المستقبل
للأبحاث والدراسات المتقدمة

اسم الموضوع : ستاكسنت 2.0:

عنوان الموضوع : سيناريو افتراضي للهجوم السيبراني على البرنامج النووي الإيراني

تاريخ النشر : 14/04/2021

اسم الكاتب : د. إيهاب خليفة

الموضوع :

أفاد بيان رسمي إيراني بأن مصنع تخصيب اليورانيوم في نطنز تعرض لعمل "إرهابي"، وذلك بعد الإعلان عن "انقطاع التيار الكهربائي" بالمنشأة النووية. في المقابل، تحدثت مصادر استخباراتية إسرائيلية عن وقوف الموساد وراء الهجوم. يأتي الحادث في منشأة نطنز في وقت تحاول فيه طهران وواشنطن إحياء الاتفاق النووي المبرم عام 2015 مع القوى الكبرى بعد أن انسحب الرئيس الأمريكي السابق "دونالد ترامب" منه قبل ثلاث سنوات، لكن مع مجيء إدارة "بايدن" أعلن وزير الدفاع الإسرائيلي "بيني جانتس" "أن إسرائيل تسعى لوضع خيار عسكري على طاولة المفاوضات مع إيران حول برنامجها النووي، وأنه شخصيًا يعمل على ذلك"، ويبدو أن الخيار العسكري هنا كان هو الهجوم السيبراني.فقد جاء استهداف البرنامج النووي الإيراني في عمل عسكري سيبراني بعد يوم واحد من إعلان إيران عن تدشين أجهزة "متطورة" للطرد المركزي تعمل على تخصيب اليورانيوم "بسرعة أكبر" تسمى "آي آر 9"، بما يعني أن المنشأة النووية بالفعل منكشفة للهجمات السيبرانية الإسرائيلية من قبل، وأن الرد السريع والفوري بمجرد تدشين أجهزة الطرد المركزي الجديدة، هو رسالة للإيرانيين بأن أيادي الإسرائيليين داخل المنشأة النووية بالفعل.وقد رد رئيس الوزراء الإسرائيلي مساء يوم إعلان الهجوم على نطنز بأن الموقف الذي يوجد اليوم في التفاوض مع إيران ليس بالضرورة أن يكون موجودًا غدًا، دون إشارة صريحة للهجوم السيبراني على المنشأة النووية الإيرانية، وهو ما يعني أن هناك تقييمًا إسرائيليًا لحجم الخسائر التي تعرضت لها المنشأة والتي قد تكون كبيرة للغاية.ويحاول هذا التحليل وضع سيناريو افتراضي يوضح عملية استهداف منشأة نطنز عبر هجمات سيبرانية قد تكون الجيل الثاني من دودة ستاكسنت التي أصابت نفس المنشأة عام 2009، وكذلك توضيح حدود القوة السيبرانية الإسرائيلية مقارنة بحدود القوة السيبرانية الإيرانية.سيناريو افتراضي.. الاستهداف الثاني لمنشأة نطنز:لم يتضح بعد حجم الخسائر الناجمة عن الهجمات السيبرانية التي استهدفت منشأة نطنز، وقد صرح وزير الخارجية الإيراني بأنه لا توجد خسائر في الأرواح البشرية، ولم يتم رصد أي تسريب لإشعاعات، وقد تم الإعلان عن أنه تم استهداف إمدادات الطاقة الكهربائية المغذية لأجهزة الطرد المركزي الجديدة، وهو ما نجم عنه خروج بعض هذه الأجهزة من الخدمة حسب تصريحات وزير الخارجية الإيراني. لكن هناك عدة مؤشرات تشير إلى أن الخسائر أكبر مما صرح به وزير الخارجية الإيراني، ويمكن توضيح ذلك في التالي:- سرعة استهداف أجهزة الطرد الجديدة فور دخولها الخدمة دليل على أن البرنامج النووي الإيراني منكشف لدى الإسرائيليين من قبل، وذلك عبر أحد سيناريوهين:1- السيناريو الأول- ستاكسنت: استهداف نظم التحكم الصناعي يضع افتراضية أن الجيل الثاني من برمجية ستاكسنت، التي قد تكون متصلة بالإنترنت على عكس الجيل الأول، قد دخلت الخدمة بالفعل، وإن لم تكن متصلة بالإنترنت، فعلى الأقل هناك جاسوس داخل المنشأة أعطى أوامر للبرمجية بالتشغيل.2- السيناريو الثاني- ثغرات صفرية: إن لم يكن ستاكسنت أو إحدى البرمجيات الأكثر تطورًا، فعلى الأقل هناك ثغرات صفرية معروفة لدى الإسرائيليين في نظم التحكم الصناعي الموجودة بالمنشأة النووية، تم رصدها من قبل وتحديدها واستغلالها في الهجمة مؤخرًا.