
SHABAKEH [NETWORK]
شبکه
۱۴۸
خرداد
۱۳۹۲

## الفبای امنیت در وب

بخش دوم

# زمانی برای مستی بدافزارها

» نویسنده: جان برودکین
» منبع: آرس تکنیکا
» ترجمه: احمد شریف‌پور


**برخی می‌گویند که ما در دوران پسا پی‌سی (Post-PC) زندگی می‌کنیم، اما بدافزارهای پی‌سی‌ها هنوز هم یکی از بزرگ‌ترین مشکلات کاربران خانگی و تجاری کامپیوترها است.**

**نمونه‌های این موضوع را در همه‌جا می‌توان مشاهده کرد؛ در ماه نوامبر اعلام شد که هکرها از یک بدافزار برای سرقت اطلاعات مربوط به موشک‌های جدید ژاپن و انتقال آن به سیستم‌های خودشان استفاده کرده‌اند. به‌تازگی مشخص شد که دو سیستم حیاتی از دو نیروگاه برق ایالات‌متحده به بدافزارهایی که از طریق حافظه فلش منتقل می‌شوند، آلوده شده‌اند. بدافزار Dexter اطلاعات کارت‌های اعتباری را از POSهای تجاری سرقت می‌کرد و در نهایت بدافزارهایی که هدف‌های جاسوسی را دنبال می‌کنند، روزبه‌روز پیچیده‌تر و خلاقانه‌تر طراحی می‌شوند.**

**در دومین بخش این مجموعه مقاله، مبانی امنیت سیستم‌های کامپیوتری را برای کسانی که با انواع مختلف بدافزارها آشنا نیستند، توضیح می‌دهیم.**

بدافزارها شکل‌های مختلفی دارند که از میان آن‌ها می‌توان به ویروس‌ها، کرم‌ها و تروجان‌ها اشاره کرد.

ویروس‌ها برنامه‌هایی هستند که خودشان را تکثیر می‌کنند تا بتوانند از کامپیوتری به کامپیوتر دیگر راه پیدا کنند و در هر یک از این کامپیوترها، داده‌ها را پاک کرده یا به سرقت می‌برند. این بدافزارها می‌توانند رفتار کامپیوترها را به شکل‌های متفاوتی تغییر دهند.

سیسکو این‌گونه توضیح می‌دهد: «تقریباً تمام ویروس‌ها به یک فایل اجرایی چسبیده‌اند. به همین دلیل ویروس‌ها ممکن است روی یک سیستم وجود داشته باشند اما تا زمانی که کاربری فایل میزبان آلوده را باز یا اجرا نکند غیرفعال باقی می‌مانند. زمانی که کد میزبان اجرا شد، کد آلوده نیز اجرا می‌شود. به‌صورت معمول فایل میزبان پس از آلوده شدن هم به‌صورت معمولی کار خواهد کرد. البته، برخی از ویروس‌ها یک کپی از خودشان را جایگزین برنامه‌های مختلف می‌کنند و به این ترتیب، آن‌ها را نابود می‌کنند. زمانی که برنامه‌ها یا اسناد آلوده به ویروس از طریق شبکه، دیسک، اشتراک فایل یا ایمیل از یک کامپیوتر به کامپیوتر دیگری منتقل شوند، ویروس هم به همراه آن‌ها منتشر می‌شود.»

کرم‌ها درست شبیه ویروس‌ها هستند، چراکه آن‌ها هم مانند ویروس‌ها برای انتشار بیشتر خودشان را تکثیر می‌کنند. از دید سیسکو بارزترین تفاوت‌های میان ویروس‌ها و کرم‌ها این‌ها هستند: «کرم‌ها کم‌وبیش مستقل از سایر فایل‌ها عمل می‌کنند اما ویروس‌ها برای منتشر شدن به فایل‌های میزبان نیاز دارند.» کرم‌ها به‌سادگی منتشر شده و نه تنها به کامپیوترهای منفرد که به کل شبکه کامپیوتری آسیب می‌رسانند. یکی از مخرب‌ترین کرم‌هایی که تاکنون در اینترنت منتشر شده است، Slammer نام داشته است که به‌تازگی دهمین سال انتشارش را پشت سر گذاشته‌ایم.

