مصطفى أحمد | نشر في ١٨ سبتمبر ٢٠٢٤,

من جهاز اتصال إلى قنبلة موقوتة.. كشف لغز انفجار أجهزة البيجر بعناصر حزب االله

في ظل تغيرات متسارعة يشهدها عالمنا الحالي وتحديدًا في المجال التقني، لم تعد الأجهزة القديمة بمنأى عن الاختراق. وأحدث دليل على ذلك إصابة المئات من عناصر "حزب االله" اللبناني، بعدما استطاع الاحتلال الإسرائيلي اختراق وتفجير جهاز الاستدعاء القديم المعروف باسم البيجر، الذي يعتمدون عليه في التواصل فيما بينهم.

لكنّ هناك لغزًا محيرًا أثار جدًلا واسعًا لدى الكثيرين، وهو كيف استطاع الكيان الصهيوني اختراق هذا الجهاز القديم وتفجيره عن بعد.

لا عليك، من أجل فهم أعمق للقصة وما حدث، سنستعرض خلال السطور التالية الجوانب التقنية وكافة السيناريوهات المحتملة التي مكّنت "إسرائيل" من اختراق وتفجير أجهزة البيجر التي يستخدمها "حزب االله".

تفجير البيجر في لبنان

انفجرت العديد من أجهزة النداء (البيجر) التابعة لعناصر "حزب االله" في جميع أنحاء لبنان أمس الثلاثاء، ما أسفر عن مقتل 12 أشخاص على الأقل -حتى الآن- وإصابة أكثر من 2800 شخص من بينهم أطباء ومهندسين مدنيين، وذلك في محاولة استهداف واضحة وصريحة من قبل الكيان الصهيوني لجماعة "حزب االله".

ووقعت الانفجارات في عدة مناطق من لبنان، بما في ذلك العاصمة بيروت ومدينة صور الجنوبية ومنطقة الهرمل الغربية. وانتشرت صور وفيديوهات على وسائل التواصل الاجتماعي لانفجارات وأشخاص

مصابين في مناطق مختلفة بأجسادهم، مثل جيوبهم أو آذانهم أو وجوههم، وتم نقلهم إلى المستشفى لتلقي العلاج اللازم.

ما هي أجهزة البيجر وكيف تعمل؟

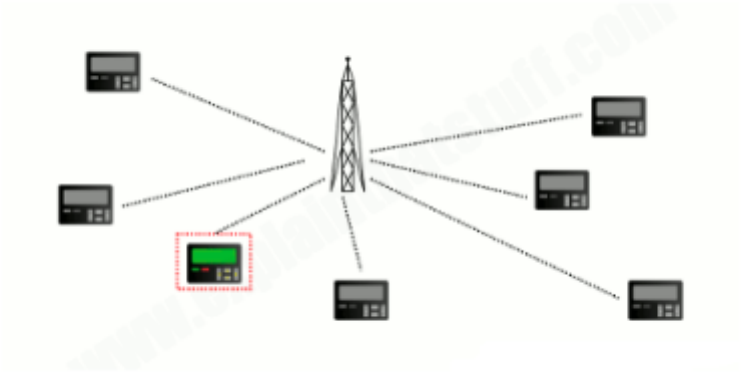
أحد إصدارات أجهزة البيجر – المصدر: Image Getty

قبل ظهور الهواتف المحمولة ومقاطعة حياتنا، كان هناك شكل آخر من أشكال نظام الرسائل الفورية يسمّى البيجر (Pager) أو جهاز النداء اللاسلكي أو الاستدعاء.

اخترع البيجر المهندس الكندي ألفريد غروس في عام 1949، وقد شاع استخدامه في أواسط تسعينيات القرن الماضي، حيث وصل عدد المستخدمين إلى أكثر من 61 مليون مستخدم. مع ظهور الهواتف المحمولة، أصبحت أجهزة البيجر أقل شعبية ممّا كانت عليه، ليصل عدد مستخدميها إلى نحو 6 ملايين مستخدم في عام 2016.

لكن البيجر لا يزال أحد الأجهزة المهمة للغاية، خاصة للأطباء وعمال الطوارئ والأمن، لما يوفره من إمكانية اتصال بينهم وبين بعضهم من دون ضجيج، حفاظًا على الهدوء اللازم للمرضى من ناحية، بالإضافة إلى عدم إلحاق أي ضرر على الأجهزة الطبية بسبب ذبذبات الهواتف الذكية.

