روت کیتها(ROOTKIT): بدتر از ویروسها

اگر فکر می‌کرده‌اید که ویروسها، برنامه‌های جاسوسی، و **هکر**ها تنها خطرات اینترنت هستند اشتباه می‌کنید. نوع دیگری از تهدید کامپیوتری وجود دارد که به طور ساکت و پنهانی عمل می‌کند و اکثر مردم از حضور آنها وقتی آگاه می‌شوند که دیگر خیلی دیر شده است. این تهدید به **روت‌کیت** (rootkit) مشهور است، که روز به روز توجه به آن بیشتر می‌شود و از دنیای یونیکس وارد دنیای ویندوز شده است.

ریشهٔ مسئله

ابتدا چند اصطلاح را توضیح می‌دهیم. روت‌کیت به هر برنامه‌ای گفته می‌شود که به روشهای زیر کار می‌کند:

۱.تهاجمی. روت‌کیت از طریق یک تظاهر نادرست وارد کامپیوتر می‌شود، گاهی با نقاب یک برنامهٔ دیگر یا از طریق یک «نصب ساکت».

۲.پنهانی. روت‌کیتها با بهره‌گیری از تکنیکهای مختلف خودشان را نه تنها از نظر کاربر پنهان می‌سازند بلکه سعی می‌کنند سیستم‌عامل نیز آنها را شناسایی نکند. **سیستم فایل** نمی‌تواند فایلهایی را که روت‌کیت را تشکیل می‌دهند ببیند، و حتی اگر این فایلها آشکار باشند، آنها ممکن است **رمزنگاری** شده باشند یا چندچهره باشند. (به عنوان مثال، آنها خودشان را برای جلوگیری از شناسایی رمزی می‌کنند.)

۳.بی‌اجازه. وقتی روت‌کیتها خودشان را نصب می‌کنند، به اجرای کارهایی ادامه می‌دهند که به احتمال زیاد شما هیچ وقت دوست ندارید روی بدهند. این کارها می‌تواند شامل ثبت کلیدزنیها و ارسال آنها به یک شخص ثالث، گروگان‌گیری داده‌ها (مثلاً محتویات نهانگاه برنامهٔ مرورگر یا ایمیل)، ایجاد تداخل با عملیات عادی کامپیوتر و مانند آن باشد.

بعضی از مردم روت‌کیت را به عنوان وسیله‌ای تعریف می‌کنند که خودش یا سایر داده‌های روی یک سیستم را پنهان می‌کند، اما اکثر روت‌کیتهای موجود، دیگر فقط اسباب‌بازیهایی نیستند که بخواهند حضور خود را اثبات کنند. آنها شرارت می‌کنند، و اگر با یکی از آنها برخورد کنید لازم است بدانید که علیه چه چیزی باید اقدام کنید.

کلمهٔ «root» در rootkit از دنیای یونیکس آمده است، که در آن **حساب مدیر سیستم** را **root** می‌نامند. اگر یک **خدمات‌دهنده** (server) یونیکس هک شود، یا به گونه‌ای از دنیای خارج به مخاطره بیفتد که یک کاربر غیرمجاز بتواند به عنوان root فرمان صادر کند، گفته می‌شود که «خدمات دهنده روت شده است». مجموعهٔ روت اولیه احتمالاً یک مجموعه از برنامه‌های خدماتی معمولی یونیکس به منظور هک‌کردن بدون به جای گذاشتن هیچ ردپایی بوده است. در میان اینها ابزار تغییر دادن کلمه‌های عبور حسابها بود؛ اگر فهرست کلمه‌های عبور به طور پنهانی فاش می‌شد، هر کسی می‌توانست کامپیوتر مسئله‌دار را دستیابی کند.