تروجان‌ها برخلاف ویروس‌ها و کرم‌ها، خودشان را تکثیر نمی‌کنند. نام آن‌ها براساس داستان باستانی اسب تروا انتخاب شده است چراکه


**شکل ۱** ایمیل آلوده که کاملاً قانونی و معتبر به‌نظر می‌رسد.

درست مانند اسب چوبین تروا، آن‌ها خود را نرم‌افزارهایی قانونی و بی‌آزار معرفی می‌کنند تا کاربران را برای نصب قانع کنند. سیسکو درمورد آن‌ها می‌نویسد: «تروجان‌ها بعد از فعال‌شدن می‌توانند به هرنوع حمله‌ای روی ماشین میزبان دست بزنند. از اذیت کردن کاربر با نشان دادن تبلیغات و پیام‌های ناخواسته یا عوض کردن تصویر پس‌زمینه دسکتاپ گرفته تا آسیب زدن به سیستم میزبان با پاک کردن فایل‌ها و دزدیدن اطلاعات یا فعال کردن و انتشار بدافزارهایی نظیر ویروس‌ها. همچنین تروجان‌ها به ایجاد درهای پشتی مشهور هستند. این درهای پشتی امکان نفوذ به سیستم را برای کاربران غیرمجاز و خرابکار فراهم می‌کنند.»

برخی از انواع حمله‌ها که تهدیدهای ترکیبی یا Blended Threats نامیده می‌شوند، خصوصیات ویروس‌ها، کرم‌ها و تروجان‌ها را با هم ترکیب می‌کنند و به این ترتیب بهتر گسترش می‌یابند و دفاع در برابر آن‌ها سخت‌تر می‌شود.

بدافزارها را علاوه‌بر ویروس‌ها، کرم‌ها و تروجان‌ها می‌توان به زیرگروه‌های دیگری مانند درهای پشتی، تروجان‌های دسترسی از راه دور، سارقان اطلاعات و باج‌افزار (Ransomware) نیز تقسیم کرد. کریستوفر الیسان (Christopher Elisan) متخصص امور امنیتی در کتابش با نام «بدافزار، روت‌کیت و بات‌نت: راهنمایی برای مبتدیان» تمام این گونه‌های مختلف را تشریح کرده است. آن‌چه در ادامه می‌خوانید خلاصه قسمت‌های مختلف این کتاب است.

## درهای پشتی

همان‌طور که از نام این بدافزارها مشخص است، درهای پشتی امکان سرک‌کشیدن به سیستم آلوده را برای هکرها فراهم می‌کنند. به‌گفته الیسان آن‌ها این کار را با دور زدن تمهیدات امنیتی از طریق «ویژگی‌ها و قابلیت‌های مستند نشده شبکه یا سیستم‌عامل انجام» می‌دهند. به‌عنوان نمونه در سال ۲۰۱۱ برای هک سیستم‌های RSA از یک درپشتی استفاده شد. این حمله یک حمله هدف‌دار بود و از طریق ارسال ایمیل‌های فیشینگ (که به‌ظاهر بی‌خطر به‌نظر می‌رسیدند) به کارکنان شبکه RSA انجام شد و هکرها توانستند جای پای خود را در سیستم محکم کنند. در عنوان این ایمیل‌ها عبارت «برنامه استخدام سال ۲۰۱۱» به چشم می‌خورد و خود ایمیل حاوی یک فایل اکسل بود. در این فایل اکسل یک فایل فلش ادوبی جاسازی شده بود که درپشتی مورد نظر را نصب می‌کرد (شکل۱).

باز کردن فایل پیوست شده در آوت‌لوک باعث می‌شد که فایل فلش موجود در آن توسط اکسل اجرا شود. با هدف گرفتن یک نفوذپذیری که امکان اجرای کد را فراهم می‌کرد، شیء فلش ادوبی یک در پشتی از نوعی که «پیچک سمی» یا Poison Ivy نامیده می‌شود را روی کامپیوترهای RSA نصب می‌کرد. این پیچک سمی پس از نصب به سرورهایی که هکرها کنترل آن را دراختیار داشتند، متصل می‌شد. شرکت امنیتی F-Secure در سال ۲۰۱۱ نوشت: «زمانی که این اتصال برقرار می‌شد، حمله‌کننده می‌توانست از راه دور کنترل سیستم آلوده را به‌صورت کامل دراختیار بگیرد. بدتر این‌که می‌توانست به کل درایوهای شبکه که کاربران دسترسی داشتند نیز دسترسی پیدا کند.»

