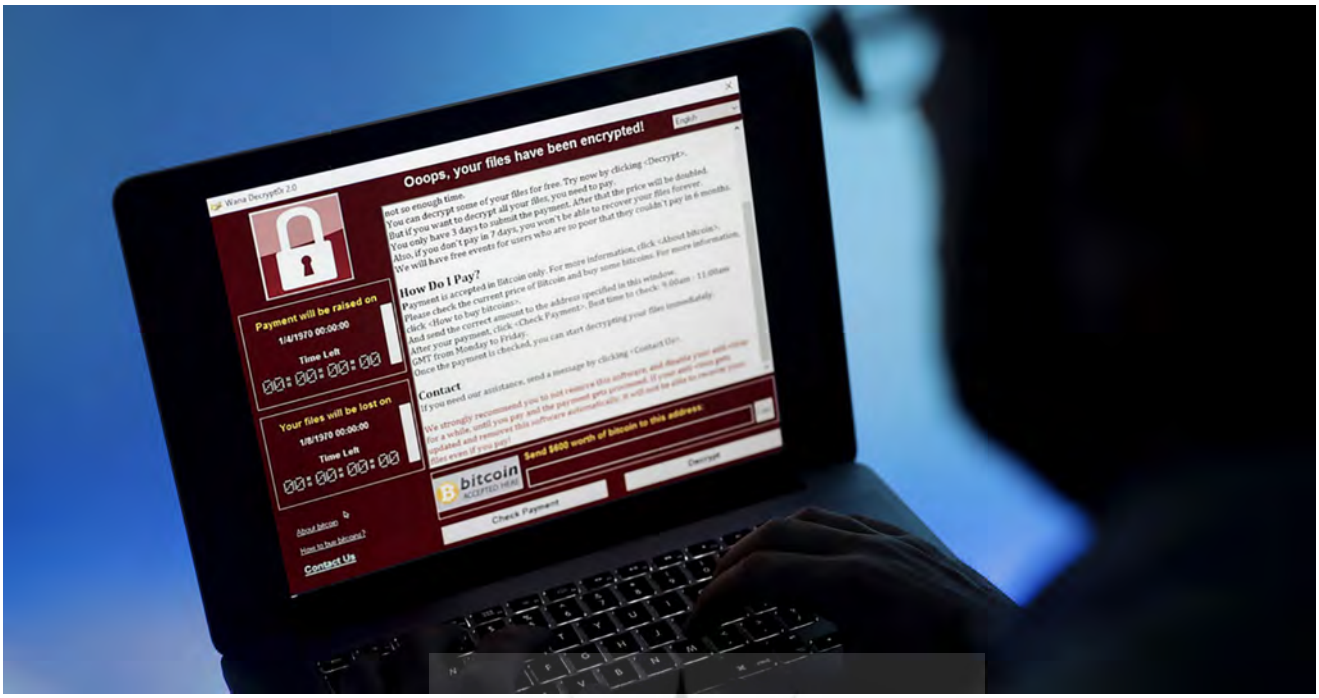

باج‌افزارها؛ ابزاری نوین در دستان مجرمین

■ تحقیق و ترجمه: فهیمه فره وشی

... در نیمه دوم اردیبهشت ۱۳۹۶، بر اساس اعلام سازمان فناوری اطلاعات، حمله باج‌افزار WannaCry بیش از دو هزار قربانی در ایران گرفته است. بر این اساس بیشترین آلودگی از طریق این باج‌افزار متعلق به اپراتورهای ارتباطی، سلامت و پزشکی و دانشگاهی بوده است. مرکز ماهر استان‌های تهران و اصفهان را دارای بیشترین آلودگی اعلام کرده است. تا اینجا این باج‌افزار بیشتر چهره بزه بودن به تهدید می‌دهد ولی گستره این تهدید در ایران در مقایسه با دیگر کشورها کم بوده؛ چرا که در یورش ۲۲ اردیبهشت، باج‌افزار WannaCry بسیاری از رایانه‌ها در جهان را قفل کرد و مانع از دسترسی کاربران به اطلاعات شد.