روت‌کیتها و ویروسها نقاط اشتراک فراوانی دارند، به ویژه از لحاظ طرز کار، اما در چگونگی گسترش خود تفاوت می‌کنند. روت‌کیتها معمولاً به گونه‌ای ساکت روی یک سیستم خاص گسترش می‌یابند. چنین سیستمی می‌تواند یک کامپیوتر حاوی داده‌های حساس باشد که کسی دیگر به دنبال آنهاست (فایلها، کلیدزنیها، داده‌ها، و مانند آن). در مقابل، ویروسها آزادانه و بی‌قاعده گسترش می‌یابند و سعی می‌کنند که روی یک سیستم تا جای ممکن خرابی به بار بیاورند. روت‌کیتها معمولاً روی یک سیستم جا خوش می‌کنند و خیلی زیاد منتشر نمی‌شوند. با این همه، ویروسها در حال حاضر شروع به استفاده از سبک پنهان‌کاری روت‌کیتها کرده‌اند و دست‌کم یک برنامهٔ جاسوسی وجود دارد که خودش را از نظر کاربر و سیستم‌عامل با حیله‌ای به سبک روت‌کیت پنهان می‌سازد (گونه‌ای نفرت‌انگیز از برنامهٔ CoolWebSearch).

روت‌کیتها معمولاً به یکی از سه طریق کار می‌کنند. یک روت‌کیت **هسته** یا **کرنل** (kernel) که مستقیماً به هستهٔ سیستم‌عامل _ کرنل _ وصل می‌شود و کدی را اضافه می‌کند که کرنل نمی‌تواند دربارهٔ آن چیزی بفهمد. یکی از روشهای متداولی که این کار را انجام می‌دهد وصل شدن آن به بخشی از کرنل است که ورودی / خروجی فایل را پردازش می‌کند؛ اگر روت‌کیت بتواند پشت پردهٔ همهٔ عملیات فایلی که در سیستم انجام می‌گیرد قرار بگیرد می‌تواند مطمئن شود که بخشهای خود روت‌کیت هرگز آشکار نخواهد شد. شبیه به باندی از دزدان است که ایستگاه

عوارضی یک بزرگراه ورودی به یک شهر را در دست گرفته‌اند: اگر یک عضو باند بخواهد وارد شهر شود بدون پول گرفتن به او اجازه می‌دهند، اما هر کس دیگری باید عوارض بپردازد. دزدان می‌توانند از این دروازه بی‌آن که شناسایی شوند عبور کنند چون خودشان این دروازه را اداره می‌کنند.

روت‌کیتهای کتابخانه‌ای (library) کمی بالاتر در سیستم‌عامل کار می‌کنند اما چیزی شبیه به همان روش را به کار می‌گیرند. آنها جلوی فراخوانیهایی از عملیات سیستمی معمول را می‌گیرند که ممکن است حضور آنها را فاش کنند. **روت‌کیتهای کاربردی** (application) برنامه‌های مفید را با نگارشهایی عوض می‌کنند که مسئله‌دار هستند، معمولاً به عنوان یک روش برای مستقرکردن روت‌کیت در سیستم. اگر برنامه‌ای را به اجرا درآورید که به نظر برسد همچون یک برنامهٔ مفید کار می‌کند اما در حقیقت یک روت‌کیت باشد، فقط سیستم خود را بی‌آن که بدانید آلوده کرده‌اید.

نظر به این که روت‌کیتها از اقدامات مختلفی برای پنهان‌کردن رد خود بهره می‌گیرند، دانستن این که یک روت‌کیت در کامپیوترتان کمین کرده است نیمی از عملیات مقابله با آنهاست.

تقریباً غیرقابل شناسایی

همچون فناوری ویروسی، فناوری روت‌کیت پیوسته در حال ترقی است، و آنهایی که دربارهٔ طرز کار روت‌کیتها پژوهش می‌کنند سعی می‌کنند یک گام جلوتر از رقبا باشند. یک مثال از یک مفهوم روت‌کیتی که هنوز آفتابی نشده است، اما دست‌کم در آزمایشگاه ساخته شده است، روت‌کیتی مشهور به VMBR است. VMBR سرواژهٔ عبارت زیر است:

Virtual Machine-Based Rootkit

البته، منظور از **کامپیوتر مجازی**، شبیه‌سازی یک پی‌سی در داخل یک پی‌سی است، با سیستم‌عامل خودش و سخت‌افزار مجازی‌شده. برنامه‌هایی چون VMware و Microsoft VirtualPC از این فناوری بهره می‌گیرند. بعضی از متخصصان، عاشق استفاده از کامپیوترهای مجازی به عنوان آزمایشگاهی برای اجرای نرم‌افزار در محیطهای کنترل‌شده هستند. پی‌سی در داخل پی‌سی را با سیستم **میهمان** نیز اشاره می‌کنند؛ پی‌سی‌ای که کامپیوتر مجازی را اجرا می‌کند **میزبان** (host) است.

