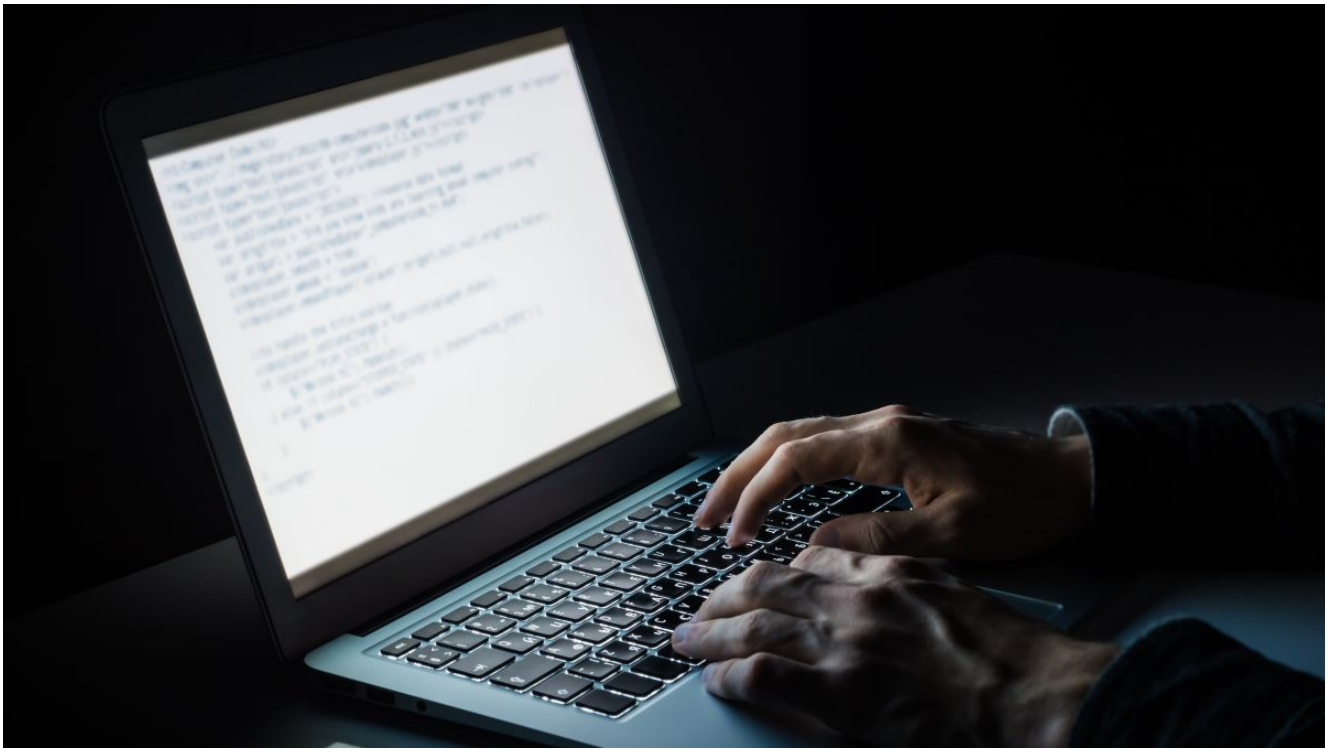
نفوذ یک محقق امنیتی به سیستم‌های اپل، مایکروسافت، تسلا و ۳۰ شرکت برجسته دیگر - دیجیاتو

یونس مرادی | جمعه، ۲۴ بهمن ۱۳۹۹

یک محقق امنیتی به نام «الکس بیرسان» با ایجاد اکسپلویت برای یک نقص در برخی اکوسیستم‌های متن باز، سیستم‌های ۳۵ شرکت سرشناس از جمله اپل، مایکروسافت، پی‌پل، شاپیفای، نتفلیکس، تسلا و اوبر را با موفقیت هدف گرفت.

این حمله شامل آپلود بدافزار در مخازن متن باز npm، PyPI و RubyGems بوده که پس از آن به صورت خودکار در اپ‌های داخلی شرکت‌ها توزیع شده است. در واقع بدون نیاز به مهندسی اجتماعی یا استفاده از تروجان، بسته‌های مخرب توسط قربانی‌ها دریافت شده است؛ مشکلی که ناشی از نقص طراحی خاصی با عنوان «سردرگمی وابستگی» است.

بیرسان پروژه‌های جعلی را با استفاده از اسامی مشابه مخازن ساخته و دریافته بود که بدون نیاز به انجام هیچ کاری از سوی توسعه دهنده اپلیکیشن‌ها به صورت خودکار بسته‌های وابستگی عمومی را دریافت می‌کنند. در برخی موارد مثل بسته‌های PyPI هر پکیجی که دارای نسخه بالاتر بود، فارغ از مکان آن در اولویت قرار می‌گرفت. همین مساله به بریسان اجازه داد زنجیره تامین نرم‌افزاری چند شرکت را با موفقیت هدف بگیرد.



بریسان پس از اطمینان از اینکه اکسپلویت به نفوذ موفق در شبکه منجر شده، شرکت‌های مورد نظر را در جریان گذاشته و تعدادی از آنها نیز به عنوان باگ‌بانتی به وی پاداش داده‌اند. برای مثال مایکروسافت نه تنها به وی بالاترین میزان باگ‌بانتی خود یعنی ۴۰ هزار دلار پاداش داده بلکه مقاله‌ای را هم در این رابطه منتشر کرده است.

اپل هم قرار است به خاطر افشای مسئولانه این حفره پاداشی را به وی اهدا کند. بریسان در مجموع تا کنون ۱۳۰ هزار دلار جایزه از این طریق دریافت کرده و به عنوان یکی از محققان امنیتی برجسته شناخته می‌شود.

دیجیاتو