ایـــن بدافـــزار با نمایـــش پیامـــی روی صفحه کامپیوتر درخواســـت پـــول دیجیتال رمزگذاری شده(بیتکوین) کرد. این حمله حدود ۱۵۰ کشور جهان از جمله بریتانیا، روســـیه، فرانسه و اسپانیا را هدف قرار داد. یوروپـــل، پلیس اتحادیه اروپا، ضمن هشدار نسبت به «تهدید فزاینده» سایبری (۱۴ می/ ۲۴ اردیبهشـــت) اعلام کرد که شـــمار قربانیان حمله سایبری به ۲۰۰ هزار رسیده است. این حمله ویروسی از یک حفره امنیتی در یکی از نسخه‌های ویندوز مایکروسافت استفاده کرده است و...

طبق آخرین اطلاعـــات، در حال حاضر باج‌افزار ghost فعال است و هدف حملات این باج‌افزار عمدتاً کاربران انگلیسی زبان هستند.

باج‌افزار (Ransomware) نوعی بدافزار اســـت که از طریق ایجاد مانع یا محدودیت در دسترسی کاربران به سیســـتم‌های کامپیوتری شـــان عمل می‌نماید. این ممانعت گاه از طریق قفل کردن کل کامپیوتر و گاه با قفل کردن برخی داده‌های خاص انجام می‌گیرد تا زمانی که در ازای پرداخت وجه خواسته شده به باج خواه قفل گشوده شود.

باج‌افزارهای امروزی نســـبت به نسخه‌ی اولیه‌ی خود به نام ایدز تروژان (AIDS Trojan) در سال ۱۹۸۹ پیشرفت قابل توجهی داشته اند. علی رغم عدم آمادگی مردم برای مواجهه با این نوع جدید از تهدید، تروژان ایدز به دلیل برخی از عوامل شکست خـــورد. در آن زمان افراد کمـــی از کامپیوترهای خانگی استفاده می‌کردند، وب جهانی تنها در حد یک ایده بود و بیشترین استفاده از اینترنت توسط کارشناســـان در حوزه‌های دانش و فناوری بود. به علاوه، پروســـه‌ی پرداخت‌های بین المللی بسیار دشوارتر از فرآیند کنونی آن بود و کمتر مبتنی بر فرایندهای رایانه ای و الکترونیکی بود.

از ســـال ۱۹۸۹ تـــا کنون، تحـــولات باج‌افزارها تا حدود زیـــادی تحت تأثیر طیف وســـیعی از تغییرات در زمینه‌های فناوری، اقتصاد، و امنیت بوده است.

باج‌افزارهای امروزی، تهدیدهای بسیار پیچیده‌ای هســـتند که می‌توانند زندگی کاربران در اقصی نقاط جهان، خصوصاً آن دســـته از کاربرانی که در کشـــورهای توســـعه یافتـــه و دارای فناوری پیشرفته هستند، را تحت تأثیر قرار دهند. دنیای باج‌افزارها بسیار شـــبیه یک اکوسیستم زندگی واقعی اســـت. باج‌افزارهایی کـــه توانایی تغییر و تطبیق خود با شـــرایط را دارنـــد باقی می‌مانند، در حالی که ســـایرین که نمـــی توانند خود را با شرایط تطبیق دهند، از صحنه‌ی فناوری حذف می‌شوند.

در سال گذشته، باج‌افزار واناکرای (WannaCry) توانســـت بیش از یک چهارم میلیون سیستم در سراســـر جهان را آلوده کرده و رمزگذاری نماید. این بدافزار از روش رمزگذاری نامتقارن اســـتفاده می‌کرد؛ در این روش بـــه لحاظ منطقی، قربانی قـــادر بـــه بازیابی کلیـــد لازم برای رمزگشـــایی

فایل‌های رمزگذاری شـده نمی باشد. پس از آن، برای مقابله با این بدافزار، یک ابزار رمزگشایی به نام واناکی (WannaKey) طراحی شد که قادر به بازیابی کلید رمزگذاری شده بود.

انواع باج‌افزارها

باج‌افـزار قفل‌کننـده (قفل‌کننـده‌ی کامپیوتر)

باج‌افزار قفل کننده این گونه طراحی شـده است که دسترسـی به منابع کامپیوتر را مسدود کند. این باج‌افزار نوعاً از طریق قفل کردن رابط کاربری کامپیوتـر و مطالبه‌ی وجهـی از کاربر جهت باز کردن دسترسـی وی عمل می‌نماید. قابلیت‌های کامپیوتر قفل شده اغلب به مواردی نظیر ارتباط کاربر با باج‌افزار و پرداخت وجوه خواسـته شده محدود می‌شود. این محدودیت‌ها به حدی است که حتی ممکن است ماوس را هم غیرفعال نموده و عملکرد صفحه کلید کامپیوتر را به اعداد موجود روی آن جهت تایپ شماره حساب و رمز پرداخت اینترنتی محدود کند.

