هكذا اخترق "سايبر حماس" أسرار الجيش الاسرائيلي

محترفون فلسطينيون شنوا هجمات سيبرانية مكثفة متزامنة عطلت مواقع حساسة وشركات كومبيوتر

تصفهم اسرائيل بـ"جنود الظل" الذين طاردتهم طوال أكثر من خمس سنوات وخططت لتصفيتهم بالاغتيال حيث نجحت مرات وأخفقت مرات أخرى. ففي عام 2021، أعلن الجيش الاسرائيلي وجهاز "الشاباك" نجاح عملية "حارس الأسوار" في تدمير مراكز التطوير والتدريب الخاصة بهم في قلب قطاع غزة، وذهبا إلى حد تأكيد القضاء عليها.

هم جنود "فيلق حماس السيبراني"، أحد مرتكزات عملية "طوفان الأقصى". هذا "الفيلق" لم يشكل مفاجأة من مفاجآت هذه العملية فحسب، بل فجر غضبا داخل الأوساط الاسرائيلية على الرغم من نفي تسببها بإلحاق أضرار جسيمة خلال الهجوم الأخير.

في تحقيق حديث نشرته شركة "كلاود فلير" يوم 23 أكتوبر/تشرين الأول 2023 تحت عنوان "الهجمات السيبرانية في الحرب الدائرة بين اسرائيل وحماس"، تأكد وقوع هجمات سيبرانية يوم 7 أكتوبر/تشرين الأول في تمام الساعة الثالثة والنصف بتوقيت "غرينتش" بهدف حجب الخدمة عن مواقع الكترونية إسرائيلية. بلغت ذروة الهجوم الأول 100 ألف طلب في الثانية واستمر لمدة 10 دقائق، ووقع هجوم ثان أكبر بكثير استمر 6 دقائق وبلغت ذروته مليون طلب في الثانية لحجب الخدمة، وفق التحقيق نفسه.

كلاود فلير" هي شركة أميركية عالمية متخصصة أساسا في الأمن" السيبراني وفي تأمين المواقع الالكترونية وحمايتها عبر شبكة ضخمة من الخوادم موزعة على 250 مدينة في أكثر من 100 دولة في كل القارات، وتقول الشركة إن خدماتها هي الأقرب الى جميع سكان العالم. وبحسب تحقيق الشركة، فإن ما حدث يوم 7 أكتوبر/تشرين الأول والأيام التي تلته، يشبه في بعض تفاصيله ما حدث خلال بداية الحرب الروسية الأوكرانية.

إلى ذلك، شددت الشركة على أن أنظمة الخدمة التابعة لها، تصدت تلقائيا، مع انطلاق عملية "طوفان الاقصى"، للهجمات التي قالت إنها استهدفت المواقع والتطبيقات التي تقدم معلومات وتنبيهات وصفتها

بالمهمة للإسرائيليين، على غرار تطبيق موجه للتحذير من وقوع هجوم وشيك.

مع ذلك، لا يعني أن ما حصل ويحصل منذ 7 أكتوبر/ تشرين الأول من هجمات، هو "حرب سيبرانية" وفق فرنسوا ديروتي، مدير المعلومات في شركة الأمن السيبراني "سيكوبا"، الذي قال في تصريح لوكالة "فرانس برس"، إن الهجمات تهدف إلى حجب الخدمة من خلال تعمد حصول حركة كثيفة تجعل الموقع الالكتروني غير متاح لساعات.

صورة لعناصر من "حماس" في غزة، فلسطين في 9 أكتوبر/Shutterstock تشرين الأول 2023.

تحسب جل الهجمات السيبرانية على خبراء "سلاح السايبر" التابع لـ "حماس"، والذي تؤكد تقارير أنه يستحوذ على بنك معلومات، أو ما سمّته صحيفة "نيويورك تايمز" الأميركية بـ"أسرار إسرائيل ونقاط ضعفها" التي جمعتها "حماس" طوال فترة تخطيطها لعملية "طوفان الأقصى".

