آیا حفره‌های امنیتی لینوکس شما را در معرض تهدیدات قرار می‌دهند؟

مواظب باشید: امنیت لینوکس در خطر است!

آیا روزگاری که همگان سیستم‌عامل ویندوز را به‌دلیل ضعف‌های امنیتی و لینوکس را به دلیل پایداری و امنیت بالا مورد تحسین قرار می‌داند را به‌خاطر می‌آورید. در آن روزگار ما گفتیم زمانی‌که لینوکس به‌طور گسترده مورد استفاده قرار گیرد، آن‌گاه مشکلات و ایرادات امنیتی آن خود را نشان خواهند داد. در حالی‌که ویندوز این روزها به سمت و سوی ایمن‌تر شدن گام بر می‌دارد، لینوکس در حال نزدیک شدن به روزهای اولیه ویندوز است.

با وجود یک تروجان و رخنه‌های امنیتی پیچیده‌ای که قدمتی 20 ساله دارند، این روزها امنیت لینوکس حال و روز خوبی ندارد. باگ Shellshock (که بعضی مواقع به‌نام Bashdoor نامیده می‌شود)، روی نسخه دسکتاپی و سرور لینوکس باعث شد تا این سیستم‌عامل به‌صورت باز در اختیار کاربران قرار گیرد. هر چند به‌روزرسانی‌های امنیتی توانسته‌اند این مشکل را حل کنند، اما این احتمال وجود دارد که شما این به‌روزرسانی را دریافت نکرده باشید. باگ امنیتی مهمی که در سال 2014 روی لینوکس کشف گردید باعث شد تا افسانه نفوذ ناپذیر بودن لینوکس شکسته شود. بله آسمان به زمین نرسید و هنوز هم لینوکس نسبت به ویندوز امن‌تر است، اما این باگ امنیتی ثابت کرد عاشقان لینوکس لازم است حداقل یک‌بار دیگر در ارتباط با محافظت از سیستم‌های خودشان دقت بیشتری مبذول دارند.

Turla برای چندین سال لینوکس را آلوده کرده بود

برای سال‌های متمادی، محققان امنیتی از وجود یک قطعه مخرب بسیار پیچیده نرم‌افزاری که به‌نام‌های Turla، Snake یا Ouroboros نامیده می‌شود باخبر بودند. آن‌گونه که از شواهد مشخص شده است، Turla بدافزاری نیست که توسط یک شخص یا یک گروه عادی طراحی شده و حمایت مالی شود. سیستم‌عامل ویندوز اولین هدف این بدافزار بود. اما سرانجام، شرکت امنیتی کسپرسکی، نسخه لینوکسی بدافزار Turla را شناسایی کرد. این تروجان سال‌هاست که بدون سر و صدا اقدام به آلوده کردن سیستم‌عامل لینوکس کرده بود. این تروجان بر مبنای یک برنامه درپشتی منبع باز به‌نام cd00r طراحی شده است. Turla به ترافیک شبکه گوش کرده و به هکرها اجازه اجرای فرامین را روی سیستم‌های لینوکسی آلوده می‌دهد. اما نکته مهم در رابطه با این تروجان به عدم نیاز به دسترسی ریشه باز می‌گردد، به‌طوری که همچون حساب کاربری استاندارد لینوکس اجرا می‌شود، همین موضوع باعث می‌شود تا هیچ‌یک از محدودیت‌های نسخه دسکتاپی لینوکس مانع آن نشود. در حالی‌که Turla یک سرویس شبکه است، اما به اندازه کافی هوشمند است تا خودش را از دست ابزار netstat پنهان سازد، در نتیجه اگر ارتباطات شبکه خود را