باج‌افزار قفل کننده معمولاً به منظور قطع رابط کاربری طراحی می‌شـود و به سیسـتم عامل و فایل‌های کامپیوتر آسـیبی وارد نمی کند. این بدان معنا است که به طور بالقوه با حذف بدافزار از روی سیستم کامپیوتر می‌توان آن را به چیزی نزدیک بـه حالت اولیه‌ی خـود بازگرداند. این ویژگی موجب می‌شـود که این نوع از باج‌افزار در مقایسـه با نوع مخرب تر خود یعنی باج‌افزار رمزنـگار، در اخذ وجوه اخاذی شـده از کارایی کمتری برخوردار باشد.

باج‌افزار رمزنگار (قفل کننده‌ی داده‌ها)

این نوع از باج‌افزارها بـرای یافتن و رمزگذاری داده‌های ارزشمند ذخیره شده بر روی کامپیوتر، و تبدیل آن‌ها به داده‌های غیرقابل اسـتفاده تا زمان دریافت کلید رمزگشـایی توسـط کاربر، طراحی می‌شود. هم چنان که زندگی مردم روز به روز به سـمت دیجیتالی شدن پیش می‌رود، اطلاعات مهم بیشـتری توسـط آنهـا بر روی کامپیوترهای شـخصی و دستگاه‌های دیجیتال ایشـان ذخیره می‌شـود. بسـیاری از کاربران نمی‌دانند که به منظور محافظت از اطلاعات در برابر خطراتی مانند سـوختن هارد دیسک، از دست دادن اطلاعات و یا دزدیده شدن کامپیوتر خود، بـدون در نظـر گرفتن خطـر احتمالی حمله‌ی باج‌افزارهای رمزنگار، لازم اسـت که از فایل‌های خود نسخه‌ی پشتیبان تهیه کنند. این امر ممکن است ناشی از عدم داشتن دانش کافی کاربـران در این زمینه و یـا عدم درک اهمیت داده‌های موجود باشـد. فراهم آوردن مقدمات فرآیند تهیه‌ی نسـخه‌ی پشتیبان نیازمند انجام برخی کارها و رعایت بعضی ضوابط می‌باشد که از حوصله‌ی کاربران معمولی خارج است.

باج‌افـزار رمزنـگار از این ضعف‌هـای امنیتی کاربـران معمولی برای اهداف اخاذی اسـتفاده می‌کنـد. طراحان این باج‌افزارهـا می‌دانند که داده‌های ذخیره شـده بـر روی کامپیوترهای شـخصی احتمالاً برای کاربران این کامپیوترها حائز اهمیت اسـت. بـه عنوان مثـال، داده‌ها می‌تواند شامل عکس‌ها و خاطرات شخصی فرد کاربر، یک پروژه‌ی دانشگاهی در انتظار تأیید و یا یک گزارش مالی مربوط به محل کار باشـد. قربانیان باج‌افزارها ممکن است به سبب ناامیدی از بازگرداندن اطلاعاتشان ترجیح دهند که وجه مطالبه شـده را پرداخت کننـد تا این که برای همیشـه آن اطلاعـات را از دسـت بدهند و یا عواقب آن دامن گیرشان شود.

یـک باج‌افزار رمزنگار عادی، پـس از نصب اقدام به جسـتجوی فایل‌ها و رمزگذاری آن‌ها می‌کند. طراحـی باج‌افزار به گونه‌ای اسـت کـه تا زمان یافتن تمامـی فایل‌هایی که ممکن اسـت برای کاربر ارزشمند باشد، مخفی بماند و قربانی زمانی از موضـوع اطلاع می‌یابد که پیام بدافزار مبنی بر رمزگذاری داده‌ها را دریافت می‌کند. در بسیاری از موارد حمله‌ی باج‌افزار، کامپیوتر به طور عادی کار می‌کند زیرا هدف بدافزار تخریب عملکرد کامپیوتر نیست. بدین معنا که کاربر کمافی السابق امکان کار بـا کامپیوتر را دارد و تنها دسترسـی وی به فایل‌های رمزگذاری شده مسدود می‌شود.

