آیا برنامهٔ ضدویروس برای تلفنهای موبایل لازم است؟

این روزها خبرهای علمی و فنی رسانه‌ها حاوی داستانهایی از ویروسهای وسایل موبایل است، و شرکتهای سازندهٔ ضدویروس در حال تهیه و بازاریابی نرم‌افزار محافظ هستند. آیا واقعاً باید نگران ویروسهای مخرب برای تلفنهای همراه بود؟

پاسخ در حال حاضر آری و نه است. بسیاری از ویروسهای تلفن همراه در حال حاضر از نوع «اثبات مفهوم» هستند، یعنی سازندگان ویروس در حال حاضر می‌خواهند ثابت کنند که ویروس تلفن همراه ممکن است و قصد خرابکاری ندارند. با این همه، تعدادی ویروس تلفن همراه وارد دنیای تلفن همراه شده است و متخصصان هشدار می‌دهند که تلفنهای همراه، به ویژه نسل جدید **اسمارت‌فونها** (smartphone؛ **گوشیهای هوشمند**) به گونه‌ای فزاینده به هدف ویروس‌نویسان تبدیل می‌شوند.

کجا، کی، و چگونه؟

هر مهاجمی برای یک حملهٔ موفق باید یک روش تحویل دراختیار داشته باشد. ارتباطات صوتی‌ای که حامل داده‌ها نیستند نفوذناپذیر هستند و نمی‌توان حمله‌ای روی آنها تدارک دید. اما، حالا که امواج رادیویی حامل تماسهای تلفن موبایل شما علاوه بر صدا می‌توانند داده‌ها را نیز حمل کنند، مانند پیامهای چندرسانه‌ای و ایمیل، دروازه‌های ورود سیل از لحاظ تئوری باز شده است.

افزون بر این، پیچیدگی و آسیب‌پذیری اسمارت‌فونهای امروزی، که امکاناتی شبیه به امکانات کامپیوتر را فراهم ساخته‌اند، ویروس‌سازان را برای ساخت ویروس و برنامه‌های مخرب دیگر به طرف گوشیهای همراه جلب کرده است. اولین تهدید تلفن همراه، به نام **Cabir**، به عنوان یک ویروس «اثبات مفهوم» در جولای ۲۰۰۴ انتشار یافت. سازندگان ویروس این کد را در اواخر سال ۲۰۰۴ در اینترنت منتشر کردند، و در فوریهٔ ۲۰۰۵ به گوشیهای نوکیا سری 6600 در دو فروشگاه گوشی موبایل کالیفرنیا سرایت کردند.

ویروس **کبیر** (Cabir)، که ابتدا فقط با سیستم‌عامل **سیمبیان سری 60** مورد استفادهٔ نوکیا، سونی‌اریکسون، و چند سازندهٔ دیگر سازگار بود حالا می‌تواند به گوشیهای مجهز به سیستم‌عاملهای Windows Mobile و NTT DocoMo نیز حمله کند. این کرم ویروسی پس از نصب، باتری تلفن را خالی می‌کند و خودش را به گوشیهای آسیب‌پذیر واقع در محدودهٔ دستیابی خود ارسال می‌کند. بعضی از گونه‌های ویروس کبیر فایلها را از گوشی موبایل پاک می‌کنند و تماسهای گران‌قیمت تلفنی برقرار می‌کنند.

از زمان انتشار ویروس کبیر، سازندگان نرم‌افزار ضدویروس بیش از بیست نوع برنامهٔ مخرب را شناسایی کرده‌اند که وسایل موبایل را هدف خود قرار داده‌اند. بسیاری از این برنامه‌های مخرب از نوع **اسبهای تروا** (Trojan horses؛ برنامه‌هایی که در ظاهر مفید به نظر می‌رسند اما در باطن هدف سوء دارند) هستند. چنین تهدیدهایی شامل اسب تروای مرگ‌آور Skulls.B است، که همهٔ امکانات تلفن همراه به جز امکان شماره‌گیری را غیرفعال می‌کند.

تهدید در کجاست؟

پس چرا همهٔ گوشیهای موبایل در خطر نیستند؟ در حال حاضر، کمتر از ۱۰درصد از استفاده‌کنندگان تلفن همراه از اسمارت‌فونها بهره می‌گیرند، در نتیجه، آلودگی ویروسی نادر است. حتی اگر از اسمارت‌فون استفاده می‌کنید، باید تحویل فایلهای مخرب را بپذیرید یا تعمداً خصوصیتی را که به شما پیغام می‌دهد یک فایل ورودی را بپذیرید یا رد کنید غیرفعال نمایید.

با این همه، اگر اینترنت را دستیابی کنید یا MMS یا پیامهای ایمیل حاوی فایل پیوستی را دریافت کنید، ممکن است به طور سهوی فایلهای مخرب را قبول کنید. از سوی دیگر، بعضی از پیامهای MMS آلوده، با متنی می‌آیند که می‌گوید آنها از طرف یک منبع رسمی و مورد اعتماد هستند.

یادآوری: MMS سرواژهٔ عبارت زیر است:

Multimedia Messaging Service

افزون بر این، دو فناوری مبادلهٔ داده‌ها، **بلوتوث** و IrDA، گوشیهای موبایل را برای تبادل داده‌ها به طور خودکار فعال می‌کنند. IrDA کمتر

مسئله دارد زیرا فقط در خط مستقیم دید کار می‌کند و برد مؤثر آن کمتر از ۳متر است. بلوتوث در فاصله‌ای نزدیک به ۱۰متر کار می‌کند و دیوار، لباس، یا چمدان برای آن مانع نیستند. اگر وسیلهٔ بلوتوث خود را طوری میزان کنید که وسایل دیگر بتوانند آن را پیدا کنند، به آسانی می‌توانید یک ویروس واقع در یک گوشی نزدیک به خود را در یک کافی‌شاپ یا مکان عمومی بگیرید.