هذا المعطى هو أبرز ما كشف عنه تقرير نشرته الصحيفة منذ أيام عن عملية "طوفان الاقصى" من مصادر شملت مقابلات مع 20 مسؤولا استخباراتيا إسرائيليا ومع جنود، بالإضافة الى ناجين من هجوم 7 أكتوبر/تشرين الأول 2023، إضافة إلى وثائق تم حجزها إثر الهجوم تعود الى مقاتلين من حركة "حماس"، ولقطات وجدت في كاميرا كانت مثبتة في قبعة واحد من مسلحي الحركة.

[illegible]

الخلاصة التي قدمتها الصحيفة تبرز أنه سبق العملية تخطيط دقيق ومعرفة غير عادية بأسرار الجيش الاسرائيلي ونقاط ضعفه. ونقلت عن ضابط وصفته بالكبير في الجيش الاسرائيلي، تشديده على أن المشاركين في الهجوم عرفوا بالضبط مكان خوادم الاتصالات ثم دمّروها في عدة قواعد عسكرية. كما أكدت "نيويورك تايمز" ان للمجموعة المشاركة في الهجوم "فهما متطورا بشكل مدهش لكيفية عمل الجيش الاسرائيلي ولتمركز وحدات في عينها، علاوة على الوقت الذي يستغرقه وصول التعزيزات".

بناء عليه، سينطلق الجيش الاسرائيلي مباشرة فور انتهاء الحرب الدائرة في التحقيق حول كيفية نجاح حركة "حماس" في اختراق دفاعاته بهذه السهولة.

وأضافت الصحيفة أن هناك قلقا سببه طريقة تجميع الكثير من المعلومات حول الجيش الاسرائيلي وحول عملياته الخاصة. وأشارت الى فرضيتين، الأولى، وجود إهمال لدى القوات الاسرائيلية في ما يتعلق بأسرارها، والثانية، اختراق نفذه جواسيس وعملاء جندتهم "حماس" من قلب منظومة الدفاع الاسرائيلية.

هذه الامكانات النوعية لحركة "حماس" على المستوى الاستخباراتي والسيبراني، كانت محل اهتمام إسرائيلي رسمي وإعلامي منذ 9 سنوات، وتحديدا مع بداية تنفيذ هجمات سيبرانية ناجحة بقيادة "جنود الظل" مثلما تلقبهم الأجهزة الاسرائيلية، أو "سلاح السايبر" بحسب تسمية "كتائب القسام" الجناح العسكري لـ"حماس"".

هجمات "حماس"

وأكد تحقيق "كلاود فير" أن ما حدث "لم يكن مجرد هجمات" من دون ان يوضح أكثر، لكن تحولت مواقع الكترونية وتطبيقات الهاتف المحمول الاسرائيلية إلى أهداف من مجموعات مختلفة من القراصنة المناصرين لفلسطين" (AnonGhost)، ومنها مجموعة "أنون غوست" التي نجحت في استغلال ثغرة في تطبيق "ريد ألرت" (Red Alert) الذي ينبه

الاسرائيليين الى وقوع هجوم، مما مكنها من كشف الخوادم وواجهات برمجة التطبيقات وإرسال تنبيهات مضللة لبعض مستخدمي التطبيق، على غرار التحذير من ضربة بقنبلة نووية.

هل ستنجو البنية التحتية لـ "سايبر حماس" من الدمار الهائلAP والشامل

بحسب التحقيق، فإن "تطبيقات خبيثة" استهدفت هواتف "أندرويد"، مكّنت من الوصول إلى معلومات حساسة لمستخدمين. ولفت التحقيق إلى أنه تم خلال الأيام التي أعقبت 7 أكتوبر/تشرين الأول، استهداف المواقع الالكترونية الاسرائيلية بالهجمات الموزعة بشكل مكثف لحجب الخدمة. وكشف أن ذلك يمثل 56 في المئة من إجمالي الهجمات. وخلص التحقيق إلى أن ذلك يشبه ما حصل عند بداية تنفيذ روسيا هجومها على أوكرانيا باستهداف مواقع وسائل الإعلام والبث الأوكرانية بشكل مكثف.

