# ثلاثية "ثغرات السيادة"

20 يونيو 2025

تقنية وذكاء اصطناعي

7 دقيقة قراءة

www.saudieinstein.com

## ثلاثية "ثغرات السيادة"



هذا المقال هو الجزء الأول من ثلاثية "ثغرات السيادة" – سلسلة تحليلية تكشف كيف تتسلل الشركات الأجنبية إلى عمق الأجهزة العربية: من سامسونغ، إلى شبكات Mossad–RAW، إلى فجوة التوطين الرقمي

——— الجزء الأول حين وقّعت سامسونغ عقدًا مع حصان طروادة هكذا دخل التطبيق الإسرائيلي AppCloud إلى هواتف العرب... ورفض المغادرة في الاتفاقات التقنية ما يشبه الزواج السرّي: يُعقد في الظلام، وتظهر نتائجه في النور. هكذا كان الأمر حين وقّعت سامسونغ، في 2022، عقدًا مع شركة إسرائيلية تُدعى IronSource، سمحت لها

بموجبه بتثبيت تطبيق اسمه AppCloud على ملايين الهواتف في منطقتنا. والحال أنّ التطبيق المذكور ليس كسائر التطبيقات التي نعرفها ونختار تحميلها؛ إنه يُزرع في الجهاز كما تُزرع أجهزة التنصّت في الجدران، خفيّاً وصامتاً ودائماً. ذاك أنّ AppCloud لا يظهر على شاشتك، ولا يطلب إذنك، ولا يُعلمك بوجوده أصلاً. يعمل في الخلفية كموظف استخبارات مجتهد: يجمع المعلومات، يرصد السلوكيات، يقترح التطبيقات، ويرسل بياناتك إلى خوادم لا تعرف أين تقع ولمن تتبع. والأنكى أنه حتى لو اكتشفت وجوده وحاولت حذفه، فإنه يعود؛ كحصان طروادة الذي دخل المدينة مرّة، فأحرقها إلى الأبد. بيد أنّ الأسئلة الحقيقية تبدأ

من هنا: لماذا اختارت سامسونغ، من بين آلاف الشركات التقنية في العالم، شركة إسرائيلية بالذات؟ ولماذا قصرت هذا التعاون على منطقة الشرق الأوسط وشمال إفريقيا دون سواها؟ ولعلّ الأكثر إثارة للريبة: لماذا على هواتف الفئات المتوسطة والرخيصة حصراً؟ والحال أنّ IronSource ليست شركة تقنية بريئة كما قد يُخيّل للبعض. سجلّها حافل بتطوير برمجيات صُنّفت لاحقاً كخبيثة، تتسلّل إلى الأجهزة وتجمع البيانات دون علم أصحابها أو موافقتهم. حتى أنّ Unity، حين استحوذت عليها في 2022، واجهت ثورة من المطورين الذين يعرفون سمعتها السوداء. لكنّ الأخطر من ذلك كلّه ما كشفته تحقيقات صحفية عن ارتباطات وثيقة بين

مـوظفين بـارزين فـي الشركـة ووحـدة الاستخبارات العسكرية الإسرائيلية 8200، تلك الوحدة المتخصصة في التجسّس الإلكتروني والحرب السيبرانية. يلوح السؤال هنا أكثر إلحاحاً: كيف نأتمن شركة بهذه الخلفية على بيانات ملايين المواطنين العرب؟ وإذ نتحدّث عن الوحدة 8200، لا يسعنا إلا استذكار ما فعلته إسرائيل بحزب الله في سبتمبر 2024. يومها، انفجرت آلاف أجهزة البيجر في أيدي عناصر الحزب وجيوبهم؛ تسع سنوات من التخطيط والتنفيذ لتحويل أداة اتصال بسيطة إلى قنبلة موقوتة. الموساد أقنع الحزب بشراء أجهزة آمنة من شركات وهمية، فيما كانت مصانعه هو من ينتجها محشوّة بالمتفجرات. راهناً، وبعد أن قتلت

العملية العشرات وجرحت الآلاف، يتساءل المرء: إذا كان هذا ما يفعلونه بأجهزة البيجر البدائية، فماذا يمكن أن يفعلوا بهواتفنا الذكية المتطورة؟ لئن كان التطبيق يعمل بصمت، فإنّ طريقة زرعه تنطق بكلّ شيء. يُثبّت AppCloud تلقائياً أثناء إعداد الهاتف لأول مرة، دون أن يُخيّر المستخدم أو حتى يُخبر. وإذ يحاول البعض حذفه، يكتشفون أنه محميّ بامتيازات النظام؛ كأنه جزء أساسي من الهاتف لا يمكن الاستغناء عنه. أغلب الظنّ أنّ اختيار منطقتنا تحديداً لم يكن اعتباطياً. ففي أوروبا، حيث قانون حماية البيانات العامة (GDPR) يفرض عقوبات صارمة على منتهكي الخصوصية، وفي الولايات المتحدة، حيث المستهلك يقاضي ويحاسب،