تتلقى أجهزة البيجر التنبيهات والرسائل النصية القصيرة من خلال موجات ترددات الراديو من محطة أساسية أو مركز إرسال مركزي، يمكن أن تكون هذه الرسائل على شكل أرقام أو حروف.



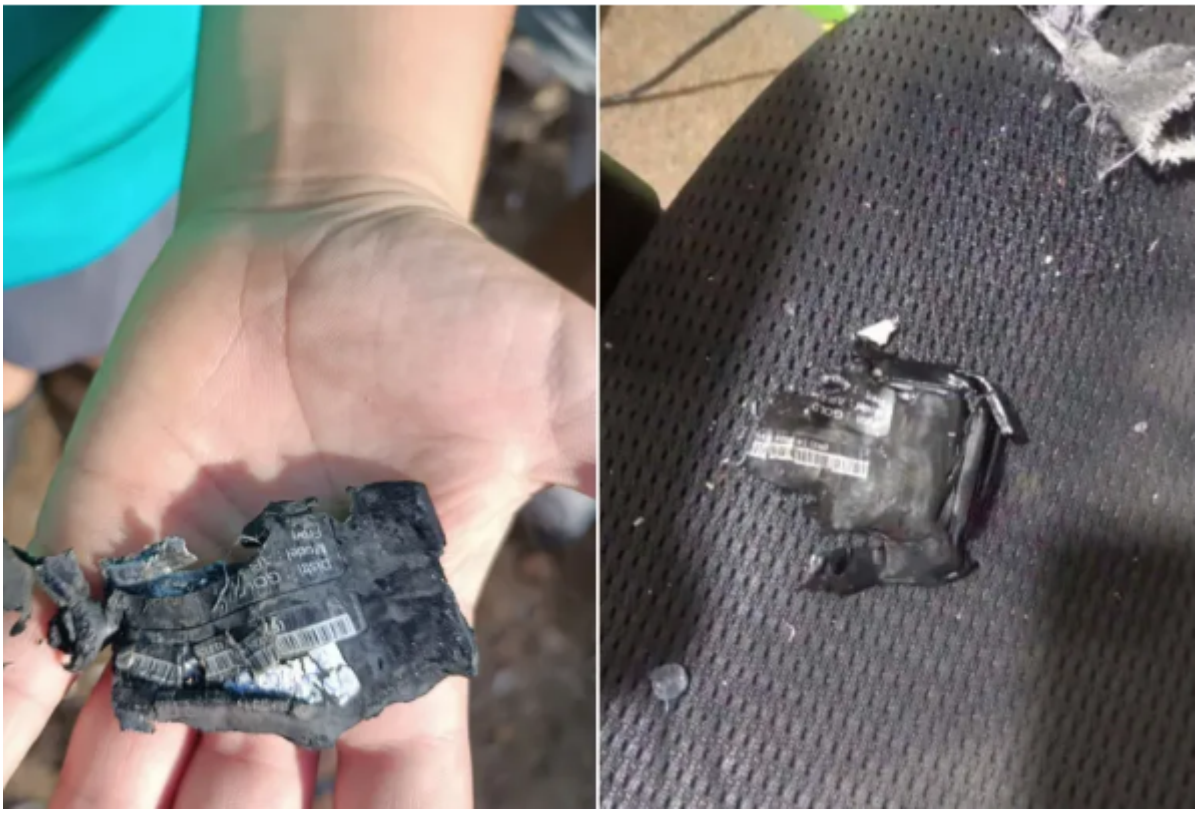
ما يميز جهاز النداء أنه يصدر نغمة أو صوتًا أو حتى اهتزاز لتنبيه المستلم بوجود رسالة، ولهذا يتم الاعتماد على البيجر في المستشفيات، وكذلك بين عناصر الإنقاذ في حالات الطوارئ.

ما السبب المحتمل لانفجار أجهزة البيجر ؟

الآن بعد أن تعرّفنا على ماهية جهاز البيجر وطريقة عمله، نأتي هنا للسؤال الأهم: ما الكيفية المحتملة لانفجار جهاز النداء لدى عناصر "حزب االله"؟

السيناريو الأول

وفقًا للمعلومات المتداولة، يعتمد "حزب االله" على أجهزة البيجر التي تعمل عبر بطاريات ليثيوم أيون، التي تتميز بخفة وزنها وطول عمرها وكفاءتها في استهلاك الطاقة، لكن على ما يبدو استغل الاحتلال الإسرائيلي عيبًا خطيرًا في تلك البطاريات، وهي الحرارة الزائدة التي تعتبر أكبر عدو لبطاريات ليثيوم أيون.