## تروجان‌های دسترسی از راه دور

الیسان می‌نویسد: «یک تروجان دسترسی از راه دور یا RAT (سرنام Remote Access Trojan) یک ابزار مدیریتی آلوده است که قابلیت‌هایی شبیه درهای پشتی دارد و اجازه دسترسی به سیستم آلوده آن هم با سطح دسترسی مدیر سیستم (Admin) را برای هکر فراهم می‌کند. تفاوت اصلی میان RAT و یک در پشتی معمولی در این است که RAT یک رابط کاربری دارد. یک کلاینت که حمله‌کننده به کمک آن می‌تواند دستوراتی را به بخش سرور که روی ماشین آلوده قرار دارد، ارسال کند.

RATها می‌توانند هزاران کامپیوتر آلوده را کنترل کرده و امکان انجام تقریباً هر کاری را برای حمله‌کنندگان فراهم می‌کنند. حمله‌کنندگان می‌توانند برنامه‌هایی را روی سیستم آلوده نصب کنند، اطلاعات آن را بدزدند یا کل آن را از کار بیاندازند.

**برخی از انواع حمله‌ها که تهدیدهای ترکیبی یا Blended Threats نامیده می‌شوند، خصوصیات ویروس‌ها، کرم‌ها و تروجان‌ها را با هم ترکیب می‌کنند و به این ترتیب بهتر گسترش می‌یابند و دفاع در برابر آن‌ها سخت‌تر می‌شود.**

## سارقان اطلاعات

با عمیق‌تر شدن در بدافزارهایی که برای سرقت اطلاعات طراحی شده‌اند، الیسان ثبت‌کننده‌های ضربه کلید یا Keylogger، ضبط‌کننده‌های دسکتاپ یا Desktop recorder و نفوذکننده‌های حافظه یا Memory scraper را تشریح کرده و توضیح می‌دهد که این بدافزارها می‌توانند گذرواژه‌ها، اطلاعات مالی، داده‌های خصوصی «یا هر چیزی که نفع یا پولی برای هکرها به همراه داشته باشد» را به سرقت ببرند.

یک ثبت‌کننده ضربه‌کلید، کلیدهایی که کاربر می‌فشارد را ثبت کرده و «آن‌ها را به‌صورت محلی ذخیره می‌کند تا بعدها مورد استفاده قرار گیرند، یا آن‌ها را به سرور راه دوری ارسال می‌کند که در دسترس هکر قرار دارد.» ضبط کننده‌های دسکتاپ به‌صورت منظم از صفحه نمایشگر کاربر عکس می‌گیرند و نفوذکننده‌های حافظه اطلاعات در حال پردازش را از حافظه کامپیوتر استخراج می‌کنند. الیسان می‌نویسد: «داده‌های در حال پردازش در حافظه کامپیوتر رمزنگاری نشده‌اند. به همین دلیل، حافظه سیستم، بهترین محل برای دزدیدن اطلاعات است.»

ثبت‌کننده‌های ضربه‌کلید ممکن است برای مقاصد کاملاً قانونی مورد استفاده قرار بگیرند. حتی برخی از شرکت‌ها نرم‌افزارهایی را برای ردگیری فعالیت‌های اعضای خانواده به فروش می‌رسانند. این کار ممکن است برای والدینی که می‌خواهند فعالیت‌های اینترنتی فرزندان‌شان را زیر نظر بگیرند، ایده جالبی به‌نظر برسد.