در حال حاضر، هیچ یک از سیستم‌عاملهای گوشی موبایل یک **برنامهٔ دیوارهٔ آتش** (firewall) توکار ندارند، در نتیجه، یک برنامهٔ مهاجم واقع در گوشی تلفن همراه می‌تواند مسائلی جدی به وجود بیاورد. پژوهشگران کرمهایی شبیه به کرمهای پی‌سی را پیش‌بینی می‌کنند که پیامهایی را بر بنیاد اطلاعات واقع در تلفن شما تولید خواهند کرد و سپس آنها را به همهٔ کسانی که در فهرست تماس شما هستند ارسال خواهند کرد. مسئلهٔ دیگر، که در اروپا و ژاپن نیز پیشتر گزارش شده است، کنترل گوشی موبایل برای استفاده به عنوان روباتهای حمله‌کننده به سایر گوشیها یا **خدمات‌دهنده‌های** (server) اینترنت است.

موقع حفاظت؟

خوشبختانه، اگر یک گوشی موبایل معمولی داشته باشید، نباید نگران باشید. ویروسها روی گوشیهای دارای سیستم‌عامل باز، و همچنین گوشیهایی که به اینترنت وصل می‌شوند، عمل می‌کنند. در نتیجه، اگر یک اسمارت‌فون داشته باشید (به ویژه از انواع مبتنی بر سیستم‌عامل سیمبیان)، لازم است که اقدامات احتیاطی را همواره رعایت کنید.

شرکت Trend Micro در حال حاضر محصولات ضدویروس رایگان برای محیطهای سیمبیان و ویندوز موبایل عرضه می‌کند:

www.trendmicro.com

شرکتهای سازندهٔ ضدویروس دیگری نیز برای بعضی از گوشیهای سیمبیان نرم‌افزار ضدویروس تهیه کرده‌اند. نشانی وب این شرکتها به قرار زیر است:

www.f-secure.com
www.kaspersky.com
www.symantec.com

این محصولات شبیه به برنامه‌های ضدویروس متداول روی پی‌سی‌ها کار می‌کنند و فایلهای ورودی و خروجی را از لحاظ الگوهای شناخته‌شده بررسی می‌کنند. برنامهٔ ضدویروس درست مانند سایر برنامه‌های کاربردی موبایل بر روی گوشی موبایل شما نصب می‌شود؛ معمولاً می‌توانید به پایگاه وب شرکت سازنده سربزنید و نرم‌افزار را مستقیماً دریافت کنید. در اکثر موارد، می‌توانید این برنامه را در کامپیوتر خود دریافت کنید و سپس با وسیلهٔ موبایل خود برای ارسال نرم‌افزار **یکسان‌سازی** (sync) کنید. اکثر گوشیها پس از تکمیل عملیات دریافت، یا به محض آن که فایل دریافتی را باز کنید، عملیات نصب را آغاز می‌کنند. (برای اطلاعات بیشتر به دفترچهٔ راهنمای گوشی موبایل خود مراجعه کنید.)

آینده‌ای نامطمئن

تا به حال، توزیع ابزار مخرب در اسمارت‌فونها به دلیل تعداد کم کاربران آنها نادر بوده است. اما این وضعیت به زودی تغییر خواهد کرد، چون قیمت اسمارت‌فونها در حال پایین آمدن است و به زودی تعداد زیادی از کاربران موبایل به سمت بهره‌گیری از آنها خواهند رفت. در نتیجه، نویسندگان ویروس نیز توجه بیشتری به اسمارت‌فونها خواهند کرد. آنها دو سیستم‌عامل سیمبیان (۸۰درصد از بازار) و ویندوز موبایل (حدود ۱۰ درصد بازار) را هدف خواهند گرفت و با اندک زحمتی می‌توانند خسارات عظیمی به وجود بیاورند.

حفاظت

به دلیل استفادهٔ گسترده‌تر مردم از گوشیهای موبایل نسبت به کامپیوترها، بهره‌گیری از خطوط دفاعی مستحکم بسیار اهمیت دارد. در مکانهای عمومی امکانات بلوتوث و IrDA (مادون قرمز) را روی Off تنظیم کنید و امکاناتی را که دریافتهای (download) خودکار را اجازه می‌دهند فعال نکنید. هیچ فایلی را، حتی یک آهنگ برای زنگ گوشی را قبول یا دریافت نکنید، مگر این که منبع را بشناسید. در مورد پیامهای MMS و ایمیل حاوی فایل پیوستی هشیار باشید، اما پیامهای متنی سالم هستند.

افزون بر این، در استفاده از اینترنت احتیاط کنید. کاربران اروپایی و ژاپنی مواردی از کلاهبرداری یا phishing با گوشی موبایل را گزارش کرده‌اند (phishing نوعی کلاهبرداری است که کلاهبردار با انواع ترفندها کاربر را فریب می‌دهد که اطلاعات خصوصی خود را فاش کند.)

ثابت‌قدم باشید. بسیاری از کاربرانی که گوشیهای موبایل آنها به ویروس مرگبار Skulls آلوده شده است گزارش کرده‌اند که آنها بارها به پرسش مربوط به یک پیام ورودی پاسخ No داده‌اند اما وقتی دیدند که این پرسش دست‌بردار نیست روی Yes کلیک کردند. نتیجهٔ این تصمیم آنها یک گوشی بی‌ارزش بود.■