- استهداف نظم إمداد الكهرباء قد يؤدي إلى خروج عدد كبير من أجهزة الطرد المركزي عن الخدمة، وليس عددًا محدودًا مثلما صرح به وزير الخارجية الإيراني.- أشار مصدر استخباراتي أمريكي إلى أن الهجمة على نطنز قد تُعيد البرنامج النووي الإيراني 9 أشهر إلى الخلف.- في كل الحالات، هناك حالة انكشاف كبيرة للبرنامج النووي الإيراني لدى إسرائيل، فعامل السرعة في الرد وحجم الخسائر يضع تساؤلاً كبيرًا حول القدرات التأمينية للمنشأة من الهجمات السيبرانية.قوة كبرى.. القدرات السيبرانية الإسرائيلية:تمتلك إسرائيل قدرات متقدمة في مجال الحرب السيبرانية، حيث توجد بها مراكز أبحاث كبرى لكل من: آبل، وجوجل، ومايكروسوفت، وأمازون، وفيسبوك، كما أنها تحصل على 20% من الاستثمارات العالمية في الأمن السيبراني، فضلاً عن ذلك توجد لديها الوحدة 8200 المسؤولة عن العمليات العسكرية في الفضاء السيبراني.والوحدة 8200 تابعة لشعبة الاستخبارات الإسرائيلية "أمان"، تأسست في عام 1952، وأصبحت مسؤولة عن قيادة وتعتبر أهم وأكبر قاعدة ،US Cyber Command وقيادة الفضاء الإلكتروني، NSA الحرب السيبرانية في الجيش الإسرائيلي، وتُشكل تحالفًا مع وكالة الأمن القومي الأمريكي تجسس إلكترونية إسرائيلية بالنقب للتنصت على البث الإذاعي والمكالمات الهاتفية والفاكس والبريد الإلكتروني في قارات آسيا وإفريقيا وأوروبا، وتم تطويرها بإضافة مهام الحرب على الفضاء الإلكتروني إليها في وقت لاحق.وقد لعبت هذه الوحدة دورًا رئيسيًّا في ضرب البرنامج النووي الإيراني من خلال تصميم فيروس "ستاكسنت"، كما أكد المعلق العسكري الإسرائيلي "عمير رابيبورت" أن الدور الذي تقوم به "وحدة 8200"، قد جعل إسرائيل ثاني أكبر دولة في مجال التنصت في العالم بعد الولايات المتحدة، وأشار "رابيبورت" إلى أن الحواسيب المتطورة التابعة لهذه الوحدة قادرة على رصد الرسائل ذات القيمة الاستخباراتية من خلال معالجة ملايين الاتصالات وملايارات الكلمات.كما أن إسرائيل لا تفرق بين الحرب السيبرانية والحرب المادية، فكلاهما واحد بالنسبة لها، أي إن التلويح بالاستخدام العسكري للقوة يعني أيضًا إمكانية استخدام القوة العسكرية السيبرانية، فمثلاً أعلنت إسرائيل قيامها بشن هجوم عسكري على أحد المباني التي ادّعت أنه يُستخدم من قبل مجموعة من قراصنة المعلومات التابعين لحركة "حماس" لشن هجمات إلكترونية ضد أهداف إسرائيلية لم يتم تحديد نوعيتها، وبذلك يُعتبر هذا الاعتداء الإسرائيلي هو أول رد عسكري على هجوم سيبراني في التاريخ.