## باج‌افزار

این نمونه از برنامه‌های آلوده، به‌صورت معمول کامپیوتر را به گروگان می‌گیرند تا زمانی که کاربر باج مورد نظر خرابکاران را پرداخت کند. این بدافزار ممکن است داده‌های کاربر را برای جلوگیری از دسترسی او، به رمز درآورد. الیسان می‌نویسد: «برای بازپس گرفتن دسترسی به داده‌هایش کاربر باید باجی را به خرابکاران بپردازد تا بدافزار داده‌هایش را از حالت رمزنگاری خارج کند یا خرابکاران راهی برای بازپس‌گیری داده‌ها دراختیار او قرار دهند. البته، بسیار هم پیش می‌آید که خرابکاران پول را دریافت کنند و به داده‌های کاربر و بقیه قضایا هیچ کاری نداشته باشد. به این ترتیب کاربر هم داده‌ها و هم پولش را از دست خواهد داد.»

همین نتیجه ممکن است با از بین بردن دسترسی کاربر به سیستم یا تهدید او به انهدام سیستم با یک تروجان نیز به دست آید(شکل۲).

باج‌افزار نتیجه سنتی دیرینه است که طی آن ویروس‌هایی با نمایش وقت و بی‌وقت تبلیغات ضدویروس‌های تقلبی و دروغین کاربران را بمباران می‌کردند. شرکت امنیتی ترند مایکرو در گزارش امنیتی سال ۲۰۱۲ خود نوشته است: «باج‌افزار ممکن است نواده بدافزارهای قدیمی فرض شود که ضدویروس‌های تقلبی را تبلیغ می‌کردند. هر دوی این تهدیدات باعث می‌شوند که کاربر درباره چیزی (مثلاً از دست دادن داده‌های حیاتی یا دانلود فایل‌های آلوده) نگران شود. پس از نگران کردن کاربر این بدافزارها از او می‌خواهند تا با پرداخت پول مشکلش را برطرف کند.»


شکل ۲ نمونه‌ای از پیغام‌هایی که در یک کامپیوتر آلوده به باج‌افزار به نمایش در خواهد آمد.

## گسترش بدافزارها

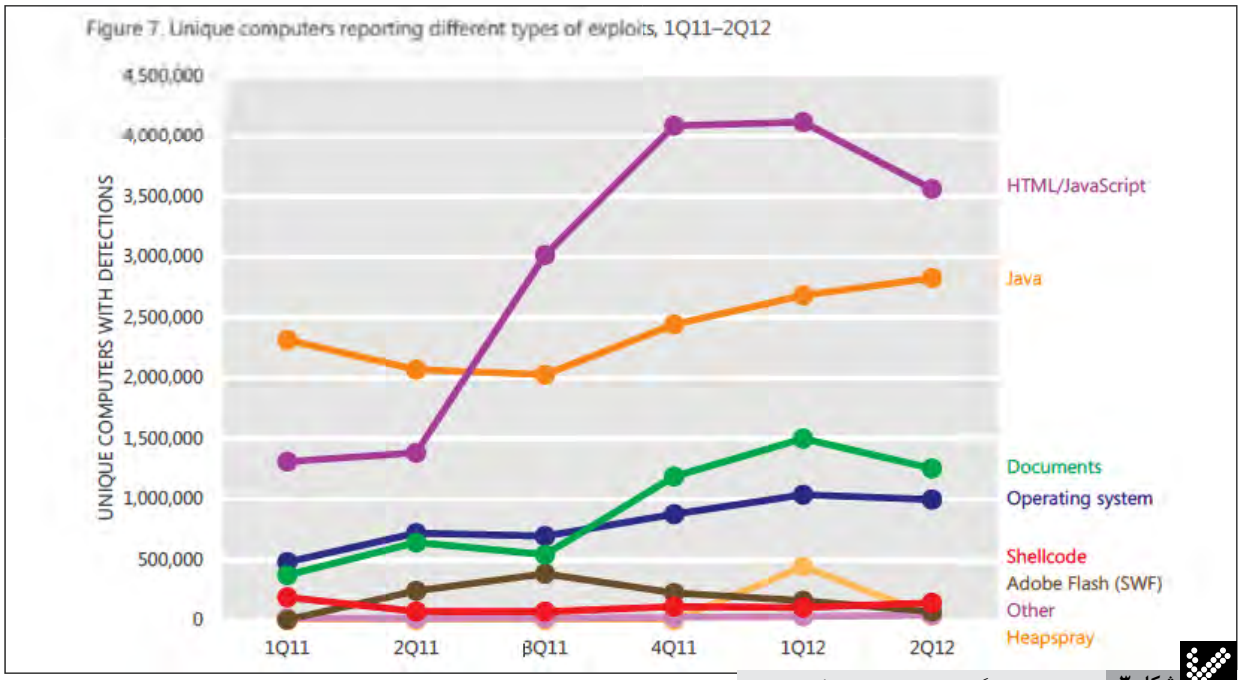
بدافزارها همیشه توسط کاربر قابل تشخیص نیستند. در واقع بهترین بدافزارها را به هیچ عنوان نمی‌توان بدون کمک گرفتن از برنامه‌های اسکن پیشرفته یا نرم‌افزارهای خاص کشف کرد. علائمی که در ادامه معرفی خواهیم کرد، می‌توانند نشانه آلودگی کامپیوتر به بدافزار باشند.

