تقرير

ابرز مجتمعات الهاكتيفيزم المعروفة منظمة «انونيموس» و«ويكيليكس»

Hacktivism: ثورة أم فوضى «أونلاين»؟

راغب غندور *

عندما تزاوجت القرصنة مع النشاط الاجتماعي والسياسي، بات لدينا ما يسمى "هاكتيفيزم" hacktivism. و"الهاكتيفيزم" ببساطة هو استخدام التكنولوجيا لتحقيق هدف سياسي أو اجتماعي، أو بمعنى آخر هو

الهاكتيفيزم هو النشاط الإلكتروني الساعي نحو التغيير الاجتماعي عبر الجمع بين قدرات البرمجة والفكر النقدي

النشاط الإلكتروني الساعي نحو التغيير الاجتماعي عبر الجمع بين قدرات البرمجة والفكر النقدي. يعتبر "الهاكتيفيزم" شعبة من شعب النشاط على الإنترنت، وتحديداً استخدام تكنولوجيا الاتصالات لأهداف عدة، تحت منطلق الاصلاح الاجتماعي أو تحقيق المطالب وتأسيس مجموعات ضغط تجاه كيان معين، وهو شكل بناء لعصيان مدني لاسلطوي. إلا أنه شكل مختلف من النشاط على الانترنت له فلسفته وأهدافه الخاصة، ومبني على ثقافات وأخلاقيات مجتمعات المخترقين الذين يستخدمون تكنولوجيا المعلومات كأدوات للضغط على منظمات فاسدة أو حكومات. إذاً تعتبر حركة "الهاكتيفيزم" شكلاً من أشكال التعبير عن الرأي السياسي، وغالباً ما تشجع على حرية التعبير، والدفاع عن حقوق الانسان وحرية تبادل وحماية المعلومات الإلكترونية بشفافية.

أكثر شكلين منتشرين لهذا النشاط هما تقنيات التشويه لمواقع الانترنت، أو ما يعرف في عالم المخترقين بالـ"defacing"، وهجمات الحرمان من الخدمات "DoS". تعتمد العملية الاولى على اكتشاف الثغرات الأمنية في الخوادم حيث يوجد الموقع المستهدف، فيعمد المخترق الى تغيير ملامح الصفحة من خلال أدوات البرمجة المتاحة لترك إشارة. يمكننا مقارنتها بفن الـ"غرافيتي"، ولكن بنسخة إلكترونية كشكل من أشكال "الاعتصام الإلكتروني". وقد تعرضت بعض المواقع الالكترونية التابعة للدولة اللبنانية لمثل هذا النوع من الهجمات، أحدثها اختراق موقع مجلس الجنوب، وموقع المجلس الاقتصادي والاجتماعي اللبناني، وموقع وزارة الاتصالات اللبنانية بعد قطع الاتصالات يومها عن عدد من المناطق اللبنانية. هذا الشكل من الاعتراض الإلكتروني غالباً ما لا يؤدي إلى إلحاق أذى جسيم.

أما هجمات الحرمان من الخدمات "DoS"، فهي، وفق شركة "بالو ألتو" المتخصصة في الأمن السيبراني، هجوم يهدف إلى إيقاف تشغيل آلة أو شبكة، ما يجعلها غير قابلة للوصول إلى المستخدمين المقصودين. تتحقق هذه الهجمات عن طريق إغراق المستهدف بكمية هائلة من البيانات والطلبات العشوائية، أو إرسال معلومات تؤدي الى تعطل النظام. يتحكم القراصنة والعابثون الإلكترونيون عن بعد في إرسال تلك البيانات إلى المواقع بشكل كثيف، ما يسبب بطء الخدمات أو زحاماً مرورياً في هذه المواقع، ويمنع وصول المستخدمين إليها نظراً إلى هذا الاكتظاظ، وعلى هذا الأساس فإن هذا النوع من الهجمات يُدعى في بعض الأوساط "إيدز الإنترنت".

في كلتا الحالتين، يحرم هجوم الحرمان من الخدمة المستخدمين الشرعيين (أي الموظفين أو الأعضاء أو أصحاب الحسابات) من الوصول الى الخدمة أو المورد الذي يتوقعونه. وغالباً ما يستهدف خوادم الويب لمنظمات رفيعة المستوى مثل البنوك والشركات التجارية والإعلامية أو المنظمات الحكومية والتجارية. على الرغم من أن هجمات DoS لا تؤدي

عالسريع

«فئران، فئران، فئران»

ـ أول عملية اختراق في التاريخ حصلت عام 1903 لتلغراف لاسلكي، وذلك عندما كان الإيطالي غوليلمو ماركوني يقيم عرضاً عاماً أمام الجمهور لإثبات عمل نظامه اللاسلكي الجديد، الذي يمكنه إرسال الرسائل على طول موجي محدّد لإنشاء قنوات اتصالات خاصة، أي إرسال رسائل بشكل آمن على مسافة طويلة. كان ماركوني على بعد أكثر من 300 ميل في كورنوال، يستعد لإرسال الرسائل إلى زميله البروفسور فليمينغ الموجود في المسرح. لكن ما إن بدأ العرض حتى بدأت تتكرر كلمة "فئران"، ولحقتها إهانة شخصية لماركوني تقول: "كان هناك شاب من إيطاليا، خدع الجمهور بشكل جميل جداً". وبذلك تم الاستيلاء على نظام ماركوني "الآمن" من قبل ساحر!