وذكّر بأن هجمات سيبرانية على المواقع الإلكترونية ترافق، عادةً، الحرب على الميدان، لأنها توفر معلوماتٍ مهمة، وقال إنه تم استهداف المواقع الإلكترونية للصحف ووسائل الإعلام الإسرائيلية مباشرة بعد بداية عملية "طوفان الاقصى".

[illegible]

يعدّ مجال برمجيات الكومبيوتر، بحسب بيانات التحقيق، القطاع الثاني الأكثر استهدافا بالهجمات السيبرانية في إسرائيل، إذ أن ما يقارب الـ 34 في المئة من الهجمات الموزعة لحجب الخدمة، استهدفت الشركات العاملة في برمجيات الكومبيوتر. ويأتي في المركز الثالث من حيث التعرض للهجمات، القطاع المصرفي وشركات الخدمات المالية وشركات التأمين. أما في المركز الرابع فجاءت مواقع الإدارة الحكومية.

تشير الأرقام أيضا إلى تسجيل أكثر من 5 مليارات طلب "نقل بيانات". وكشف التحقيق أن هذه الطلبات هي جزء من الهجمات الهادفة لحجب الخدمة. وتقول الشركة إنه لم تكن هناك خلال الفترة التي سبقت 7 أكتوبر/تشرين الأول أي طلبات لحجب الخدمة بالنسبة إلى المواقع التي تستخدم "كلاود فاير"، وإن نسبة الهجمات المكثفة لحجب الخدمة ارتفعت يوم الهجوم بمعدل 1 من كل 100 هجوم موجه للمواقع الالكترونية الاسرائيلية. وقد تضاعف هذا الرقم 4 مرات يوم 8 أكتوبر/تشرين الأول.

"شعار جنود "سلاح السايبر" التابع لحركة "حماس

في المقابل، كشف التحقيق أنه تم التصدي خلال الفترة نفسها تلقائيا لما يزيد على 454 مليون طلب نقل بيانات لحجب الخدمة استهدفت "المواقع الالكترونية الفلسطينية التي تستخدم "كلاود فاير.

من يملك المعلومة يملك الميدان

حيثيات (Israel Hayom) "وانتقد مقال صادر في صحيفة "إسرائيل هيوم عملية "طوفان الاقصى" ووقائعها، خصوصا لما كشفته من ثغرات على مستوى أجهزة الاستخبارات والدفاع ومن اختراق لهما.

وتساءلت في مقال بعنوان "أين كانت المخابرات ولماذا استغرقت كل هذا الوقت؟ الاسئلة الصعبة التي يتعين على لجان التحقيق الإجابة عنها"، عن سر "الفشل الاستخباراتي الهائل"، مذكِّرةً بإقدام الجيش قبل أشهر من الهجوم على تقليص عدد قواته المتمركزة في غزة قبل نقلها إلى يهودا والسامرة.

كما ذكّرت بتصريحات مسؤولين كبار من الجيش عند تفسيرهم خلفيات هذا القرار وكيف استندوا فيه إلى معطيات تؤكد أن حركة "حماس" لا

تعتزم التصعيد باعتبارها منشغلة بتوفير الرفاهية لسكان القطاع الذين يدخلون إسرائيل بالآلاف للعمل يوميا. ويؤشر ذلك إلى تفوق الجهة المقابلة، أي حركة "حماس"، التي شنت هجوما خططت له بدقة. أما قاعدة هذا التفوق، بحسب الإعلام العبري، فهي "من يملك المعلومة يملك الميدان".

"[illegible]"

[illegible] "[illegible]"

وأكد تقرير "نيويورك تايمز" أن لحركة "حماس" "معرفة دقيقة بأسرار الجيش الاسرائيلي بشكل مذهل". ويتقاطع هذا التقرير مع تصريحات خبراء في الأمن السيبراني ومسؤولين عسكريين عن دور "سلاح السايبر" التابع لـ"كتائب القسام" في مهمتين محوريتين: الأولى، على مستوى استخباراتي كان وراء نجاح العملية، والثاني على مستوى اختراق مواقع بشكل مكثف تسبب في شلل حال دون تدخل سريع للأجهزة الاسرائيلية.