نخستین مورد تعداد زیاد پیام‌های به‌اصطلاح popup است. به‌خصوص آن‌هایی که نرم‌افزارهای ضدویروس را تبلیغ می‌کنند (این ضدویروس‌ها تقلبی هستند). دومین نشانه رفتار غیرطبیعی مرورگرهای اینترنت است؛ مثلاً صفحاتی که نمی‌توان آن‌ها را بست. صفحه خانگی یا موتور جست‌وجوی مرورگر اینترنت خود به خود عوض می‌شود یا نوارابزارهایی خود به خود نصب می‌شوند. نشانه دیگر برنامه‌هایی هستند که بدون هیچ دلیل خاصی اجرا می‌شوند.

قفل شدن سیستم برای مدت زمان طولانی یا کند شدن ناگهانی و غیرطبیعی آن می‌تواند یکی دیگر از نشانه‌های آلودگی سیستم باشد. تغییر یا پاک شدن فایل‌ها و پوشه‌ها هم نشانه دیگر آلودگی است. علاوه‌بر این موارد، می‌توان به دریافت حجم عظیمی از پیغام‌های خطای سیستمی نیز اشاره کرد. همچنین برنامه دیواره آتش ممکن است هشدارهایی را در مورد برنامه‌هایی که کاربر نمی‌شناسد، به نمایش درآورد.

بدافزارها انواع مختلفی از آسیب‌پذیری‌ها را در برنامه‌های مختلف یا خود سیستم‌عامل مورد استفاده قرار می‌دهند، اما به‌صورت معمول بیشتر از طریق مرورگرها منتشر می‌شوند. نمودار شماره ۱ که در گزارش بخش امنیتی مایکروسافت منتشر شده است نشان می‌دهد که HTML و جاوا اسکریپت (زبان نشانه‌گذاری و برنامه‌نویسی که قسمت اعظم وب را تشکیل می‌دهند) اصلی‌ترین روش آلوده شدن سیستم‌های کامپیوتری هستند. رتبه دوم به جاوا تعلق دارد که به‌واسطه نصب انواع پلاگین‌ها مورد هجوم حجم عظیمی از حمله‌ها در مرورگرهای مختلف قرار گرفته است(شکل۳).

بدافزارها می‌توانند تقریباً بدون نیاز به انجام هیچ عملی از سوی کاربر، سیستم‌های کامپیوتری را آلوده کنند. به‌عنوان مثال، تنها بازدید از سایتی (حتی رسمی و قانونی) که توسط یک هکر الوده شده باشد می‌تواند برای آلوده کردن سیستم کاربر کافی باشد. حمله‌هایی که به اصطلاح Drive-by download نامیده می‌شوند نیز، با رفتن کاربر به




**شکل ۳** شماره سیزدهم گزارش بخش امنیتی مایکروسافت

صفحات وبی که از نفوذپذیری‌های مرورگر یا پلاگین‌های آن استفاده می‌کنند، باعث آلوده شدن سیستم‌ها می‌شوند. تولیدکنندگان نرم‌افزارها به صورت معمول حدود یک هفته تا یک ماه پس از آشکار شدن یک نفوذپذیری، وصله‌های امنیتی را عرضه می‌کنند که این آسیب‌پذیری‌ها را برطرف می‌کنند. همین امر باعث به‌وجود آمدن یک بازی موش و گربه میان توسعه‌دهندگان نرم‌افزارهای سالم و خرابکاران شده است. البته، هنوز هم بسیاری از بدافزار برای ایجاد آلودگی و گسترش به‌نوعی به انجام عملی از سوی کاربر (مثلاً باز کردن پیوست یک ایمیل یا دانلود فایلی آلوده از طریق اینترنت) وابسته هستند.

