سايبر الخلافة: جيش داعش الإلكتروني الذي هزم أجهزة المخابرات العالمية

كتبه أحمد عزيز | 8 مايو ,2016

"فجأة وجدنا أنفسنا في ظلام تام، وافتقدنا إلى المعلومات التي يمكننا تعقبها لوقف أي مخطط للتنظيم"، بهذه الجملة بدأ مايكل ستاينباخ مساعد مدير مكتب التحقيقات الفيدرالي FBI، حديثه لصحيفة التايم بعد هجمات باريس وبروكسل، تعليقًا على اتهامات بفشل الاستخبارات الأمريكية والفرنسية والبريطانية في اكتشاف مخططات تنظيم داعش الإرهابي بالدول الغربية، مشيرًا إلى أن التنظيم يخفي تطبيقاته للدردشة والتراسل بين أعضائه بوسائل ابتكارية حديثه تصعب من تتبعها.

ستاينباخ قال أيضًا إن مسؤولين كثر بمكتب التحقيقات تقدموا بطلب للكونجرس الأمريكي للسماح لهم بتوسيع صلاحياتهم، ليتمكنوا من الدخول إلى تطبيقات الرسائل لأشخاص مشكوك فيهم مثل تطبيقي "الواتس آب" و"كيك"، وكذلك إلى التطبيقات القادرة على تدمير البيانات مثل "ويكر" و"سورسبوت"، التي يستخدمها مئات الملايين من المستخدمين، بينهم بعض المسلحين حول العالم، لأنها تضمن أمان الرسائل والخصوصية.

ثورة داعش التقنية

بدأت ثورة داعش التكنولوجية مع البدايات الأولى لظهور التنظيم للعلن في سوريا والعراق، وظهر ذلك في قدرته على تصوير وبث مقاطع فيديو سينمائية، وإخراج للمذابح التي يرتكبها يوميًا ضد مخالفيه، مستعينًا على تلك القدرات بتجنيد الأفراد ذوى المهارات فى البرمجة والاختراق، واستهدف

التنظيم مجموعة من أهم الهاكرز والمخترقين في العالم من أجل مساعدته في تنفيذ الهجمات الإلكترونية، والبقاء بعيدًا عن يد المخابرات الدولية.

ونجح التنظيم في العام 2014 في تجنيد شابًا أمريكيًا بارعًا في الاختراق، زود التنظيم بمعلومات حول استخدام العملة الافتراضية "بيتكوين" لإخفاء تبرعاتهم المالية للتنظيم، كما أطلعهم على وسائل لتشفير حواراتهم على الإنترنت، وظل يعمل تحت قيادة الهاكر البريطاني "جنيد حسين"، الذي كانت مهمته تدريب عناصر داعش على عمليات الأمن والاختراق، ضمن مجموعة أطلق عليها لقب "سايبر الخلافة".

دليل إلكتروني

وفي نهاية العام 2015 أصدر التنظيم مجلة إلكترونية، متخصصة لتعليم الجهاديين أساسيات الحرب الإلكترونية ضد الغرب، ونشر العدد الأول من المجلة باللغة الألمانية، وتم تداوله على مواقع التواصل الاجتماعي "تويتر" و"فيس بوك" و"تيليجرام"، يحذر خلاله من الاختراق والتعامل بحرص مع البرامج والأجهزة بمختلف أنواعها، وتضمنت المواد المنشورة في المجلة موضوعات عن كيفية البقاء في أمان عبر الإنترنت عند التواصل مع الجهاديين حول العالم، وأخرى تطرح عدة بدائل عن بعض التطبيقات المشهورة مثل "WhatsApp" و"Gmail" و"Hotmai"، بالإضافة إلى دليل من 12 خطوة عن استخدام تويتر، يوصي تفعيل خيار التحقق من تسجيل الدخول، للتأكد بشكل قوي من أن كلمة المرور الخاصة آمنة ولم يستخدمها أحد.

