امنیت USB دچار مشکل ریشه ای است - دیجیاتو

امیر صادقپور | شنبه، ۱۱ مرداد ۱۳۹۳

اغلب ما می دانیم که کول دیسک مان ممکن است به راحتی آلوده به ویروس یا بدافزار شود. و همه فکر میکنیم این مشکل با کمک یک آنتی ویروس یا فرمت کردن آن، رفع می شود. اما مشکل امنیت USB ها بسیار عمیق تر است. مهم نیست که با کمک چه ابزارها یا روش هایی آنها را پاکسازی می کنید، مشکل در نحوه کارکرد آنهاست.

در ادامه این مطلب با ما باشید تا از جزئیات بیشتری در خصوص این مشکل امنیتی در یواس‌بی ها آگاه شوید.

دو محقق به نام های Karsten Nohl و Jakob Lell ایراد امنیتی خطرناکی در این ابزارها یافته اند که نشان می دهد USBها در این زمینه از ریشه دچار مشکل هستند. آنها با نوشتن یک بد افزار به نام BadUSB که امکان ایجاد تغییر بر روی USB را دارد، نشان داده اند که می توانند به صورت ناشناس کنترل یک کامپیوتر را در دست بگیرند. در واقع این بد افزار الزاما نباید روی یک کول دیسک یا درایو یواس‌بی معمولی وجود داشته باشد، بلکه مشکل از سفت افزار کنترل کارکرد USBها است. بخشی که عملکرد آن را کنترل می کند. اثر کد نوشته شده توسط این دو، می تواند حتی در صورت پاکسازی کامل یک یواس‌بی توسط یک کاربر با دانش متوسط بر روی آن باقی بماند و به گفته سازندگان آن رفع اثر آن نیز ساده نیست.

به گفته نول و لِل در کنفرانس بلک هت در لاس و گاس، این مشکل با یک وصله امنیتی قابل حل نیست. چرا که آنها بر روی اغلب نسخه ها و مدل های موجود USB آن را آزمایش کرده اند. شرکت ها باید کاری در خصوص تولید یواس‌بی هاشان بکنند.

با دستکاری اطلاعات پایه و برنامه نویسی مجدد Firmware در یواس‌بی ها، می توان کارکرد عادی آنها را تغییر داد.
آقایان نول و لِل از محققان موسسه امنیت و مشاوره SR Labs، در مراحل اول کارشان بر روی سرعت شیوع اطلاعات یواس‌بی ها تحقیق کردند. همچنین این دو ماه ها با استفاده از مهندسی معکوس بر روی روش های برقراری ارتباط و کنترل سفت افزار ابزارهای مبتنی بر یواس‌بی -از جمله چیپ های کنترلی که اجازه انتقال اطلاعات را از کامپیوتر به یواس‌بی و برعکس را می دهند- کار کردند. در این تحقیقات آنها متوجه شدند که می توان راهی پیدا کرد که با دستکاری این اطلاعات

پایه و برنامه نویسی مجدد Firmware (سفت افزار یا میان افزار) این ابزارها، کارکرد آنها را تغییر دهند، طوری که پس از اعمال تغییرات، متخصصان آی تی هم پس از بررسی متوجه نشده و ابزار مربوطه را سالم و پاک به حساب آورند.

در این روش در واقع هیچ کدام از فایل هایی که روی یک کول دیسک ذخیره می شوند هدف یک ویروس یا بدافزار خاص قرار نمی گیرند. بلکه کدی آلوده در بطن مرکز کنترل کارکرد USB تعبیه می شود.

اما همانطور که اشاره شد، این مساله اصلا محدود به کول دیسک ها نمی شود. تمامی ابزارهایی که به نوعی از USB استفاده می کنند می توانند هدف حمله باشند. از کیبرد و ماوس گرفته تا پرینتر، اسکنر و حتی تلفن های هوشمند! سفت افزار USB تمامی آنها قابلیت برنامه ریزی مجدد را دارد. در آزمایشات انجام شده، حمله به یک تلفن همراه اندرویدی که از طریق یواس‌بی به کامپیوتر وصل بود شبیه سازی شده و نتیجه متاسفانه موفق بوده است.