"جمعة طلحة مؤسس "سلاح السايبر

يعد "سلاح السايبر" من أهم الوحدات التابعة لـ"كتائب القسام"، وجرى الإعلان عنه رسميا منذ عام، وتحديدا يوم 13 أكتوبر/تشرين الأول 2022. كانت المناسبة مناسبتين في آن واحد بالنسبة إلى "الكتائب" التي قررت أولا، إخراج نشاط منظومتها السيبرانية من سرية استمرت لثماني سنوات، وثانيا، تكريم مؤسس "سلاح السايبر" المهندس جمعة طحلة، الذي وصفته "الكتائب" بـ"الشهيد"، قالت إنه "عمل على تأسيس وتأهيل وتطوير" فيلقها العسكري السيبراني.

وأوضحت "الكتائب" أن الشروع في تأسيس الفيلق انطلق منذ عام 2014 وتم تكليف طحلة هذه المهمة باعتباره "الشخصية الأنسب"، مضيفة أن طحلة "بدأ منذ اللحظات الأولى لتوليه الملف بجمع الكوادر المتخصصة، وإعداد المقدرات، وإجراء التجارب مع فريق متخصص، ومتابعة مراحل بناء هذا الكيان الحديث متابعة حثيثة".

وأكدت أن "المهندس طحلة سخر اهتمامه في تطوير العمل السيبراني في شكل كبير واقترح إنشاء كيان مساند لسلاح السايبر القسامي، فكان

صاحب فكرة تأسيس جيش القدس الالكتروني". وأقرت "الكتائب" بأن عمليات التجنيد تقوم على "فكرة حشد أكبر قدر ممكن من الطاقات على مستوى الأمة العربية والاسلامية التي لديها الخبرة في مجال السايبر"، وبأنها تقوم بتوجيهها لشن هجمات سيبرانية ضد المصالح الاسرائيلية ومنظوماتها.

وكشفت "الكتائب" يوم الإعلان عن إنجازاتها في هذا المجال خلال فترة النشاط السري، أنه كان للهجمات التي شنتها الأثر الكبير على أنظمة إسرائيل باختلاف مهامها وتخصصاتها.

الأمثلة التي قدمتها "الكتائب" على الهجمات متعددة. أولى العمليات كانت "قطع الكهرباء عن كيبوتس مفلاسيم شمال شرق قطاع غزة"، كما نشرت جردة لهجماتها السيبرانية يمكن تلخيص أبرزها في ما يلي:

– هجوم سيبراني واسع على قواعد ومواقع عسكرية ومنشآتٍ أمنية وأهداف حساسة طال 30 ألف هدفٍ خلال عدوان مايو/أيار 2019.
– التموضع في نظام صافرات الإنذار الخاص بشركة "ايفقلو" وتفعيل الصافرات في مناطق متعددة من إسرائيل.
– اختراق ترددات إشارات اللاسلكي التابع للجيش الاسرائيلي على حدود غزة مرات عدة والتنصت عليه.
– اختراق جهاز مدير قسم السايبر في شركة الصناعات الجوية الاسرائيلية.
– سحب بيانات ومعلومات أمنية وعسكرية بحجم 19 جيغا.
– اختراق نظام شبكة الحافلات "إيجد".

وأقرّ الجيش الاسرائيلي بأن الهجمات كانت نوعية، وأكد في عام 2018 بشكل وُصف بالنادر اختراق "حماس" هواتف العشرات من جنوده.

عملية "القلب المكسور"… قبل غزة

وأطلق الجيش الاسرائيلي عملية "القلب المكسور" في 2018 وفق موقع "أي 24" العبري للتصدي لهذا الاختراق الذي قال إنه جاء إثر عملية محكمة من "حماس" مكّنتها من جمع معلومات وصور لمقار الجيش وصور لمعسكرات وغرف القيادة. وتم الاختراق بتطبيقات دردشة كانت في الأصل تطبيقات تجسس، نافيا نجاحها في تحقيق أي ضرر أمني محسوس.

ثم بدأت بعدها عمليات استهداف الأجهزة الاسرائيلية لناشطين في "سلاح السايبر"، وتقول تقارير استخباراتية إسرائيلية نقلتها وسائل إعلام عبرية، إن هؤلاء الناشطين تلقوا تدريبات لاكتساب قدرات إلكترونية بين ماليزيا وتركيا وإيران.

