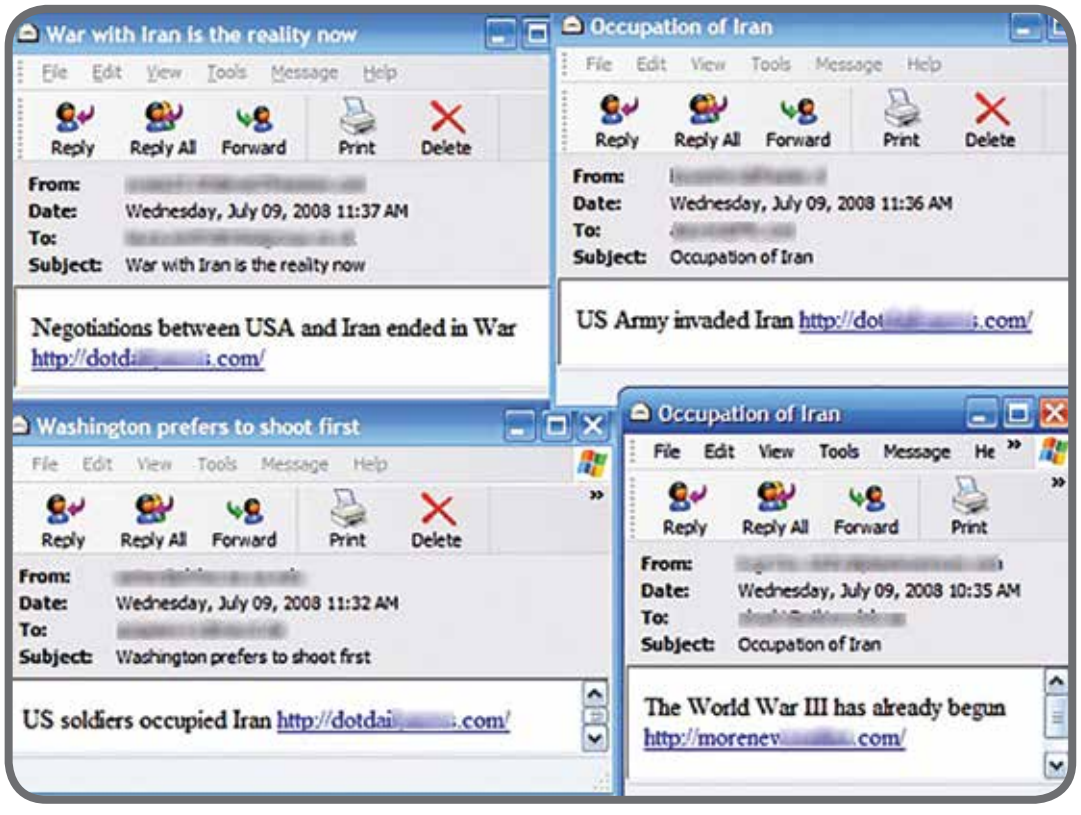
بسیاری از نسخه‌های کرم توفان قربانی را فریب می‌دهند تا برنامه را از طریق پیوندهای جعلی به داستان‌های خبری یا ویدئوها، دانلود کند. افراد پشت این حملات اغلب موضوع ایمیل را تغییر می‌دهند تا رویدادهای جاری را منعکس کنند