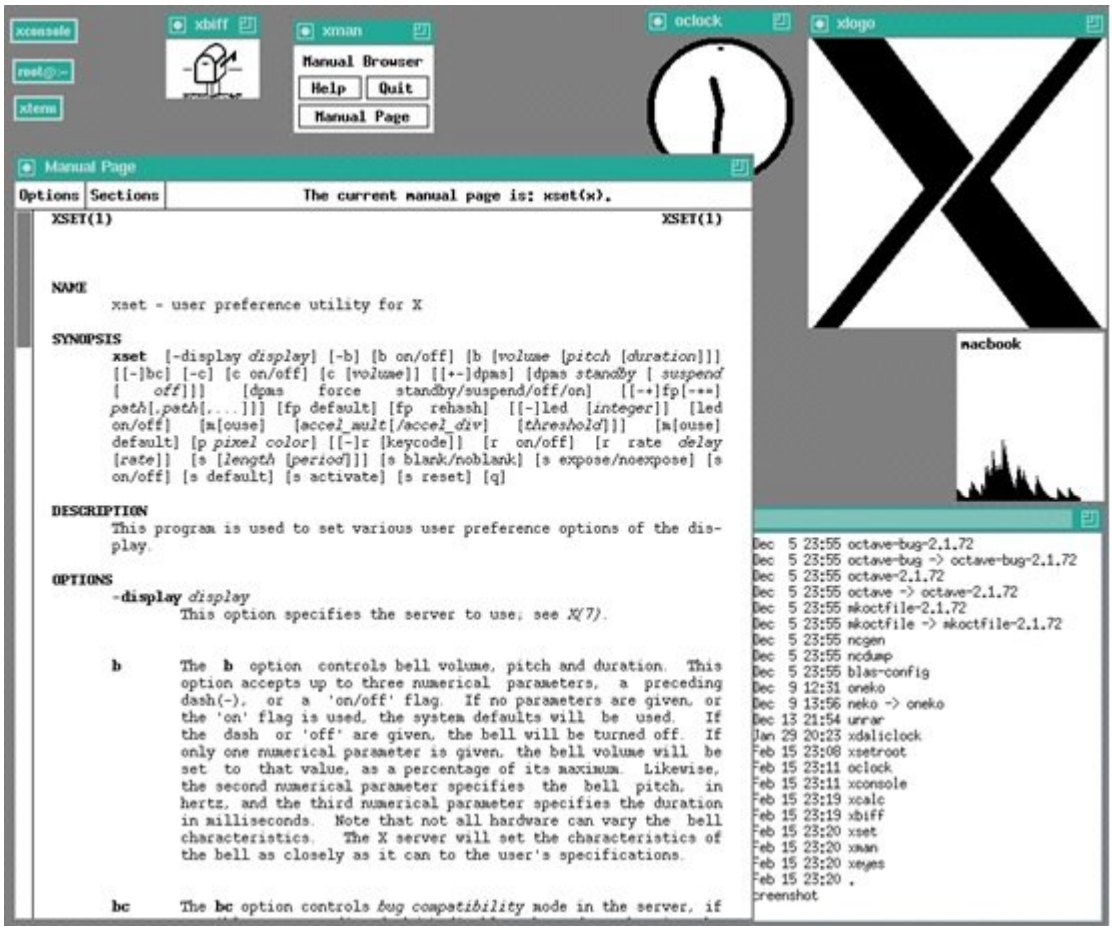
تحت نظارت و بازرسی قرار داده و به آن گوش کنید (listening) از وجود آن آگاه نخواهید شد.

آیا دلیلی برای ترسیدن وجود دارد؟

این بدافزار به چند دلیل ترسناک است. اول آن‌که نشان داد تروجان‌ها توانایی آلوده‌سازی سیستم‌های لینوکس را دارند. دوم آن‌که عدم دسترسی به ریشه هیچ مانعی برای فعالیت‌های بدافزارها محسوب نمی‌شود. اما مهم‌تر از همه، این که این توانایی را دارد تا تمامی فعالیت‌های بانکی آنلاین را تحت حساب کاربری، یک کاربر انجام دهد، که همین موضوع دسترسی آزاد و بدون محدودیت را در اختیار تروجان‌های لینوکسی قرار می‌دهد. با توجه به تحقیقات انجام گرفته از سوی کسپرسکی به دلیل این‌که یک دولت حامی مالی Turla است در نتیجه این احتمال وجود دارد که کاربران عادی هدف این تروجان نبوده و شاید شما کاربر لینوکس اصلا هدف Turla محسوب نشوید. Turla به‌گونه‌ای طراحی شده است تا به نظارت و جاسوسی از شرکت‌های بزرگ پرداخته و شماره کارت‌های اعتباری را سرقت نکند. این تروجان برای سال‌های متمادی اقدام به آلوده‌سازی کامپیوترها در سرتاسر جهان کرده است. بله، امکان وجود تروجان برای سیستم‌عامل‌های لینوکسی نه تنها منتفی نیست، بلکه وجود هم دارند.