وحتى في كوريا الجنوبية، موطن سامسونغ نفسها، لا أثر لهذا التطبيق المشبوه. أما نحن، سكّان المنطقة الرخوة قانونياً، فصرنا حقل تجارب مفتوحاً للشركات التي تخشى المساءلة في بلدانها؛ كما صرنا حقل تجارب للاستعمار ذات يوم، وللديكتاتوريات بعد ذلك، وللإرهاب لاحقاً. التاريخ يُعيد نفسه، لكن بأدوات رقمية هذه المرّة. وإذ نتساءل عن دور الجهات الرقابية، نصطدم بصمت مريب. جهاتنا الرقابية؟ مشغولة، كالعادة، بأمور أهمّ: حجب المواقع الاباحية، رفع قضايا على التغريدات النقدية للوزارات، مناقشة تصميم انفوجرافك عن انجازات التحول الرقمي والأمن السيبراني. أمّا شركة إسرائيلية تتجسّس على ملايين المواطنين؟ تفصيل صغير لا

يستحقّ الاهتمام. إن كانت هذه الجهات تعلم بالأمر وتغضّ الطرف، فتلك خيانة للأمانة؛ وإن كانت لا تعلم، فتلك غفلة لا تُغتفر. في الحالتين، نحن أمام فشل ذريع في حماية الأمن الرقمي الوطني. لعلّ المفارقة الأكثر إيلاماً أننا نتحدّث عن السيادة الرقمية والتحوّل الرقمي واقتصاد المعرفة، فيما أبسط حقوقنا الرقمية مُنتهكة بموافقة ضمنية من شركات نثق بها. كأنّ الثقة نفسها صارت سلعة رخيصة، تُباع وتُشترى في سوق التطبيع التقني الصامت. تطبيع لا يحتاج لمصافحات أو اتفاقيات معلنة؛ يكفيه تطبيق خفيّ في هاتفك.

والحال أنّ الخطر لا يكمن في AppCloud وحدها، بل فيما يمثّله من نموذج جديد للاختراق:

ناعم، مُقنّن، يدخل من الباب لا من النافذة. اليوم تطبيق تسويقي يجمع بيانات الاستهلاك؛ غداً بوابة خلفية تتسرّب منها معلومات أكثر حساسية. اليوم نتحدث عن تفضيلات المستخدم؛ غداً قد نتحدث عن أسرار أمنية أو معلومات استراتيجية.

إنّ الذي سمح لـ IronSource بالتسلّل دون مساءلة، هو نفسه الذي سيسمح لغيرها بالولوج؛ ما دامت البوابات مشرّعة والحرّاس نائمون.

راهناً، ثقّة حاجة ماسّة لتحقيق وطني شامل في هذه القضية. يبدأ بحظر التطبيق فوراً. يمرّ بمطالبة سامسونغ بتفسير واضح وخطة محدّدة لإزالته من جميع الأجهزة -فورًا- مع عقوبات

حازمة. ينتهي بوضع ضوابط صارمة على التطبيقات المُثبّتة مسبقاً. التطبيقات يجب أن تكون: معلنة. قابلة للحذف. مُراجَعة أمنياً. وإلاّ فلا.

بيد أنّ المشكلة أعمق. إنها ثقافة الاستسلام الرقمي. نقبل الشروط دون قراءتها. نمنح الأذونات دون تفكير. نسمح بانتهاك خصوصيتنا مقابل خدمات مجانية ندفع ثمنها من حرياتنا وكرامتنا.

وكأننا، في عصر المعلومات، اخترنا أن نكون آخر من يعلم. وفي زمن الحقوق الرقمية، رضينا أن نكون الأكثر انتهاكاً. كأنّ قدرنا أن نكون دائماً في ذيل القافلة، سواء كانت قافلة التحرّر السياسي أم قافلة التحرّر الرقمي.

قـد يكـون AppCloud، فـي نهايـة المطـاف، مجـرد تطـبيق تسـويقي مزعـج لا أكثـر. لكـنّ الطريقة التي دخل بها، والجهة التي تقف خلفه، والصمت الذي يحيط به، كلّها تشير إلى أننا أمام نمط جديد من الاحتلال: احتلال رقمي، صامت، يتسلّل عبر الأسلاك والموجات، ويحتلّ العقول قبل الأرض.

أم أنّنا، كالعادة، ننتظر أن يحتلّونا رقمياً كما احتلّونا أرضياً؟