ـ أول مخترق في التاريخ هو نيفيل ماسكلين الذي ينحدر من عائلة من الساحرين والمخترعين، وقد اهتم هذا الساحر البريطاني بالتكنولوجيا اللاسلكية. وكانت الاتصالات اللاسلكية إمكانات السحر الحقيقي لماسكلين، لأنها مكّنته من "قراءة العقل" في أعين الجمهور الذي لم يكن يفهم إشارات مورس التي يستعملها للتواصل مع مساعدته. وفقاً للعديد من الكتاب، كان ماسكلين قادراً على إرسال رسالة إذاعية لاسلكية من محطة أرضية إلى منطاد في السماء، إلا أن طموحاته في مجال التكنولوجيا اللاسلكية أحبطت بسبب براءات الاختراع التي يملكها ماركوني.

ـ شكل اختراع ماركوني تهديداً لصناعة السلكي والبرق. ورداً على ذلك، استأجرت شركة الشرق للتلغراف نيفيل ماسكلين لمراقبة عمل ماركوني. تمكّن ماسكلين من بناء مستقبلات عريضة النطاق قادرة على اعتراض ما يسمى "الإرسال الآمن" لماركوني من دون معرفة ترددات الموجات. وعليه لم يجد الساحر وسيلة أفضل للانتقام من ماركوني سوى بإثبات فشل اختراع الإيطالي أثناء قيامه بعرضه الأول لهذه التقنية عبر اختراقها!

ما الفرق؟

قبعات سوداء وبيضاء ورمادية!

تتردد كثيراً بين الناس عبارات مثل «اختراق» و«مخترقين» أو hackers، فتسود صورة سوداوية لهؤلاء الأشخاص ذوي الاختصاصات التقنية، كأنهم عصابات جلّ ما يفعلونه هو إيذاء الناس في العالم السيبراني.عالم المخترقين الشاسع يشبه المجتمعات، فهناك الجيد وهناك السيّئ، وكلٌّ لديه «قبعته» الخاصة.

الهاكر أو قرصان الانترنت، هو شخص كفء، يمتلك المعلومات التقنية التي تمكّنه من استغلال نقاط الضعف في الأنظمة والشبكات، انطلاقاً من فكرة أن النظام خالٍ من المشاكل. هدفه يختلف تبعاً لمنظومته الأخلاقية، لذلك ينقسم متسللو الأنظمة إلى ثلاثة أقسام أخلاقية أو «قبعات». فمن هم أصحاب القبعات السوداء (black hats) وأصحاب القبعات البيضاء (white hats) وأصحاب القبعات الرمادية (gray hats)؟

القبعات البيضاء

المخترقون الذين اتخذوا هذا الخط الأخلاقي هم غالباً ما يمثلون «قوة الخير». إنهم الأخيار في العالم السيبراني، الذين باتوا يعرفون بـ«اختصاصيي الحماية الإلكترونية». عملهم يدور حول إجراء تجارب الاختراق على الأجهزة والخوادم من خلال استخدام سياسات ومنهجيات عبر تطبيق معايير حماية عالمية مثل ما تعتمده «Ec Council» و«Sans Security». هدف هؤلاء إجراء ما يلزم لاكتشاف الثغرات. ظهرت كلمة «مخترق أخلاقي» عند اعتمادها ضمن شركة IBM لإيضاح الفرق بين المخترقين. بحسب تعريف شركة Symantec Norton، يقوم الـ white hat باستخدام أساليب الاختراق نفسها المتعارف عليها في مجتمعات خبراء الأمن الإلكتروني، أي برمجيات الاختراق نفسها، ولكن الفرق الوحيد هو طلب الإذن من الشركات والانظمة الحكومية قبل القيام بهذا العمل، أو تعيينهم من قبلها أو تبليغ المعنيين في حال اكتشاف ثغرة ما من دون استغلالها.

إن الملزمات الأخلاقية لأي مخترق تختلف من فرد إلى آخر. وتاريخياً، تحوّل العديد من الـ black hat إلى white hat، مثل كيفين ميتنك المعروف بـ«كندور»، والذي افتتح شركة حماية إلكترونية بعد تمضيته خمس سنوات في السجون