هر چند وقت یک‌بار، مقامات راهی برای ردیابی ویروس به منشأ آن پیدا می‌کنند. در مورد ویروس‌های سامر و نتسکی نیز چنین بود. یک جوان ۱۷ساله آلمانی به نام Sven Jaschan این دو برنامه را ایجاد کرد و آنها را در اینترنت منتشر کرد. در حالی که این دو کرم به روش‌های متفاوتی رفتار می‌کردند، شباهت‌های کد باعث شد کارشناسان امنیتی معتقد شوند هر دو کار یک شخص هستند. کرم سامر از طریق آسیب‌پذیری ویندوز مایکروسافت به رایانه‌ها حمله کرد و برخلاف سایر کرم‌ها، از طریق ایمیل پخش نشد. در عوض، هنگامی که ویروس رایانه‌ای را آلوده کرد، به‌دنبال سیستم‌های آسیب‌پذیر دیگر می‌گشت. با آن سیستم‌ها تماس گرفت و به آنها دستور داد ویروس را دانلود کنند. این ویروس آدرس‌های IP تصادفی را برای یافتن قربانیان احتمالی اسکن می‌کند. این ویروس همچنین سیستم عامل قربانی را به‌گونه‌ای تغییر داد که خاموش کردن رایانه بدون قطع برق را دشوار می‌کرد. ویروس نتسکی از طریق ایمیل‌ها و شبکه‌های ویندوز حرکت می‌کند. این ویروس آدرس‌های ایمیل را جعل می‌کند و از طریق یک فایل پیوست ۲۲۰۱۶ بایتی منتشر می‌شود. همان‌طور که گسترش می‌یابد، می‌تواند باعث حمله شود زیرا سیستم‌های در حال فروپاشی سعی می‌کنند تمام ترافیک اینترنت را مدیریت کنند. سازنده ویروس هیچ زمانی را در زندان سپری نکرد. او به یک سال و ۹ ماه حبس تعلیقی محکوم شد. از آنجا که او در زمان دستگیری زیر ۱۸ سال داشت، از محاکمه شدن به‌عنوان بزرگسال در دادگاه‌های آلمان اجتناب کرد.

مای‌دوم

ویروس مای‌دوم کرم دیگری است که می‌تواند سیستم‌عامل رایانه قربانی ایجاد کند. ویروس اصلی مای‌دوم ـ انواع مختلفی وجود داشته است ـ دو محرک داشت. یک محرک باعث شد که ویروس از اول فوریه ۲۰۰۴ حمله Dos را آغاز کند. عامل دوم به ویروس دستور داد تا توزیع خود را در ۱۲ فوریه ۲۰۰۴ متوقف کند. حتی پس از توقف انتشار ویروس عفونت‌های اولیه فعال باقی ماندند. در اواخر همان سال، شیوع دوم ویروس مای‌دوم باعث غم و اندوه چندین شرکت موتورهای جست‌وجو شد. مانند سایر ویروس‌ها، مای‌دوم به‌عنوان بخشی از فرآیند تکثیر خود، رایانه‌های قربانی را برای یافتن آدرس‌های ایمیل جست‌وجو کرد اما همچنین درخواست جستوجو را به موتور جست‌وجو ارسال و از آدرس‌های ایمیل موجود در نتایج جست‌وجو استفاده می‌کند. در نهایت، موتورهای جست‌وجو مانند گوگل شروع به دریافت میلیون‌ها درخواست جست‌وجو از رایانه‌های خراب کردند. این حملات سرعت خدمات موتورهای جست‌وجو را کاهش داد و حتی باعث از کار افتادن برخی از آنها شد. مای‌دوم از طریق ایمیل و شبکه‌های همتا به همتا گسترش یافت. به گفته شرکت امنیتی MessageLabs، از هر ۱۲ پیام ایمیل، یک پیام حامل ویروس در یک زمان بود. مانند ویروس Klez، مای‌دوم می‌توانست ایمیل‌ها را جعل کند، به‌طوری‌که ردیابی منبع ویروس بسیار دشوار شد.