امنیت سیستم‌عامل ویندوز در نسخه‌های کنونی نظیر ویستا و هفت یا ویندوز ۸ به شدت افزایش یافته است. این کار از طریق ویژگی‌هایی نظیر User Account Control که مانع از نصب برنامه‌ها بدون اطلاع کاربر می‌شوند، انجام شده است. سیستم‌های دفاعی نظیر تصادفی سازی چیدمان فضای آدرس‌دهی (Address Space Layout Randomization) و ممانعت از اجرای داده‌ها (Data Execution Prevention) نیز استفاده از آسیب‌پذیری‌ها را برای حمله‌کنندگان سخت‌تر کرده‌اند. اما وجود آسیب‌پذیری در نرم‌افزارهایی غیر از سیستم‌عامل (مثلاً جاوا) رو به افزایش بوده است. کامپیوترهای مک اپل مدت‌ها به‌عنوان سیستم‌هایی امن درنظر گرفته می‌شدند که این امر به‌واسطه سهم اندک‌شان از بازار بود. اما آن‌ها هم‌اکنون به هدف بزرگ‌تری برای خرابکاران تبدیل شده‌اند.

در گزارش پیشرفت مرکز واکنش‌های امنیتی مایکروسافت آمده است: «ممانعت از به‌وجودآمدن آسیب‌پذیری‌های امنیتی در پروژه‌های نرم‌افزاری در مقیاس بزرگ تقریباً ناممکن است. تا زمانی که انسان‌ها کدهای نرم‌افزارها را می‌نویسند، هیچ نرم‌افزاری کامل نخواهد بود و اشتباهاتی که منجر به ناکامل بودن نرم‌افزار می‌شوند به وقوع خواهند پیوست.»

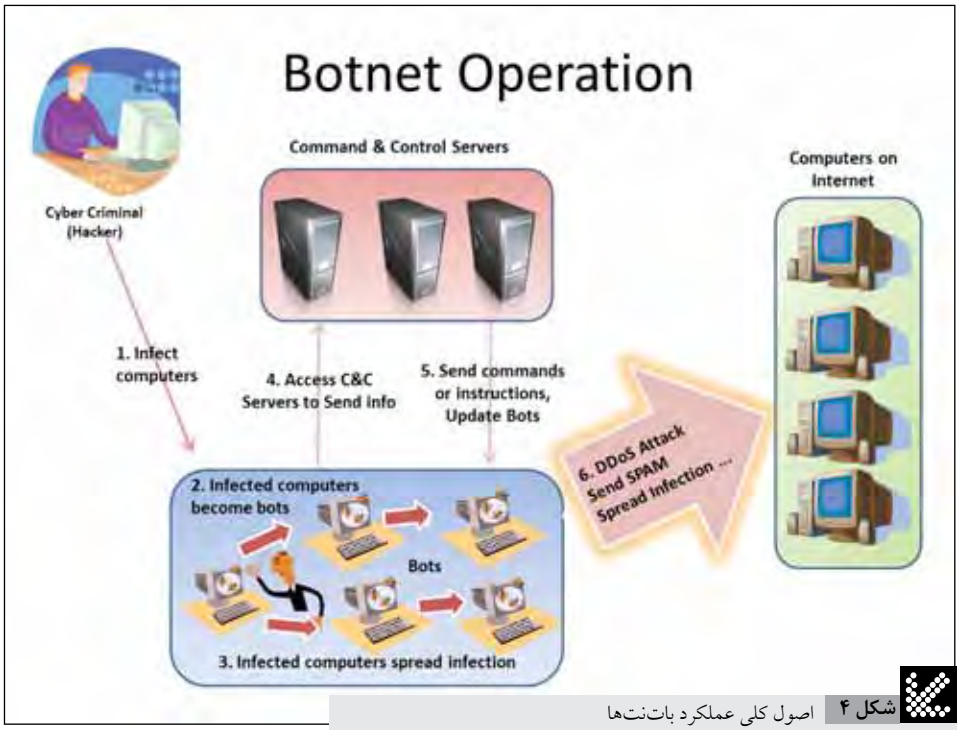
حتی محصولات امنیتی نیز از این موضوع در امان نیستند. همان‌طور که به‌تازگی مشخص شده است، دیواره‌های آتش، VPN و ابزارهای فیلترینگ اسپمی که توسط باراکودا نتورکز (Barracuda Networks) به فروش رسیده‌اند، درهای پشتی داشته‌اند که به هکرها اجازه می‌دادند از راه دور به این سیستم‌ها متصل شده و اطلاعات حیاتی را به سرقت ببرند.