بقايا أحد أجهزة البيجر المنفجرة في عدة مناطق بلبنان – المصدر: منصات التواصل الاجتماعي

عندما ترتفع الحرارة بشكل أكبر من الطبيعي، يمكن أن يؤدي الأمر إلى انفجار البطارية، وهذا يحدث في العديد من الهواتف الذكية الحديثة.

وعلى ما يبدو، ووفقًا لمصادر مقربة من "حزب االله" لـ"أسوشيتد بريس"، فإن الاحتلال لم يخترق أجهزة البيجر لأنها قديمة جدًا، لكنه استطاع اختراق بطارية الليثيوم أيون، أو بمعنى أدق تمّ اختراق الخادم الخاص بأجهزة "حزب االله"، ومن ثم تحميل سكريبت أو نص برمجي معيّن، الأمر الذي تسبّب في زيادة الضغط على البطارية ومن ثم ارتفاع الحرارة بشكل كبير.

يمكن أن تنفجر بطارية ليثيوم أيون عند درجات حرارة تصل إلى 1100 درجة فهرنهايت (590 درجة مئوية)، لكن الأسوأ من ذلك هو أنها تدخل في مرحلة تسمّى "الهروب الحراري (Thermal Runaway)" عند درجة حرارة أكثر انخفاضًا، إذ تؤدي قد النقطة هذه عند .مئوية درجة 130 وهي، التفاعلات الكيميائية الداخلية إلى ارتفاع سريع في درجة الحرارة، وهو ما يؤدي في النهاية إلى انفجار البطارية.

وهكذا تسبّب الأمر في انفجار البطارية والجهاز. بالنسبة إلى الأضرار الجسدية، فهي متفاوتة من شخص إلى آخر، حيث يمكن أن تكون الأضرار خفيفة إذا كان البيجر بعيدًا عن جسم الشخص، وقد تكون مميتة في حال كان الجهاز ملتصقًا بجسم الشخص.

يمكن دحض هذا السيناريو ببساطة، حيث تعتمد بعض البطاريات على برامج الأجهزة الخاصة لتنظيم الاستخدام ودرجة الحرارة، لذلك من الممكن نظريًا اختراق جهاز النداء وتحفيز بطاريته على التسخين إلى الحد الذي تنفجر فيه. في الوقت نفسه، تُظهر مقاطع الفيديو التي تمّ نشرها على الشبكات الاجتماعية أن أجهزة البيجر انفجرت على الفور في وقت واحد، بدلًا من الاشتعال، لذا قد يكون السيناريو الثاني هو الأرجح.

السيناريو الثاني

في حال كنت غير مقتنع بالسيناريو الأول، وما زلت تتساءل كيف انفجرت المئات من أجهزة البيجر في وقت واحد، هناك سيناريو آخر أكثر إقناعًا، ومفاده أن الاحتلال قد عبث بأجهزة البيجر واخترقها في مرحلة ما من سلسلة التوريد، قبل أن تصل تلك الأجهزة اللاسلكية إلى عناصر "حزب الله".

هذه الرواية أكثر إقناعًا، ذلك لوجود معلومات نشرتها صحيفة "وول ستريت جورنال" الأمريكية وأكدت عليها "نيويورك تايمز"، تقول إن هناك شحنة من أجهزة بيجر استلمها عناصر "حزب الله" منذ 5 أشهر تقريبًا، وقد احتوت هذه الشحنة على حوالي 3 آلاف جهاز من فئة AR924 التي تصنعها شركة Gold Apollo التايوانية.

جهاز AR924 Apollo Gold

ويعتقد الخبراء أن لدى "إسرائيل" عملاء داخل "حزب الله". هؤلاء العملاء أجروا تعديلات على أجهزة البيجر وزرع متفجرات متناهية الصغر بداخلها في مرحلة التصنيع، قبل تسليمها إلى عناصر "حزب الله". ومن ثم يتم تفجير تلك الأجهزة عن بُعد عندما تتلقى رسالة معيّنة، أو عن طريق ترددات خاصة يتم إرسالها عبر أحد المسيّرات الإسرائيلية، والتي تحلق على مسافة قريبة من تلك الأجهزة.