ويعمد التنظيم إلى إرسال رسائل يومية لما يقارب مئتي ألف شخص، يدعوهم خلالها للانضمام له، مرفقة بتعليمات ومواد تثقيفية وتعريفية بالتنظيم والحياة بين جنباته، حتى مقاطع الفيديو والتغريدات اليومية التي ينشرها التنظيم عبر حساباته كنوع دعائي وجودي، يكلف من بين أعضائه من يتتبع معيدي نشرها من الجماهير والتواصل معهم، ودعوتهم لنشر رسائلهم على التطبيقات المدمرة للبيانات، حتى لا يتم تعقبها من قبل أي جهاز أمني، حتى مقاطع يوتيوب التي تنتشر من خلال قنوات مختلفة للتنظيم ابتكر عناصره برامج تعيد إطلاقها بمجرد حذفها، وحذر جميع مقاتليه من استخدام أجهزة مزودة بتقنية GPS، وهواتف جلاكسي لأن بطاريتها يمكن تعقبها.

غزو عنكبوتي

الآن وبحسب مصادر معلوماتية كثيرة وتقارير استخباراتية عدة، تمتلك داعش أكثر من 3000 موقع إلكتروني، و90 ألف صفحة باللغة العربية على "فيس بوك"، و40 ألف صفحة أخرى بلغات مختلفة، تستخدمها جميعها لبث أفكارها المتطرفة حول العالم، خصوصًا أنها تبث بعدد من اللغات بينها الفرنسية والإنجليزية والألمانية والصينية وغيرها، ناهيك عن نشاط اللجان الإلكترونية التابعة للتنظيم على مواقع التواصل بشكل مكثف، حيث يبث التنظيم يوميًا أكثر من 200 ألف تغريدة مقسمة على عدة لغات.

ويعمد التنظيم لاستخدام عدد من التطبيقات في التخطيط لعملياته يصعب على إدارات أمن

الإنترنت حول العالم اختراقها، تبدأ بتطبيق "تيليجرام"، وهو تطبيق لتبادل الرسائل النصية يحافظ على تشفير الرسائل، ويُبقي هوية المستخدم خفيّة، بالإضافة إلى "الواتس آب" و"ويكر" وهي جميعًا تتيح تشفير الرسائل؛ مما يجعل التجسس على محتواها أمرًا فائق الصعوبة، وأحيانًا مستحيلاً، خاصة إذا ما أضفنا إلى ذلك أن العناصر التقنية للتنظيم نجحت في ابتكار أدوات قادرة على تشفير التطبيقات الأخرى، بينها تطبيق التشفير "أسرار المجاهدين" Mojahedeen Secrets"، التي تشفر الرسائل الإلكترونية، و"أسرار الدردشة"، التي تشفّر المحادثات بين حسابات "AIM" و"Google.Talk" و"MSN" وYahoo"، وعمل التنظيم على التواصل بين أعضائه عن طريق برامج مثل الجهادين، وشبكة الفداء، وشبكة الشموخ الإسلامية، وكلها تخفي عناوين الـ IP والهوية، وتنشر مادتها عبر شبكة الـ "TOR"، التي لا يمكن حذف محتواها.

تحذيرات أنونيموس

في السابع عشر من يناير الماضي، حذرت جماعة "أنونيموس" المتخصصة في اختراق شبكات الإنترنت والأنظمة الإلكترونية حول العالم، من أن المتتبع لمصادر التغريدات الداعشية على شبكة الإنترنت، من الصعب أن يجد أية معلومات أو آثار تشير إلى تلك المصادر، كون التنظيم يعتمد على ما وصفته "أنونيموس" بـ "الشبكة المظلمة"، وهي مجموعة مواقع لا تستطيع محركات البحث أرشفتها، ويتم الوصول لها بطرق تقليدية يدوية، لأنها تخفي الكلمات الدلالية ببياناتها.

