

- **مدیرمسئول:** محمدامین ایمانجانی
- **قائم‌مقام مدیرمسئول:** مسعود فروغی
- **سرمدیر:** محمد زعیم‌زاده
- **دبیر وقایع اسرائیلیه:** محمدصادق علیرزاده
- **تلفن و فکس:** ۶۲۹۹۴۹۵ (۰۲۱)
- **کدپستی:** ۱۱۳۵۶۳۳۸۱۶
- **جاب:** چاپخانه دانشگاه آزاد اسلامی
- **نشانی:** خیابان حافظ، پایین‌تر از جمهوری، روبه‌روی ساختمان بورس ساختمان فرهیختگان، طبقه سوم

چگونه اپلیکیشن‌ها به ابزارهای جاسوسی و درآمدزایی رژیم اسرائیل بدل شدند؟

کلیک‌هایی در خدمت جنگ



ناعمه اصفهانیان

در پشت چهره بی‌خطر صدها اپلیکیشن محبوب اندروید و آیفون، از ویرایشگرهای عکس و ویدئو گرفته تا بازی‌ها و ابزارهای روزمره، ردپای توسعه‌دهندگانی دیده می‌شود که پیش‌تر در واحدهای سایبری و جاسوسی ارتش رژیم اسرائیل فعالیت داشته‌اند. این اپ‌ها که

میلیاردها بار در جهان دانلود شده‌اند، بی‌سروصدا به چرخ اقتصادی رژیم خدمت می‌کنند؛ رژیمی که متهم به نسل‌کشی و جنایت‌های جنگی است. کاربران، بی‌خبر از پشت پرده این محصولات، داده‌های شخصی خود را در اختیار ساختارهایی قرار می‌دهند که اغلب هویت مالکان واقعی‌شان در هاله‌ای از ابهام پنهان است.

جاسوس‌ها در کمین

تحقیقات تازه نشان می‌دهد پشت پرده بسیاری از اپلیکیشن‌های پرطرفدار در فروشگاه‌های Google Play و App Store، توسعه‌دهندگانی قرار دارند که پیش‌تر در ارتش و سازمان‌های اطلاعاتی اسرائیل فعالیت داشته‌اند. این کشف، زنگ هشدار را درباره سوءاستفاده از داده‌های کاربران، نقض حریم خصوصی و پیوند پنهان فناوری‌های روزمره با ماشین جنگی و سیاست‌های اشغال‌گرایانه رژیم اسرائیل به صدا درآورده است. اما کدام اپلیکیشن‌های محبوب، بیشترین نقش را در این شبکه پرابهام بازی می‌کنند؟

ZipoApp: یکی از بازیگران اصلی

یکی از بازیگران کلیدی پشت پرده اپلیکیشن‌های پرمخاطب اسرائیلی، شرکت Zipo Apps است. این شرکت با مدل کاری مشخصی فعالیت می‌کند؛ خرید اپلیکیشن‌های پر پتانسیل و سپس تجاری‌سازی آن‌ها در مقیاس جهانی. محصولات تحت مالکیت Zipo شامل مجموعه‌ای از ابزارهای ویرایش عکس و ویدئو است که در مجموع صدها میلیون بار روی گوشی‌های کاربران نصب شده‌اند؛ اپ‌هایی مانند Collage Maker Photo Editor که بیش از ۵۰ میلیون بار تنها در گوگل پلی دانلود شده‌اند. سایر اپ‌های این مجموعه نیز به ویرایش تصاویر، نوزاد، روتوش چهره و افزودن جلوه‌های بصری اختصاص دارند.

در سال ۲۰۲۲، گال آویدور، مدیرعامل و بنیان‌گذار Zipo، در نخستین و تنها گفت‌وگوی رسانه‌ای‌اش اعلام کرد که تمام بنیان‌گذاران شرکت از اعضای سابق واحد اطلاعاتی ۸۲۰۰ ارتش اسرائیل بوده‌اند، واحدی که مسئول عملیات‌های گسترده‌شوند، جاسوسی سایبری و تحلیل داده در سطح منطقه‌ای است. Zipo Apps اکنون یکی از نمادهای پیوند میان فناوری محبوب مصرف‌کننده و ساختار اطلاعاتی - نظامی اسرائیل به شمار می‌رود، پیوندی که اغلب در سایه و به دور از آگاهی عمومی کاربران شکل می‌گیرد.