بدافزارها اغلب می‌توانند با استفاده از روت‌کیت‌ها از شناسایی شدن توسط کاربر و نرم‌افزارهای امنیتی فرار کنند. روت‌کیت‌ها اجازه دسترسی سطح بالا به بخش‌های حیاتی سیستم را برای بدافزار و در نتیجه هکر فراهم کرده و می‌توانند حتی وجود یک بدافزار را مخفی کنند. یک روت‌کیت در واقع «نرم‌افزاری است که برای جلوگیری از شناسایی شدن در سطوح بسیار پایین به سیستم‌عامل حمله می‌کند.» روت‌کیت به‌خودی خود بدافزار نیست، بلکه یک فناوری است که بدافزارها از آن برای رسیدن به اهدافش آن هم به‌صورت پنهانی استفاده می‌کند. به گفته کسپرسکی، روت‌کیت‌ها «می‌توانند وجود برخی پرداره‌ها، فولدرها، فایل‌ها یا حتی کلیدهای رجیستری را مخفی کنند.»

در کنار حمله به کامپیوترهای آلوده، یکی از اصلی‌ترین استفاده‌های بدافزارها ایجاد بات‌نت است. بات‌نت شبکه عظیمی از کامپیوترهای به اصطلاح زامبی است که برای انواع مختلف کارهای غیرمجاز مورد استفاده قرار می‌گیرد.

کامپیوتری که جزء یک بات‌نت شود، لزوماً به صاحب خود آسیب نمی‌رساند. در عوض این سیستم آلوده در بات‌نت حالت تهاجمی به خود می‌گیرد و دستوراتی را که از سرور تحت کنترل هکر دریافت می‌کند، به اجرا در می‌آورد.

الیسان می‌نویسد: «یک مأمور یا agent بات‌نت می‌تواند یک فایل اجرایی مستقل یا یک فایل DLL یا قطعه کدی باشد که به فایل اصلی بدافزار افزوده شده است. عملکرد اصلی این agent برقرار کردن ارتباط با دیگر اجزای شبکه بات‌نت است.» (شکل۴)




**شکل ۴** اصول کلی عملکرد بات‌نت‌ها

بات‌نت‌ها را می‌توان برای کاربردهای خرابکارانه متعددی به‌کار گرفت. یکی از مشهورترین نمونه‌ها حمله‌های از کار انداختن سرویس یا DoS (سرنام Denial of Service) است که در آن هکرها با ارسال ترافیک‌های بسیار سنگین به سوی یک سرور خاص آن را از کار می‌اندازند. بات‌نت‌ها را می‌توان برای حمله‌های کلیک تقلبی هم مورد استفاده قرار داد. در این حمله‌ها کامپیوترهای یک بات‌نت روی تبلیغات خاصی (که به‌طور معمول، توسط خود حمله‌کننده میزبانی می‌شود) کلیک می‌کنند تا حمله‌کننده هزینه این کلیک‌ها را دریافت کند. یک بات‌نت منفرد می‌تواند حمله‌های متعددی را انجام دهد. در واقع بسیاری از مجرمانی که بات‌نت‌ها را راه‌اندازی می‌کنند آن‌ها را به دیگر مجرمان اجاره می‌دهند و این اجاره‌کنندگان راه‌های متعددی برای کسب درآمد از این بات‌نت‌ها می‌یابند.