X.Org مشکلاتی امنیتی با تاریخچه 20 ساله!

سال گذشته، ما فهرست طولانی از آسیب‌پذیری‌های امنیتی را در سرور گرافیکی X.Org و کتابخانه‌های مرتبط با آن مشاهده کردیم. بعضی از این حفره‌های امنیتی قدمتی بیش از بیست سال دارند، محققی که موفق به شناسایی این حفره‌های امنیتی شد، اعلام کرد، امنیت X.Org یک فاجعه کامل بوده و بسیار بدتر از آن چیزی که در ظاهر به‌نظر می‌رسد است. فهرستی از این آسیب‌پذیری‌ها در آدرس public knowledge منتشر شده است. توزیع کنندگان لینوکس اقدام به ارائه به‌روزرسانی‌های امنیتی برای سرور X.Org و درایورهای Nvidia کردند، اما با وجود عرضه این به‌روزرسانی‌ها باز هم نمی‌توان با قاطعیت کامل به امنیت X.org اعتماد کرد.



X.org یک مشکل امنیتی بزرگ است، به دلیل این‌که بر مبنای معماری X11 قرار دارد که نزدیک به 30 سال از عمر آن می‌گذرد. اما فناوری‌های سروری جایگزینی همچون Wayland and Ubuntu’s Mir قرار است جای X.org را بگیرند.