Bazaar: ابزار ویرایش عکس

بایستوانه امنیتی اسرائیل

یکی دیگر از اپلیکیشن‌های پرطرفدار حوزه ویرایش عکس که ردپای رژیم اسرائیل در آن مشهود است، Bazaar نام دارد؛ محصولی که با ظاهر فریبنده و کاربردی‌اش، میلیون‌ها بار توسط کاربران در سراسر جهان دانلود شده است. اما پشت این اپ به ظاهر بی‌ضرر، چهره‌ای امنیتی و نظامی نهفته است. Bazaar توسط دروهر و استاس گوفمن تأسیس شده؛ دو افسر سابق ارتش رژیم صهیونیستی (IDF) که تجربه فعالیت اطلاعاتی در ساختار امنیتی اسرائیل را در کارنامه دارند. استاس گوفمن، به‌ویژه، فراتر از خدمت سربازی اجباری، حدود یک دهه در ارتش اسرائیل باقی مانده و تا سال ۲۰۱۱ در پروژه‌های اطلاعاتی خدمت کرده است.

Facetune: اپلیکیشن پرحاشیه ویرایش چهره

Facetune، توسعه یافته توسط شرکت اسرائیلی Lightricks، برای اندروید و آیفون در دسترس است و بیش از ۵۰ میلیون بار دانلود شده است. برخی کاربران در فروشگاه اپل این برنامه را کلاهبرداری خوانده‌اند، زیرا برای عملکرد کامل خود نیاز به دسترسی به شناسه‌های منحصر به فرد کاربران و موقعیت مکانی دارد. یارون اینگر، یکی از هم‌بنیان‌گذاران Lightricks، پنج سال در واحد ۸۲۰۰، واحد سایبری فوق‌محرمانه ارتش رژیم اسرائیل خدمت کرده است.

Moovit؛ با ظاهر خدمات شهری

اما پیوندی عمیق با ارتش عبری

Moovit اپلیکیشن حمل‌ونقل شهری است که در سطح جهانی محبوب شده و بیش از یک میلیارد کاربر دارد. بسیاری ممکن است ندانند که این اپ نیز توسط اعضای سابق ارتش رژیم اسرائیل تأسیس شده است. از جمله بنیان‌گذاران آن نیر ارز (Nir Erez) است که سال‌ها در مرکز تخصصی رایانه‌ای ارتش به نام مامرام (Mamram) فعالیت کرده است. مامرام بخشی از ساختار سایبری ارتش عبری است که در تبلیغات رسمی به عنوان «ترتیب‌کننده جنگجویان سایبری» شناخته می‌شود. این واحد که مدیریت اینترنت نظامی ارتش را در اختیار دارد، در طراحی و اجرای حملات دیجیتالی و جمع‌آوری داده‌ها علیه فلسطینی‌ها نقش کلیدی دارد. Moovit شریک رسمی بسیاری از رویدادهای بین‌المللی از جمله بازی‌های المپیک، مسابقات فوتبال اروپا (یورو) و کمپانی مایکروسافت است که با آن همکاری فنی دارد. این مشارکت هابه مشروعیت بخشی جهانی به محصولات نظامی دولت عبری کمک کرده و کانال‌هایی برای توسعه درآمد‌های بین‌المللی برای اقتصاد جنگی رژیم فراهم می‌کنند.

Call App: برای شناسایی تماس‌های اسپم

باصدها میلیون نصب، Call App یکی دیگر از محصولات اقتصاد نظامی رژیم اسرائیل است. بنیان‌گذار و مدیرعامل Call App، آمیت آن (Amit On)، در دهه اول سال ۲۰۰۰ به مدت سه سال در واحد ۸۲۰۰ ارتش خدمت کرده است. این اپلیکیشن اکنون بیش از ۱۰۰ میلیون کاربر دارد.

Gett؛ جابه‌جایی امن اما ناامن

در حوزه حمل‌ونقل هوشمند، Gett که تمرکزش روی جابه‌جایی شرکتی است و به‌ویژه در لندن برای گرفتن تاکسی‌های مشکی محبوب است، توسط روی مور (Roi More) و شاهار وایز (Shahar Waiser)، دو عضو سابق واحد ۸۲۰۰ تأسیس شده است. همچنین نیاید از Waze غافل شد؛ اپلیکیشن معروف مسیریابی که احتمالاً مشهورترین اپ اسرائیلی دهه گذشته است، ویز در سال ۲۰۱۳ با قیمت ۱.۳ میلیارد دلار توسط گرگل خریداری شد و بنیان‌گذاران آن نیز جاسوسان سابق واحد ۸۲۰۰ بوده‌اند.

Fooducate: رژیم غذایی در خدمت نسل‌کشی

یکی دیگر از اپلیکیشن‌های در حال رشد سریع اسرائیلی که در برنامه اپرا، نیویورک تایمز و CNN معرفی شده، Fooducate است که یک اپلیکیشن پیگیری رژیم غذایی ست. بنیان‌گذار آن، همی وینگارتن (Hemi Weingarten)، مأموریت‌های بمباران رابرای نیروی هوایی رژیم اسرائیل انجام داده است.

