禪

[illegible]

[illegible]

[illegible] Honeywell [illegible]

[illegible] Honeywell [illegible] Honeywell [illegible]

[illegible] 40 [illegible] …[illegible]

Synack

Dropcam NEST Synack

هکرها میتوانند شروع به فروش دستگاههای هوشمند پیشپیکربندی در بازار سیاه کنند و بعد با کمترین مهارت و اکسپلویت از آسیبپذیریهای دیگر دستگاهها استفاده کنند . مور میگوید تاکنون دیده یا شنیدهام که نشانی IP محلی دوربینهای نظارتی درون یک پارکینگ، گاراژ، باغ و مانند اینها توسط هکرها جستوجو و اسکن شود تا براساس آنها بتوانند الگو و برنامه کاری و زندگی اهالی خانه را کشف کنند و بفهمند چه زمانهایی خانه هستند و چه زمانهایی خانه را ترک میکنند . این اطلاعات به سرقتهای هوشمندانه کمک میکند. روش دیگر، خراب کردن یا مشکلدار کردن دستگاهی مانند دوربین و نصب بدافزار و دستکاری آن در هنگام تعمیر است .

حتی هکرها میتوانند دستگاههای هوشمند و دوربینهای نظارتی را قبل از اینکه به دست کاربر برسد، خریداری و با نصب بدافزار دوباره بستهبندی کنند و در بازار بفروشند . مور و همکارانش این نوع حملات را آزمایش کردند . چند دوربین نظارتی معروف از بازار خریداری و با دستکاری و تغییر آنها مشابه روز نخست بستهبندی کردند و در بازارهای آنلاینی مانند eBay به همکاران فروختند . نتیجه آزمایش این بود که تفاوت محصولات بسیار کم است و هیچکس متوجه نخواهد شد.

دسته بندی:
امنیت
تاریخ انتشار :
03:15 - 30/02/1394
برچسب:
هک - اینترنت اشیا - IoT

□□□□□ منبع: https://www.shabakeh-mag.com/security/656