وفي هذا السياق، أشار مايك ديمينو، الخبير الأمني والمحلل السابق لدى وكالة الاستخبارات المركزية الأمريكية، إلى أن العملاء نجحوا في توصيل الأجهزة إما عن طريق انتحال صفة مورّدين، وإما عن طريق اختراق سلسلة التوريد الخاصة بـ"حزب الله"، عبر استغلال نقاط ضعف معينة مثل شاحنات النقل والسفن التجارية.

وفي سياق آخر، أكّد تشارلز ليستر، الخبير لدى معهد الشرق الأوسط، استنادًا إلى تسجيلات الفيديو، أنه تم إخفاء عبوة ناسفة بلاستيكية صغيرة بجوار بطارية يتم تفجيرها عن بُعد عن طريق إرسال رسالة.

أصابع الاتهام ناحية تايوان

تعدّ شركة Apollo Gold التايوانية واحدًا من أكبر مصنعي أجهزة البيجر في العالم، وقد وُجّهت أصابع الاتهام ناحيتها نظرًا إلى تورطها في عملية تصنيع الأجهزة المتفجرة، والتي يحتمل كما ذكرت في السيناريو الثاني أنه قد تم اختراق سلاسل التوريد الخاصة بها، وحقن الأجهزة بمتفجرات تزن -وفقًا لبعض المصادر- 20 غرامًا.

وفي هذا السياق، نفى مؤسس شركة Apollo Gold التايوانية، هسو تشينغ كوانغ، هذا الاتهام، وأوضح أن هذه الأجهزة تم تصنيعها من قبل مورّع أوروبي لديه علاقة مع الشركة منذ حوالي 3 سنوات، كما ذكر هسو وجود حالة شاذة في التعامل مع هذا الموزع، كالتحويل المصرفي الذي استغرق وقتًا أطول من المعتاد.

تظهر الصور المتداولة على وسائل التواصل الاجتماعي أجهزة بيجر متضررة من طراز Apollo Gold AR924 في لبنان، ومع ذلك لم تتمكن المصادر الإخبارية، مثل "إن إن سي"، من التحقق من صحة هذه الصور أو تحديد السبب الدقيق للأعطال بشكل مستقل.

هل فعلتها حقًا "إسرائيل"؟

تستخدم "إسرائيل" تقنيات وأدوات متطورة للتجسس على أعدائها وتتبّعهم، بما في ذلك حماس و"حزب االله". كما أنشأت نظام مراقبة بعيد المدى يعتمد على تقنية التعرّف على الوجه لمراقبة الفلسطينيين في الضفة الغربية.

لكن هذه المرة، كان هذا الهجوم واسع النطاق بشكل غير مسبوق. لأول مرة يتم استهداف الآلاف من أعضاء "حزب االله" في وقت واحد عبر الأجهزة الخاصة بهم، والتي في الأساس تستخدم نظرًا إلى قدمها ومحدودية برمجياتها، ما يفرض صعوبة اختراق هذه الأجهزة.

الحقيقة التي لا مفر منها أن "إسرائيل" قد فعلتها بالفعل، واستطاعت توجيه ضربة موجعة لأحد معارضيها في المنطقة. ووفقًا لإميلي هاردينغ، نائبة مدير برنامج الأمن الدولي في مركز الدراسات الاستراتيجية والدولية، وهو مركز أبحاث في واشنطن، إن العملاء الإسرائيليين اعترضوا على الأرجح أجهزة البيجر في مكان ما في سلسلة التوريد، وتم تجهيزها بمتفجرات قبل أن يحصل عليها "حزب االله".

من جانبه، قال جينزن جونس، مدير شركة ARES الاستشارية المتخصصة في مجال الاستخبارات التقنية، عبر تغريدة نشرها على حسابه الرسمي على منصة إكس: "تشير مقاطع الفيديو التي شاهدتها إلى أن المواد المتفجرة كانت مدمجة في أجهزة البيجر. والنطاق الواسع يشير إلى هجوم معقّد على سلسلة التوريد، وليس سيناريو تمّ فيه اعتراض الأجهزة وتعديلها أثناء النقل".

هل "إسرائيل" قادرة على تنفيذ هذا الهجوم؟

إن القدرات السيبرانية لـ"إسرائيل" معروفة جيدًا. تعمل وحدة 8200 التابعة لجيش الدفاع الإسرائيلي، والتي تضم آلاف الجنود، على تطوير التكنولوجيا الخاصة بجمع المعلومات الاستخباراتية ومراقبة الأهداف العدائية. أحدث مثال على ذلك، عندما استخدمت "إسرائيل" بيانات الهاتف الذكي من أجل مراقبة وتتبّع الفلسطينيين خلال حرب الإبادة المستمرة على قطاع غزة.