Shellshock کابوسی بزرگ برای کاربران دسکتاپی و سروری لینوکس

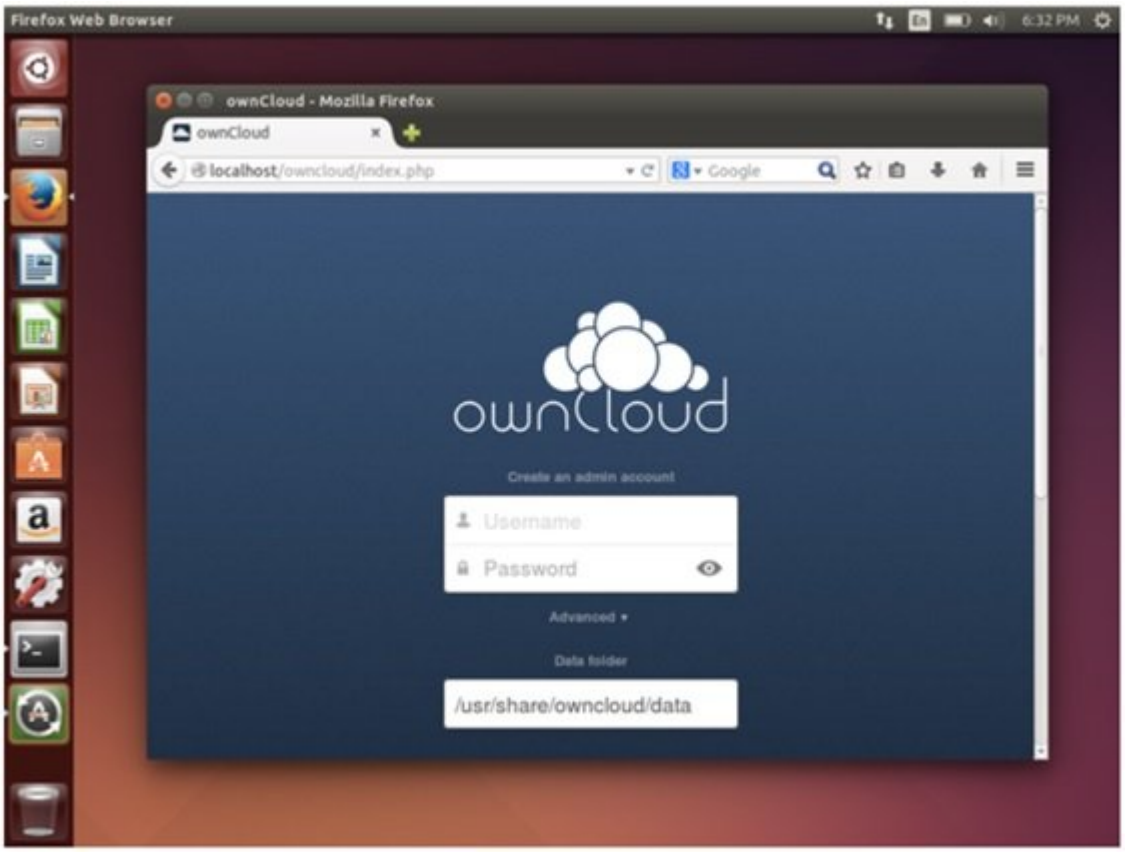
آیا Shellshock که یک باگ در پوسته Bash (سرنام Bourne Again Shell) بوده و توسط لینوکس و سیستم‌های یونیکس مورد استفاده قرار می‌گیرد، را به یاد می‌آورید. کارشناسان امنیتی در آن روزگار اعلام کردند، که این باگ امنیتی هیچ تأثیری روی کاربران دسکتاپی نمی‌گذارد. کامپیوترهای ویندوزی Bash را در اختیار ندارند. در دنیای مک تنها کاربران حرفه‌ای از bash استفاده می‌کنند.

اما برای دسکتاپ‌ها و سرورهای لینوکسی که از Bash استفاده می‌کردند، اوضاع چندان جالب نبود. اما چه عاملی باعث ایجاد وحشت شده بود؟ هر درخواستDHCP که توسط کامپیوتر شما ساخته می‌شد، از طریق Bash حالت اجرایی پیدا می‌کرد. در نتیجه، اگر با استفاده از لپ‌تاپ لینوکسی خود به یک هات‌اسپات عمومی بی‌سیم متصل می‌شدید در معرض خطر قرار می‌گرفتید. به دلیل این‌که سرور DHCP در واکنش به درخواست شما این توانایی را داشت تا درخواستی را در قالب اجرای یک دستور به سیستم شما تحمیل کرده تا اقدام به دانلود تروجانی کند. نمونه‌ای از این فرآیند را در آدرس an easy proof-of-concept attack می‌توانید مشاهده کنید.

به‌روزرسانی‌های امنیتی، توانستند این تهدید را به سرعت برای کاربران دسکتاپی برطرف کنند، اما آسیب‌پذیری Shellshock به مدت بیست سال روی Bash وجود داشت. هر چند ما هیچ‌گونه نشانه‌ای از حملات گسترده‌ای که کاربران دسکتاپ را نشانه رفته بود مشاهده نکردیم، اما این تمام ماجرا نیست. این آسیب‌پذیری به رویای نفوذ ناپذیر بودن لینوکس پایان داد، به‌طوری که تا قبل از شناسایی این آسیب‌پذیری همگان بر ایمن بودن لینوکس نسبت به سیستم‌عامل ویندوز تأکید داشتند. اما Shellshock به ما نشان داد لینوکس نیز می‌تواند آلوده باشد.