لم تكن هذه الحادثة هي الأولى لاستهداف منشأة نطنز، بل سبق وتم استهداف أجهزة الطرد المركزي الإيرانية عبر "دودة ستاكسنت" التي تسببت في إخراج ما يقرب من ألف من أجهزة الطرد المركزي عن الخدمة، ولذلك تعتبر ستاكسنت أول نموذج لاستخدام سلاح سيبراني في استهداف البرنامج النووي الإيراني، والتي اعتُبرت حينها من أخطر أنواع الأسلحة السيبرانية التي تم تطويرها، وقد مثلت نقلة نوعية في خطورة الحروب السيبرانية، فبفضل ستاكسنت انتقلت الحرب من تدمير البيانات وسرقتها إلى تدمير المكونات المادية نفسها ونظم التشغيل وليس فقط البيانات.وقد تم اكتشاف ستاكسنت عام 2009 عندما أصابت أجهزة الطرد المركزي الإيراني في منشأة نطنز لتخصيب اليورانيوم، وتسببت في تعطيل وخروج عدد كبير منها عن العمل، حيث استهدفت نظم تشغيل أجهزة الطرد المركزي التي تعمل عبر برنامج من صنع شركة سيمنز الألمانية، وقامت بتسجيل مؤشرات تتعلق بعملية تخصيب اليورانيوم، ثم قامت بالتلاعب بآلية عمل أجهزة الطرد وتخريبها، حيث لدى SCADA التحكم الصناعي ستاكسنت القدرة على إعادة برمجة وحدات التحكم المنطقي القابلة للبرمجة، وإخفاء التغييرات التي تم تنفيذها، وفي الوقت نفسه عرض المعلومات القديمة التي قامت بتسجيلها على الشاشات لكي يظهر الأمر للمراقبين والفنيين بأن كل شيء يسير بصورة طبيعية، حتى نجحت في إنهاء مهمتها.وبصورة عامة، تقوم ستاكسنت بمهاجمه أنظمة التحكم الصناعية المستخدمة على نطاق واسع في المنشآت الهامة، مثل: خطوط نقل النفط، ومحطات توليد الكهرباء، والمفاعلات النووية، وغيرها من المنشآت الاستراتيجية الحسّاسة، وتقوم بالانتقال بين الأجهزة عبر مستغلة إحدى نقاط الضعف في برنامج التشغيل ويندوز.ليس ذلك فحسب، فقد نقلت شبكة "سي إن إن" الإخبارية الأمريكية عن "شون مكجيرك"، رئيس دائرة أمن الإنترنت USB أجهزة بوزارة الأمن الوطني الأمريكية، قوله أمام الكونجرس: "هذه البرمجية يمكن أن تدخل تلقائيًّا في أي نظام، وتسرق صيغة المنتج الذي يتم صنعه، وتغير خلط المكونات في المنتج، وتخدع المشغلين وبرامج مكافحة الفيروسات عبر إيهامهم بأن كل شيء على ما يرام".قوة متوسطة.. القدرات السيبرانية الإيرانية:أولت إيران اهتمامًا كبيرًا بتعزيز قدراتها السيبرانية، وهو ما يتضح في عدد من المؤشرات، فقد تضاعفت الموارد المالية المخصصة لتعزيز قدراتها في هذا المجال، وبلغت الميزانية التي وضعتها إيران لتطوير قدراتها السيبرانية في البداية حوالي 76 مليون دولار أمريكي سنويًا، غير أنه بدءًا من عام 2011، تصاعد الإنفاق الإيراني حتى بلغ حوالي 1 مليار دولار، بهدف امتلاك التكنولوجيا السيبرانية، والبنية التحتية، وتطوير القدرات. كما زعم الحرس الثوري الإيراني في عام 2012 أنه قام بتجنيد حوالي 120 ألف شخص على مدار السنوات الثلاث السابقة.وفيما يتعلق بتقييم القدرات السيبرانية الإيرانية، يُلاحظ أن التقديرات تتضارب في هذا الإطار، ففي حين تبالغ بعض التقديرات في تقييم القدرات السيبرانية الإيرانية، وتقدر أن قوتها تأتي في المرتبة التالية للصين، وهو تقدير مبالغ فيه بدرجة كبيرة؛ فإن بعض التقديرات الأخرى، تصنّفها باعتبارها قوة سيبرانية من الدرجة الثالثة، إذ إنها لا تمتلك قدرات سيبرانية متقدمة، تشابه الدول الرئيسية الفاعلة في هذا المجال، مثل الولايات المتحدة وروسيا والصين وإسرائيل.