یاقوت کبود

در اواخر ژانویه ۲۰۰۳، یک ویروس وب سرور جدید در سراسر اینترنت پخش شد. بسیاری از شبکه‌های رایانه‌ای برای حمله آماده نبودند و در نتیجه ویروس چندین سیستم مهم را از بین برد. سرویس خودپرداز بانک آمریکا سقوط کرد، شهر سیاتل در خدمات ۹۱۱ دچار اختلال شد و خطوط هوایی قاره‌ای مجبور شدند چندین پرواز را به‌دلیل خطاهای بلیت الکترونیکی لغو کند. مقصر ویروس SQL Slammer بود که به یاقوت کبود نیز معروف است. براساس برخی برآوردها، ویروس قبل از این‌که نرم‌افزارهای آنتی‌ویروس این مشکل را برطرف کنند بیش از یک‌میلیارد دلار خسارت وارد کرده است. پیشرفت حمله اسلمر به‌خوبی مستند شده است. تنها چند دقیقه پس از آلوده‌کردن اولین سرور اینترنتی خود، ویروس هر چند ثانیه تعداد قربانیان خود را دوبرابر می‌کرد. ۱۵ دقیقه پس از اولین حمله، ویروس اسلمر تقریبا نیمی از سرورهایی را که به‌عنوان ستون‌های اینترنت عمل می‌کنند، آلوده کرد.

ویروس اسلمر یک درس ارزشمند داد: اطمینان از داشتن آخرین نرم‌افزار آنتی‌ویروس کافی نیست. هکرها همیشه به‌دنبال راهی برای سوءاستفاده از هر نقطه‌ضعفی هستند، به‌خصوص اگر آسیب‌پذیری به‌طور گسترده شناخته‌شده نباشد. درحالی‌که هنوز مهم است که سعی کنید ویروس‌ها را قبل از این‌که به شما حمله کنند، از بین ببرید، همچنین مهم است که یک برنامه بدترین سناریو برای عقب‌نشینی درصورت وقوع فاجعه داشته باشید.

انتظار برای نابودی

برخی از هکرها ویروس‌ها را طوری برنامه‌ریزی می‌کنند که روی رایانه قربانی فقط برای حمله در یک تاریخ خاص به حالت غیرفعال بنشینند. در اینجا یک نمونه سریع از برخی ویروس‌های معروف که دارای محرک‌های زمانی هستند آورده شده است:

ویروس میکل‌آنژ در ۶ مارس ۱۹۹۲ فعال شد ـ میکل‌آنژ در ۶ مارس ۱۴۷۵ به دنیا آمد.

ویروس چرنوبیل در ۲۶ آوریل ۱۹۹۹ فعال شد ـ سیزدهمین سالگرد فاجعه فروپاشی چرنوبیل

ویروس نیگزم بار خود را در سوم هر ماه فعال می‌کند و فایل‌های رایانه قربانی را پاک می‌کند.

فقط رایانه‌ها قربانی نیستند

همه ویروس‌ها روی رایانه‌ها تمرکز نمی‌کنند. برخی دیگر وسایل الکترونیکی را هدف قرار می‌دهند. در اینجا فقط یک نمونه کوچک از چند ویروس بسیار قابل حمل آورده شده است:

کامان واریر به گوشی‌های هوشمندی که از سیستم‌عامل سیمبین (OS) استفاده می‌کردند، حمله کرد.

ویروس جمجمه همچنین به گوشی‌های سیمبین حمله کرد و به‌جای صفحه اصلی در گوشی قربانیان، صفحه‌نمایش جمجمه‌ها را به نمایش گذاشت.

RavMonE.exe ویروسی است که می‌تواند دستگاه‌های iPod MP۳ ساخته‌شده بین ۱۲ سپتامبر ۲۰۰۶ و ۱۸ اکتبر ۲۰۰۶ را آلوده کند.

فاکس‌نیوز در مارس ۲۰۰۸ گزارش داد که برخی از ابزارهای الکترونیکی با ویروس‌های از پیش نصب شده کارخانه را ترک می‌کنند. این ویروس‌ها هنگامی که دستگاه را با دستگاه خود همگام می‌کنید به رایانه شما حمله می‌کنند.

اواخر سال ۲۰۰۶ بود که کارشناسان امنیت رایانه برای اولین بار این کرم را شناسایی کردند. مردم شروع به نامیدن این ویروس به اسم کرم توفان کردند

رایانه‌های مک به‌دلیل مفهومی به نام امنیت تا حدی در برابر حملات ویروس محافظت می‌شوند. اپل به‌دلیل حفظ سیستم‌عامل (OS) و سخت‌افزار خود به‌عنوان یک سیستم بسته شهرت دارد