لكن هذا ليس كل شيء. على مدار عقود، تعرّض معارضو "إسرائيل" لهجمات متكررة، حيث قامت الأجهزة الإسرائيلية باغتيال عدد من قادة فصائل المقاومة وخصوم آخرين، والأهم من ذلك إن التكنولوجيا لعبت دورًا محوريًا في عدد كبير من هذه العمليات.

في عام 1996، استشهد يحيى عياش، الذي كان يُعرف بلقب "المهندس" ويعدّ من أبرز صانعي القنابل

في حركة حماس. نجح عملاء إسرائيليون في اغتياله بواسطة هاتف محمول ملغّم. تم زرع المتفجرات داخل الهاتف، وعندما استخدمه عياش انفجر الجهاز، ما أدّى إلى مقتله على الفور. هذا الاغتيال أثار ردود فعل واسعة، وأدى إلى تصعيد التوترات في المنطقة، حيث اُعتبر ضربة قوية للبنية التحتية للمقاومة الفلسطينية في ذلك الوقت.

وفي عام 2010، كُشف عن برمجية خبيثة عُرف باسم "ستوكسنت (Stuxnet)"، والتي طورتها الولايات المتحدة و"إسرائيل" وفقًا لتقارير عديدة. استهدفت هذه البرمجية أنظمة التحكم الصناعية في منشآت تخصيب اليورانيوم في إيران، حيث تمكنت "ستوكسنت" من تعطيل وتشويه عمل أجهزة الطرد المركزي، ما أدّى إلى تأخير البرنامج النووي الإيراني بشكل كبير. انتشرت البرمجية إلى آلاف الأجهزة حول العالم، ما أثار مخاوف بشأن الأمن السيبراني والأسلحة الرقمية.

لا يمكن تجاهل دور شركة "إن إس أو غروب (Group NSO)" الإسرائيلية، التي طوّرت برنامج التجسس "بيغاسوس". يمكن لهذا البرنامج اختراق الهواتف الذكية دون علم المستخدم، ما يتيح الوصول إلى الرسائل والمكالمات والبيانات الشخصية، وحتى تفعيل الكاميرا والميكروفون عن بُعد.

اُستخدم "بيغاسوس" للتجسس على مجموعة واسعة من الأفراد، بما في ذلك صحفيين وسياسيين ونشطاء حقوق الإنسان في مختلف أنحاء العالم. هذا الاستخدام أثار انتقادات حادة ومخاوف بشأن انتهاكات حقوق الإنسان والخصوصية، ودفع بعض الحكومات والمنظمات إلى المطالبة بتنظيم ومراقبة أكثر صرامة لمثل هذه التقنيات.

بالإضافة إلى هذه الأمثلة، هناك سلسلة طويلة من الاغتيالات والعمليات السرية المنسوبة إلى جهات إسرائيلية، والتي تستهدف علماء ونشطاء وقادة عسكريين في دول مختلفة. هذه العمليات تثير تساؤلات جدّية حول مدى التزام "إسرائيل" بالقوانين الدولية ومعايير حقوق الإنسان. تظهر هذه الأحداث كيف يمكن للتكنولوجيا أن تستخدم كأداة فعّالة في الصراعات السياسية والأمنية، وتبرز الحاجة إلى حوار دولي حول الضوابط الأخلاقية والقانونية لاستخدام مثل هذه التقنيات.

أخيرًا، البيجر عبارة عن أجهزة أحادية الاتجاه، وبالتالي لا يمكن تعقبها ولهذا يتم استخدامها من قبل عناصر "حزب الله" في التواصل فيما بينهم بشكل آمن، ودون خوف من أي محاولة لتتبّعهم أو رصدهم.

لكن لكل شيء وجهان، الوجه المخيف للبيجر أنه غالبًا ما يستخدم قنوات اتصال غير مشفرة وبرامج قديمة، ما يجعله هدفًا سهلًا للغاية للمخترقين. وهكذا سواء بالسيناريو الأول أو الثاني، تمكنت "إسرائيل" من الإيقاع بمئات العناصر من "حزب الله" بضربة واحدة، وتحوّلت وسيلة التواصل القديمة والآمنة إلى قنبلة موقوتة فتاكة.

رابط المقال: https://www.noonpost.com/246322/