اگر برایتان سوال پیش آمده که از این باگ امنیتی چه استفاده هایی می شود کرد باید بگوییم تقریبا هر کاری که خودتان می توانید با کامپیوتر انجام دهید و حتی هر کاری که کامپیوتر خودش می تواند انجام دهد از این طریق برای حمله کننده میسر است! دسترسی و کنترل غیرمجاز به کامپیوتر، های‌جک کردن ترافیک اینترنت، لاگ گیری کیبرد، تغییر دی‌ان‌اس، حمله MITM، جاسوسی ارتباطات قربانی و بسیاری موارد دیگر که ممکن است حتی به ذهنتان هم نرسد. تنها چیزی که مورد نیاز است دسترسی دو طرف (قربانی و حمله کننده) به اینترنت است.

با شیوع ویروس ها و بدافزارهایی که از طریق کول دیسک ها شیوع پیدا می کنند، بسیاری از ما تنها یاد گرفته ایم این کول دیسک ها یا فایل های مشکوک داخلشان را باز نکنیم. اما در خصوص این باگ، راهی معمول برای کشف مشکل یا پیشگیری از آن وجود ندارد.

شرکت های تولید کننده یواس‌بی ها، هیچ امضای مورد اعتمادی برای کدهای پیشفرضی که چیپ های کنترلی یواس‌بی ها را هدایت می کند ندارند.
مشکل اینجاست که شرکت های تولید کننده یواس‌بی ها، هیچ امضای مورد اعتمادی برای کدهای پیشفرضی که چیپ های کنترلی یواس‌بی ها را هدایت می کنند ندارند و بدین ترتیب می توان به راحتی کدهای آلوده و مخرب را بر روی آنها جایگزین کرد.

در تحقیقات نول و لِل مشخص شده که از لحاظ تئوری امکان سرایت این ایراد از کامپیوترها به سایر یواس‌بی ها و برعکس وجود دارد. به این معنی که هر زمان که یواس‌بی ای به یک کامپیوتر آلوده وصل می شود، بدون اینکه کسی متوجه شود، امکان جایگزین سفت افزار آلوده در آن وجود دارد. همین مساله در مورد اتصال یک یواس‌بی آلوده به یک کامپیوتر سالم نیز وجود دارد. سرایت دو طرفه، و به شدت قابل شیوع است. بدین ترتیب هیچکس نمی تواند و نباید به هیچکس دیگری اعتماد کند!

این دو قصد ندارند بدافزار BadUSB را که نوشته اند در کنفرانس بلک هت منتشر کنند چرا که نگران عواقب خطرناک آن و پخش سریعش هستند. اما آنها سعی کرده اند با آگاهی دهی به کاربران و شرکت ها، آنها را از این مشکل آگاه کنند. در این مرحله مهمترین مساله آگاهی و متقاعد شدن سازندگان از امکان بروز این مشکل است. و در صورتی که از سوی این سازندگان حرکت پیشگیرانه ای مشاهده نشود، عمر یواس‌بی برای تمام کسانی که به امنیت خود اهمیت می دهند سرآمده است.

البته در تماس های این دو محقق با یک سازنده تایوانی محصولات مرتبط -که نامش فاش نشده- به این مشکل اشاره شده که شرکت مربوطه عملی بودن آن را غیرمحتمل دانسته و به گفته های نول و لِل توجهی نکرده است. در حالی که نتیجه تحقیقات چیز دیگری نشان می دهد. البته نول معتقد است که این مشکل تنها در کوتاه مدت برقرار است و نهایتا سازندگان در خصوص پیشگیری از بروز آن اعمال لازمه را انجام خواهند داد. اما بهتر آن است که تا آن زمان تا حد ممکن از اتصال هر ابزار غیرقابل اعتمادی به پورت یواس‌بی کامپیوترتان اجتناب کنید. همچنین ابزارهای خودتان را هم به کامپیوترهای دیگران متصل نکنید. هر چند که این ابزارها ممکن است کاربرد حقیقی خود را با این رویه از دست بدهند.

تا اطلاع ثانوی بهتر است از یواس‌بی ها و پورت های یواس‌بی کامپیوتر خود با احتیاط بیشتری استفاده کنید.

دیجیاتو