تحذيرات أنونيموس جاءت في توقيت كانت تخطط فيه داعش بالفعل لهجمات في أوروبا، مثل باريس وبلجيكا وألمانيا وإيطاليا، حتى إن التنظيم دعا معظم منتسبيه بتلك الدول لوقف التواصل عبر تطبيق التراسل "واتس آب"، ونقل الدردشات البينية بينهم إلى تطبيق "تيليجرام"، وهو تطبيق قوي التأمين انتشر بعد فضيحة التجسس الخاصة بوكالة الأمن القومي الأمريكية NSA، حيث سعت العديد من الشركات إلى إصدار تطبيقات للتواصل تتبنّى معايير تشفير قوية، تجعل من شبه المستحيل على الحكومات تعقب المراسلات والتجسس عليها، ناهيك عن تتبع أصحابها، خصوصًا وأن الـ "تيليجرام" يعتمد تقنية التشفير على هواتف المُستخدمين، وليس عبر مُخدّم وسيط، أي أن الشركة المطوّرة للتطبيق نفسها لا تستطيع التجسس على محادثات المستخدمين، كما يقدم التطبيق ميزات أخرى مثل إمكانية التدمير الذاتي للرسائل بعد فترة زمنية معينة، وإمكانية استخدام التطبيق دون الحاجة لربطه بأي رقم هاتف أو بريد إلكتروني، واستغل التنظيم تلك الميزة في توجيه النصائح لعدد من الموالين له بتلك الدول، سواء بتجنب أماكن بعينها ضمن خريطة الاستهدافات، أو حتى خطة الهروب في حالة انكشاف أمر أي منهم، بل إن رسائل مطولة وجدت بهواتف بعض المقبوض عليهم، لم يمر عليها أكثر من 12 ساعة قبل توقيفهم، كانت تتضمن خطة الخروج من تلك الدول عبر الحدود البرية واليونانية باتجاه تركيا للالتحاق بعناصر التنظيم في كل من سوريا والعراق.

خلال الشهر الماضي خرجت التحقيقات الأوربية في تفجيرات باريس بحقيقة مفادها أن تنظيم "داعش" الإرهابي يستخدم برامج الهواتف الذكية المشفرة بنجاح في التخطيط العسكري بصورة سرية، ولتجنيد مقاتلين جدد، ويقوم بإرسال رسائل مشفرة تتضمن معلومات باستحداث مراكز إلكترونية للقيادة، وإدارة الهجمات الانتحارية عبر إرسال المعلومات الضرورية عبر الإنترنت إلى الهواتف

المحمولة التابعة لمنفذي الهجوم.

بالإضافة لـ "التيليجرام" والتطبيقات الآمنة التي يستخدمها التنظيم، بدأت أنظار عناصره في التوجه مؤخرًا إلى تطبيق جديد يمكنها استبداله بالتليجرام حالة التخطيط لعمليات لها بالجانب الروسي، لأن التيليجرام يتبع شركة روسية، ومن الممكن أن يكون مخترق من قبل المخابرات بموسكو، ولجأت قيادات التنظيم إلى برنامجي "Surespot"و"Kik"، حيث يسمح الأول "Surespot" بتشفير الرسائل النصية وهي في طريقها إلى المستلم، ويبقى المرسل وحده هو من يتحكم في الرسائل عبر هذا البرنامج، إذ يمكنه إزالة جميع الرسائل في أية لحظة، ويشمل ذلك النسخ التي وصلت إلى المستلم، ولا يسمح البرنامج لأحد باستثناء المرسل إليه، بالاطلاع على مضمون الرسالة، أما برنامج "Kik" فيسمح للمستخدمين بإرسال رسائل مشفرة وصور.

"الراوي" بديل آمن

مؤخرًا وبعد تضييق الخناق على أفراد التنظيم منذ شهرين تقريبًا، ومطاردتهم بحذف المجموعات التي قاموا بإنشائها على تطبيق التيليجرام، لجأ عناصر التنظيم إلى ابتكار تطبيق جديد اطلقوا عليه اسم "الراوي" Alrawi وهو تطبيق للمراسلة الفورية لكنه يختلف عن الواتس آب والتيليجرام في طريقة الشفير التي تزيد أمر اختراقه صعوبة، وأضاف تقنيو داعش إلى تطبيق الراوي تطبيق آخر يطلق عليه AmaqAgency، وهما تطبيقان لا يتوافران بشكل مباشر على الإنترنت ولا يعملان إلا على الهواتف بنظام أندرويد، لتستمر بذلك الحرب المعلوماتية والتقنية بين التنظيم والاستخبارات الدولية.

رابط المقال : https://www.noonpost.com/11651/