یک VMBR از این فناوری به روشی کاملاً پنهانی بهره می‌گیرد به طوری که وقتی نصب شود کنترل دنبالهٔ بوت را در کامپیوتر به دست می‌گیرد و خودش را بوت می‌کند. سپس VMBR به عنوان یک میزبان کار خواهد کرد و سیستم‌عامل معمول شما را به عنوان یک میهمان و در درون خود بار خواهد کرد. به این ترتیب، VMBR می‌تواند به طور کامل همهٔ جوانب اجرای سیستم‌عامل را از خارج کنترل کند. حال سوءاستفاده‌کننده می‌تواند هر قطعهٔ اطلاعاتی روی آن ماشین، از کلیدزنیها گرفته تا داده‌های شبکه را بی‌آن که کاربر متوجه بشود برباید. خود سیستم نیز طوری فریب داده می‌شود که متوجه حضور VMBR نشود.

خوشبختانه، VMBRها هنوز در خارج از آزمایشگاه متولد نشده‌اند، اما اگر کنجکاو باشید رساله‌های متعددی از مهندسان دانشگاه میشیگان و بخش تحقیقات مایکروسافت را در پایگاه وب زیر می‌توانید بخوانید:

www.eecs.umich.edu/virtual/papers/king06.pdf

فتنهٔ سونی

نکتهٔ حیرت‌آور در توزیع بدترین روت‌کیت دنیا تا به حال آن است که این روت‌کیت از طریق هکرهای شریر یا جانیان زیرزمینی منتشر نشده است. شرکت سونی مسئول توزیع یک روت‌کیت به عنوان بخشی از اقدام خود علیه کپی‌برداری غیرمجاز بوده است. این روت کیت را مؤلف برنامهٔ Rootkit Revealer، به نام مارک روسینوویچ کشف کرد و گزارش خود را در پایگاه وب زیر آورد:

www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

او یک سی‌دی Sony BMG را در دیسکران قرار داد، یک برنامهٔ پخش خودکفا به اجرا درآمد که نسخه‌های محافظت شده در برابر کپی‌برداری موسیقی روی دیسک را پخش می‌کرد. این سی‌دی به طور پنهانی برنامه‌ای به نام XCP را بی‌آن که به کاربر بگوید در کامپیوتر نصب کرد. این برنامه جلوی کپی‌برداری از آهنگهای روی سی‌دی را می‌گیرد اما در ناپایداری سیستم نقش دارد و مسائلی نیز به وجود می‌آورد. راهی برای حذف این برنامه از کامپیوتر نیز وجود ندارد. مقالهٔ روسینوویچ طوفانی به وجود آورد و سونی مجبور شد که استفاده از XCP را متوقف کند **(cp.sonybmg.com/xcp)**

سلاحهای دفاعی

خبر خوب آن است که روت‌کیتها کاملاً غیرقابل شناسایی نیستند. نقطهٔ قوت آنها نقطهٔ ضعف آنها نیز هست. این حقیقت که روت‌کیتها فایلها را از سیستم‌عامل پنهان می‌کنند می‌تواند علیه خود آنها به کار گرفته شود.

یکی از اولین روشها برای ریشه‌یابی روت‌کیتها بوت‌کردن سیستم به یک سیستم‌عامل پاک از طریق یک سی‌دی، گرفتن یک فهرست دیرکتوری از همهٔ فایلهای روی سیستم، و سپس مقایسهٔ آن با یک فهرست مشابه تولید شده از داخل سیستم‌عامل مورد ریشه‌یابی است. اگر دو فهرست مختلف باشند، فایلهای حذف شده از فهرست سیستم‌عامل مورد ریشه‌یابی، شک‌برانگیز است.