جذب سرمایه خارجی

بیشتر این اپ‌ها، با برند «نوآوری اسرائیلی» در کشورهای غربی (به‌ویژه آمریکا) ثبت شده‌اند، اما توسعه و مدیریت فنی‌شان در رژیم اسرائیل انجام می‌شود. این شرکت‌ها از صندوق‌های سرمایه‌گذاری بزرگ (VC) آمریکایی، اروپایی و حتی آسیایی ده‌ها میلیون دلار سرمایه اولیه جذب کرده‌اند. برای مثال Facetune بیش از ۲۰۰ میلیون دلار سرمایه جذب کرده است. Moovit تا پیش از خرید توسط اینتل، ۱۳۳ میلیون دلار از سرمایه‌گذاران جهانی دریافت کرده بود و Gett بیش از ۸۵۰ میلیون دلار جذب کرد تا به اویر اسرائیلی تبدیل شود. این سرمایه‌گذاری‌ها نه تنها برای توسعه این اپ‌هاست، بلکه زیرساخت فناوری اطلاعات، کارمندان اسرائیلی و فضای سایبری بومی را تأمین مالی می‌کنند. از سوی دیگر، اکثر این اپ‌ها دارای نسخه‌های پولی هستند و کاربران از کشورهای مختلف، به‌ویژه اروپا و آمریکا، هزاران دلار در روز برای اشتراک در این اپ‌ها می‌پردازند. Facetune، Call App، Collage Maker و Bazaar در لیست پردرآمدترین اپ‌های ویرایش عکس و ارتباطی قرار دارند. Gett در بخش حمل‌ونقل شهری فعالیت کرده و سهم بازار قابل توجهی در تل‌آویو، لندن و نیویورک دارد. Fooducate و Moovit از طریق داده‌کاوی و تحلیل داده کاربران برای شرکت‌های بیمه، خرده‌فروشی یا حمل‌ونقل نیز درآمد کسب می‌کنند. این درآمدها مستقیماً یا از طریق شرکت‌های واسطه، وارد اقتصاد اسرائیل می‌شوند؛ مالیات پرداخت می‌شود و شرکت‌ها توسعه می‌یابند.

تقویت «اکوسیستم نظامی-فناورانه» اسرائیل

بسیاری از مؤسسان این اپ‌ها، پیش‌تر عضو یگان ۸۲۰۰ یا دیگر نهادهای سایبری ارتش رژیم بوده‌اند و تجربه‌شان در جمع‌آوری داده، شنود، تحلیل کلان‌اطلاعات و رمزگشایی، در این شرکت‌ها به کار گرفته می‌شود. در نتیجه، بخش بزرگی از درآمد این شرکت‌ها، وارد چرخه‌ای می‌شود که در آن نیروی انسانی متخصص سایبری تقویت می‌گردد، فناوری جدید تولید می‌شود و نهایتاً به نهادهای نظامی و امنیتی اسرائیل خدمت می‌کند. طبق گزارش‌هایی مانند گزارش Start-Up Nation Central و تحقیقات دانشگاهی، فناوری‌های غیرنظامی (مثل اپلیکیشن‌ها) بیش از ۱۵ درصد از GDP اسرائیل را تشکیل می‌دهند و بخش بزرگی از بودجه‌های اطلاعاتی/امنیتی با درآمد‌های حاصل از این بخش تأمین می‌شود.

سخن پایانی

گزارش‌های گویند اعضای سابق واحد ۸۲۰۰ اکنون در شرکت‌های بزرگ فناوری مانند متا، گوگل، اپل، آمازون، مایکروسافت و OpenAI (که به عنوان پیشروترین شرکت هوش مصنوعی جهان شناخته می‌شود) مشغول به کار هستند و این بیش از پیش نشان می‌دهد که نفوذ رژیم اسرائیل تا چه حد عمیق و پنهانی در زندگی دیجیتالی در تمام دنیاریشه‌دوانده است. این تحقیقات هم‌چنین فاش می‌کنند که رژیم به‌طور نیایدی وابسته به حفظ سلطه دائمی بر فلسطینی‌هاست، زیرا تنها چیزی که این رژیم به‌طور واقعی تولید می‌کند، شرکت‌های فناوری‌ای هستند که توسط اعضای سابق ارتش (IDF) تأسیس شده‌اند. نکته تکان‌دهنده در تحقیقات جدید این است که واحد ۸۲۰۰ ارتش اسرائیل، بخش بسیار محرومانه جنگ سایبری، در حال توسعه سیستم‌های پیشرفته هوش مصنوعی است که در تسهیل نسل‌کشی رژیم عبری در غزه نقش دارند.