تعددت الاستهدافات، وتقدم الصحف الاسرائيلية تفاصيل في خصوصها على غرار محاولة جهاز الموساد عام 2021 اختطاف عمر البلبيسي، خبير الكومبيوتر المتخصص في اختراق أجهزة "أندرويد". البلبيسي هو من قادة "سلاح سايبر حماس" وتمت محاولة اختطافه في مدينة كوالالمبور وإجباره على التحقيق "عبر الفيديو". وبحسب "نيوز 1" الاسرائيلي، قام جهاز الموساد في أبريل/نيسان 2018، باغتيال الدكتور فادي البطش، وهو أيضا من قادة "سلاح سايبر حماس".

وخلال عملية "حارس الأسوار" قام الجيش الاسرائيلي، بناء على معلومات من جهاز "الشاباك"، بتصفية عدد من أهم قيادات "سلاح السايبر"، في مقدمهم جمعة طحلة، الذي يوصف بصاحب حقيبة البحث والتكوين، واليد اليمنى لزعيم الجناح المسلح لحركة "حماس" محمد الضيف.

[illegible]

الاسرائيلي مقالا بعنوان "قدرات حماس تضررت بشكل Ynet" ونشر موقع قاتل"، قائمة مفصلة بقادة "سلاح السايبر" الذين قام الجيش الاسرائيلي بتصفيتهم في عملية واحدة عام 2021 وعددهم 20 في عملية "حارس الأسوار"، قال الجيش و"الشاباك" إنها الأولى من نوعها والأهم. تمثلت العملية في تدمير مبنى "التدريب والتطوير" التابع لـ "فيلق حماس السيبراني"، وكان الهدف وفق الموقع، الإضرار بشكل قاتل بقدرة "حماس" على مواصلة الهجمات السيبرانية، وبمثابة عملية إعدام لهذه المنظومة، بما يؤدي إلى تأخير بناء قدرتها في الميدان.

أعدّ دراسة أميركية نشرها (Atlantic Council) وكان المجلس الأطلسي مركز الدفاع الاسرائيلي (صادرة عام 2022) أكدت أنه تم تجاهل توسيع "حماس" قدراتها السيبرانية الهجومية خلال السنوات الأخيرة، والتي تطورت خصوصا في مجال التجسس الداخلي والخارجي.

وبحسب الدراسة، فإن منظومة "حماس" السيبرانية" أو "سلاح السايبر"، تضاهي "قوة الأمن الداخلي وتماثل منظومة الاستخبارات الرئيسية لحركة حماس"، وتتكون من أعضاء من "قوة المجد" الأمنية التابعة لـ"كتائب عز الدين القسام". وتتراوح مسؤوليات قوى الأمن الداخلي بين التجسس واستهداف المعارضة السياسية والانشقاق من داخل الحركة وأجهزتها الأمنية.

ستكون التطورات المقبلة للحرب الدائرة كفيلة بالوقوف على مدى تطور المنظومة السيبرانية لحركة "حماس". ومهما تكن النتائج، فإن "سلاح السايبر" ألحق ضررا كبيرا بإسرائيل بشكل يلخصه رام ليفي، أحد مطوري المنظومة السيبرانية في مكتب رئيس الوزراء الاسرائيلي سابقا، بقوله في تصريح لبوابة المالية الالكترونية العبرية "بيز بورتال": "يُنظر إلى إسرائيل بالفعل على أنها قوة سيبرانية، وعندما أنشأنا النظام السيبراني كتبنا أنه يجب أن تمتلك إسرائيل قدرات من شأنها التأثير على العالم كله من خلال معلومات استخباراتية عالية الدقة، لكن هذا لا يعني أن إسرائيل بلد محمي. هناك اعتقاد خاطئ بأننا محميون. إننا بعيدون عن الحماية في أماكن عدة والهجمات التي حدثت ستلحق قطعا الضرر بسمعة الصناعة السيبرانية الاسرائيلية".

كوثر زنطور

المصدر: مجلة "المجلة" العربية