ويمكن إرجاع تضارب التقييمات إلى عامل مهم، وهو إرجاع بعض الهجمات السيبرانية المتقدمة إلى إيران، في حين أنه بعد فترة من الوقت، عُثر عليها في منشآت بتروكيماوية سعودية، والتي استهدفت (Malware) يتضح وقوف دول أخرى وراءها. ومن ذلك على سبيل المثال، تحميل إيران مسؤولية توظيف برمجيات خبيثة نظم التحكم الصناعي، والتي في حال تم تنفيذ الهجوم سوف يترتب عليه إحداث تفجيرات في المنشأة، غير أنه اتضح لاحقًا أن هذه البرمجيات الخبيثة مرتبطة بالحكومة الروسية. ويمكن القول إنه من خلال عدد من المؤشرات يتضح أن القدرات السيبرانية الإيرانية ليست متقدمة على غرار القوى الكبرى، وهو ما يُستدل عليه من خلال بعض المؤشرات التالية:1- ضعف قدرات إيران الدفاعية السيبرانية: تعاني إيران من تراجع قدراتها السيبرانية الدفاعية، وهو ما يتضح في اعتمادها بصورة أساسية على استخدام قدراتها الهجومية من أجل الرد على الهجمات التي تتعرض لها. ومن ذلك على سبيل المثال، الهجوم السيبراني على شركة أرامكو السعودية في عام 2012 وعام 2016، وكذلك شركة راس غاز القطرية، في الشهر نفسه من أجل الرد على الهجمات السيبرانية التي تعرضت لها.2- التطور المحدود للهجمات السيبرانية المتتالية: إن قدرات إيران السيبرانية الهجومية لا تتطور بصورة كبيرة من هجوم إلى آخر، فقد استخدمت نفس الأدوات السيبرانية في مهاجمة شركة "لاس فيجاس ساندس" في عام 2014، وكذلك في مهاجمة المملكة العربية السعودية بعدها بعامين، وتحديدًا في عامي 2016 و2017.3- تخلف قدرات إيران السيبرانية مقارنة بالدول المتقدمة في هذا المجال: تكشف متابعة الأنشطة السيبرانية الإيرانية بوضوح عن افتقادها إلى التنظيم، والمهنية المتوقعة في الجيوش السيبرانية التابعة للدول، وهو ما يحد من قدراتها على شن هجمات سيبرانية أكثر تعقيدًا، وأنها لم تتمكن بعد من اختراق أي مولد كهربائي، أو أدوات التحكم في شبكات الكهرباء، وهو إن كان مؤشرًا على تفكير إيران في اختراق المحطات الكهربائية بهدف استهدافها، وتعطيلها أو تخريبها في أي أزمة مستقبلية؛ إلا أنه لم يتم رصد أي فيروس إيراني يمتلك هذه القدرة حتى الآن، وهو ما يكشف عن عدم تقدم قدراتها السيبرانية في هذا الإطار.4- قدرات إيران في التجسس وتعطيل المواقع والخدمات ومحو البيانات: يمكن القول إن قوة قدرات إيران في المجال السيبراني تتمحور حول 3 نقاط رئيسية، وهي:- التجسس وجمع المعلومات: وبالتحديد في مجال الطاقة، وتستهدف بصورة رئيسية الولايات المتحدة الأمريكية من خلال محاولة سرقة التقنيات الأمريكية لتطوير البرنامج النووي والصاروخي الإيراني، ولكن ما زالت القدرات الإيرانية أضعف من أن تخترق الدفاعات الأمريكية العسكرية.- تعطيل المواقع والخدمات: وذلك عبر استهداف المواقع الحكومية والخدمية والعسكرية ومحاولة تعطيلها عبر هجمات إنكار الخدمة لإخراج الموقع مؤقتًا عن العمل أو تغيير واجهة الموقع أو الحساب الإلكتروني ووضع شعارات وعبارات تؤيد إيران.- التخريب ومحو البيانات: وتستهدف إيران عبر هذا الأسلوب القطاع الاقتصادي والصناعي وقطاع الطاقة في المملكة العربية السعودية، .وهو أخطر ما في القدرات الإيرانية الحالية لأنه يستهدف قطاعات حيوية، ويعمد فيها إلى التخريب عبر محو البيانات، وليس عبر التدمير المادي للأجهزة حتى الآن