اجرای این کار به طور دستی بسیار دشوار است. در نتیجه، برنامه‌هایی برای خودکارسازی این عملیات ساخته شده است. مشهورترین آنها برنامهٔ Rootkit Revealer است:

www.sysinternals.com/utilities/rootkitrevealer.html

این برنامه دیسک را دوبار بررسی می‌کند، یک بار از طریق سیستم فایل و بار دوم با دستیابی داده‌های دیسک. نتایج سپس با هم مقایسه می‌شوند، و اگر فایلی سعی کند که مخفی شود، به عنوان یک اختلاف بین دو فهرست فایل نشان داده خواهد شد.

مایکروسافت نیز یک برنامهٔ بسیار قدرتمند مقابله با روت‌کیتها به نام Strider GhostBuster ساخته است:

research.microsoft.com/rootkit

این برنامه نیز شبیه به RootkitRevealer کار می‌کند، اما یک روش مقایسهٔ اضافی سیستم فایل با یک بررسی مجزای بوت‌شده با سی‌دی دارد. این روش برای ریشه‌یابی روت کیتها بسیار قدرتمندتر است اما آهسته عمل می‌کند چون به بوت کردن کامپیوتر نیاز دارد. با این همه، در زمان چاپ این مقاله، هنوز GhostBuster برای استفادهٔ عمومی در دسترس قرار نداشت.

یک خوبی پدیدهٔ روت‌کیت آن است که بسیاری از روالهایی که مؤلفان روت‌کیت استفاده می‌کنند به خوبی مستند شده است. پایگاه Rootkit.com نمونه‌های بسیاری را دارد. این پایگاه همچنین بحثی دربارهٔ فایدهٔ استراتژیهای روت‌کیت نیز دارد. به عنوان مثال، می‌توان نرم‌افزار ضدویروس را طوری طراحی کرد که خودش را در برابر حملات مستقیم ویروسها پنهان کند.

حذف روت کیت

اگر روی کامپیوتر خود یک روت‌کیت پیدا کنید، واکنش اولیهٔ شما شاید این باشد «چگونه از شر این چیز خلاص شوم؟» پاسخ کوتاه؟ خودتان را به زحمت نیندازید. نظر به این که روت‌کیتها را به دشواری می‌توان حذف کرد، معمولاً زحمت این کار ارزش ندارد. حتی اکثر متخصصان بدون صدمه زدن به سیستم‌عامل، در عملیات حذف روت کیت، نمی‌توانند آن را حذف کنند و به شما توصیه خواهند کرد که کل کامپیوتر را پاکسازی کنید.

بنابراین، با یک کامپیوتر آلوده به روت‌کیت، همچون زمین سوخته رفتار کنید. از داده‌هایی که می‌توانید یک **نسخهٔ پشتیبان** تهیه کنید، دیسک سخت را پاک کنید، و همه چیز را از اول نصب کنید. در مورد نرم‌افزارهایی که نصب می‌کنید محتاط باشید، چون معلوم نیست که روت‌کیت از کدام یک از سی‌دی‌های شما آمده است.

برنامه‌ای به نام RKDetector به شما امکان خواهد داد که فایلهایی را که یک روت‌کیت استفاده می‌کند حذف کنید، حتی زمانی که کامپیوتر بر **روی خط** (آن‌لاین) است. برنامه‌های دیگر مفید عبارتند از Black light، Klister، و VICE. نشانی پایگاه وب این برنامه‌ها به ترتیب به قرار زیر است:

www.rootkitdetector.com
www.f-secure.com
www.rootkit.com/project.php?id=14
www.rootkit.com/project.php?id=20

اگر کامپیوتر آلوده، حاوی داده‌های مهمی باشد، مثلاً یک server با داده‌های مهم باشد، آن را پاک نکنید، با متخصصان روت‌کیت مشورت کنید.

دست‌کم یک روت‌کیت وجود دارد که مورد استفادهٔ یک گروه هکر تروریست قرار گرفته است. این گروه دهها هزار کامپیوتر را با به کارگیری **حفره‌های امنیتی** واقع در AOL Instant Messenger به گروگان گرفته بودند. با وجود این، احتمالاً شما با چنین وضعیتی برخورد نخواهید کرد، اما این اثر روت‌کیتها وجود دارد.□