آیا وصله‌های امنیتی را دریافت کرده‌اید؟

با تشکر از سیستم بسته‌بندی و مخزن نرم‌افزاری که لینوکس بر پایه آن کار می‌کند، شما ممکن است وصله‌های امنیتی که توسط طراحان عرضه شده است را دریافت نکرده باشید. به احتمال زیاد، شما آن‌ها را از طریق مرورگر خود و به‌روزرسانی‌های امنیتی را از طریق مبادی رسمی که وظیفه پشتیبانی را بر عهده دارند دریافت می‌کنید، اما چه کسی مسئولیت بسته‌های دیگر را بر عهده دارد؟



بدون شک درس‌های زیادی از مشکلات موجود در مدل به‌روزرسانی ownCloud متعلق به اوبونتو می‌توان یاد گرفت. یک قطعه نرم‌افزاری سروری که به‌روزرسانی‌های اوبونتو را دیگر دریافت نمی‌کند. طراحی که مسئولیت بسته‌بندی آن‌را بر عهده داشت به ناگاه تصمیم گرفت کار خود را متوقف کند، در نتیجه ownCloud همچنان با آسیب‌پذیری‌ها تنها ماند. اوبونتو تنها یک نمونه کوچک در این زمینه بود. زمانی‌که تصمیم می‌گیرد از توزیع‌کنندگان کوچک لینوکسی استفاده کنید باید نهایت دقت را مبذول دارید. Manjaro توسعه مبتنی بر لینوکس، مدت زمان طولانی است که به‌روزرسانی‌های امنیتی را دریافت نکرده است. اگر از توسعه‌های کوچکی که توسط یک طراح برای تفریح ساخته شده است استفاده کنید، به مشکلاتی همچون مواردی که به آن‌ها اشاره کردیم مواجه خواهید شد. همین موضوع باعث می‌شود تا مصرف کنندگان در برابر مخاطرات جدی قرار گیرند.

امنیت سیستم‌های لینوکسی شکسته شده است

باید گفت سیستم لینوکسی شما آن‌گونه که تصور می‌کردید، ایمن نیست، رخنه‌های جدید نشان می‌دهند که این سیستم‌عامل آن‌گونه که باید نمی‌تواند در مقابل حملات ایستادگی کند. البته همه کامپیوترها در زمینه امنیت بد عمل می‌کنند. آن‌چنان‌که کوین نورتون در مقاله "همه چیز شکسته شده است" اشاره کرده است، بله، حتی لینوکس، و مهم‌تر از آن همه نرم‌افزارهای کامپیوتری که در فهرست برترین‌های لینوکس قرار دارند می‌توانند بر این سیستم‌عامل تأثیرگذار باشند. لینوکس همچنان با حفره‌های امنیتی به حیات خود ادامه خواهد داد و آسمان به زمین نخواهد رسید! سیستم لینوکسی شما هنوز در مقایسه با سیستم‌عامل‌های رومیزی شبیه به ویندوز از امنیت بیشتری برخوردار است. هکرها همچنان علاقه دارند به اهدافی که بر پایه سیستم‌عامل ویندوز مستقر شده‌اند حمله کنند. لینوکس در مقایسه با ویندوز از معماری امنیتی بسیار بهتری برخوردار است. البته لازم نیست بعد از خواندن این مقاله بلافاصله از نرم‌افزار ضد ویروس خود برای اسکن سیستم‌تان استفاده کنید، اما آگاه باشید به‌کارگیری لینوکس به این معنا نیست که نسبت به سیستم‌های دیگر در امنیت کامل قرار دارید. شبیه به سیستم‌های ویندوزی و مک، سیستم‌های لینوکس از

حفره‌های امنیتی زیادی پر شده‌اند. ما هنوز نتوانسته‌ایم همه آن‌ها را به‌طور کامل شناسایی کنیم. بنابراین بهتر است زمانی‌که درباره امنیت سیستم‌عامل لینوکس سخن به میان می‌آید فروتن باشید و سعی نکنید بدون دلیل از آن دفاع کنید. این احتمال وجود دارد که باگ Shellshock دیگری در چند قدمی شما قرار داشته باشد.

منبع:

پی‌سی‌ورلد

تاریخ انتشار:
21 شهریور 1394

نشانی منبع: https://www.shabakeh-mag.com/are-network/1532