شـاید اولین نمونه از حمله‌ی گسـترده‌ی یک باج‌افزار کـه رمزگذاری یک کلیـد عمومی در اینترنت را هـدف قرار گرفته بود توسـط یک ویروس تروژان (Trojan horse) در فاصله‌ی زمانی سـپتامبر تا ماه می سـال ۲۰۱۳ اتفاق افتاد. بدافزار مطالبه‌ی وجه در قالب بیت کوین را کرده بود و متخصصان بر این عقیده بودند که روش رمزگذاری به شکلی بود که پس از اجرای کامل، برنامه را کاملاً غیرقابل نفوذ کرده بود. در هر صورت، در ماه می ۲۰۱۴ یک شرکت امنیتی توانست با حمله به سرور فرمان و کنترل بدافزار، دسترسی به کلید رمزگذاری آن را بازیابی نماید. بـه منظور دفاع در برابر حملـه‌ی باج‌افزار، یک ابزار آنلاین که بـه طور رایگان کلید رمزگذاری را بازیابی می‌کرد در اختیار کاربران قرار گرفت.

قوانین مقابله با بدافزارها

به موجب قانـون جدید حفاظـت از داده‌های اتحادیـه‌ی اروپا که از ماه مـی ۲۰۱۸ به اجرا درآمده اسـت، به محض آگاه شدن از به سرقت رفتن اطلاعات بایسـتی مراتب بدون فوت وقت (ظرف ۷۲ سـاعت) به اطلاع مسئولان نظارتی برسـد مگر در شـرایطی که خطری اشـخاص مرتبـط با موضوع را تهدید نماید. واضح اسـت که اکثر مواقع ارزیابی خطر احتمالی یا بالقوه‌ای که اشـخاص را تهدید می‌کند در مراحل اولیه دشـوار می‌باشـد. جریمه‌های مربوط به نقض این مقررات قابل توجه است، فلذا برای هرگونه تأخیر در اطلاع به مقامات مسـئول باید دلایل موجهی وجود داشته باشد.

در ماه می ۲۰۱۸، یک شـرکت انگلیسـی به نام PML با مراجعه به دادگاه ادعا نمود که توسـط یک فرد ناشناس مورد اخاذی اینترنتی قرار گرفته است و شـخص هکر اطلاعات به سرقت رفته را روی یک وب سـایت قرار داده و برای دسترسی به آن اطلاعات شناسه کاربری و رمز عبور تعیین نموده و تهدید کرده است چنانچه شرکت ظرف دو هفته مبلغ سـیصد هزار پوند به وی پرداخت نکنـد، آن اطلاعات را بر روی وب سـایت مزبور منتشـر خواهد کرد. دادگاه در قدم اول، دستور داد تا اطلاعات وب سـایت حـاوی داده‌های به سرقت رفته مورد بررسـی قرار گیرد. پس از آن که مشخص شد که هاست (میزبانی) وب سایت مزبور در یکی از کشـورهای اروپایـی قرار دارد، شـرکت PML از دادگاه آن کشـور خواست تا قراری جهت توقف فعالیت وب سـایت مورد نظر صادر نماید. شـخص هکر پس از آن اقدام به قرار دادن اطلاعات به صورت خرد بر روی سایت‌های مختلف نمـود و در ازای بازگرداندن اطلاعات به شرکت، مبلغ مورد مطالبه‌ی خود را به صد هزار پوند کاهش داد. پس از آن که دادگاه به این وب سایت‌ها اخطار نمود که در صورت ادامه‌ی انتشار این اطلاعات از فعالیـت آن‌ها جلوگیری خواهد شـد، وب سـایت‌های مزبور اقدام به حذف آن اطلاعـات از روی صفحات خود نمودند و پس از آن اقـدام دیگری از جانب فرد هکر برای ادامه‌ی اخاذی مشاهده نشد و پرونده مختومه گردید هر چند شـرکت تجاری ضررهای جدی را متحمل گردید که ناشی از انتشار اطلاعات مالی و تجاری شرکت بود.

منابع:

Levinec.(2018,August17).Ransomware. Retrieved from Microsoft: www.microsoft.com

Murphy, R. (2017, May 12). How Does Ransomware Work? Retrieved from Carbonblack: www.carbonblack.com

Lau, K. S. (2015, August 6). The evolution of ransomware. Retrieved from Symantec: www.symantec.com