بات‌نت‌ها منشأ بیشترین ایمیل‌های اسپم دنیا نیز هستند. بات‌نت Rustock در اوج دوران فعالیتش در آگوست ۲۰۱۰ به تنهایی مسئول ۶۰ درصد ترافیک اسپم دنیا بود. این بات‌نت در اوایل سال ۲۰۱۱ با عملیاتی بسیار پیچیده از کار انداخته شد.

## حمله به کسب‌وکارها

کسب‌وکارها به دلایل متفاوت و مختلفی از بدافزارها آسیب می‌بینند. یک بانک یا شرکتی که کارت‌های اعتباری را توزیع می‌کند، ممکن است با آلوده شدن سیستم‌های مشتریانش پول از دست بدهد. سایت‌ها همان‌طور که پیش‌تر هم گفته شد، ممکن است با حمله‌های DoS از سوی بات‌نت‌ها روبه‌رو شوند. حمله‌کننده‌ها حتی ممکن است با یافتن تنها یک جای پای محکم در یکی از سیستم‌های آلوده شرکت، آسیب زیادی را متوجه آن شرکت کنند.

بانک‌ها و سایر مؤسسه‌های مالی مدت‌ها است هدف حمله بدافزارهایی قرار می‌گیرند که سعی می‌کنند با دستکاری سایت بانک به حساب‌های مشتریان دسترسی پیدا کنند. البته، بانک‌ها هم ملاحظات امنیتی بسیار سخت‌گیرانه‌ای را برای حفاظت از حساب‌های کاربران‌شان به‌کار می‌برند. اما حمله‌کنندگان نیز با سیستم‌های انتقال خودکار ATS (سرنام Automatic Transfer System) پیشرفته قدرت خود را افزایش داده‌اند.

به گفته ترند مایکرو در سال ۲۰۱۲ «حمله‌های ATS به یکی از تهدیدهای اصلی برای کسب‌وکارهای کوچک تبدیل شده بود. ATSها مشکل فرد میانی یا middleman را که اغلب یک ثبت‌کننده ضربه‌کلید یا فایل آلوده WebInject بود را از سر راه هکرها برداشته‌اند. به جای سرقت اطلاعات (مثلاً اطلاعات حساب بانکی) آن هم به‌صورت غیرفعال (Passive) این حمله‌های ATS به‌طور مستقیم پول را از حساب قربانیان به حساب هکرها حواله می‌کنند. این کار تشخیص کلاهبرداری‌های مالی را دشوارتر می‌کند، زیرا از دید بانک یک تراکنش معمولی و قانونی از سوی کاربر به اجرا درآمده است! در عوض، بدافزارهای سنتی بانکی برای انتقال وجه به دخالت عامل انسانی نیاز داشتند که فرآیند کندتری بود و به سادگی توسط بانک‌ها شناسایی می‌شد.»

ترند مایکرو همچنین می‌افزاید حمله‌ها و نفوذهای متعددی نیز در سال ۲۰۱۲ انجام شدند که کسب‌وکارهای خاصی را هدف گرفته بودند. این حمله‌ها اغلب با یافتن تنها یک ضعف کوچک در زنجیره امنیتی شرکت‌ها انجام می‌شدند.

مک‌آفی در توضیح یک نمونه موردی می‌نویسد: «معمولاً گسترش بدافزار به آرامی انجام می‌شود. نخستین دستگاهی که آلوده می‌شود اغلب یک ایستگاه کاری یا لپ‌تاپی است که سیستم امنیتی قدرتمندی ندارد. سیستمی که ضدویروسی روی آن نصب نشده است یا ضدویروس آن به روز نیست یا از کار انداخته شده است. همچنین وصله‌های امنیتی سیستم‌عامل و برنامه‌های آن نصب نشده‌اند. گاهی حتی کاربران بی‌اطلاع با نصب پلاگین‌های مختلف روی مرورگرشان، بازدید از سایت‌های مشکل‌دار یا کلیک روی لینک‌های مشکوک ایمیل‌ها، دارایی‌های شرکت و موقعیت خودشان را به خطر می‌اندازند.»

همه این‌ها دلیل خوبی است تا سیستم‌های‌مان را به روز نگه داریم، آخرین وصله‌های امنیتی را نصب کنیم و همواره مراقب سایت‌ها و ایمیل‌هایی که نامناسب به‌نظر می‌رسند باشیم.