العرب
الأحد 2021/05/02
السنة 43 العدد 12048

هل بدأ العد التنازلي ليوم القيامة السيبراني

تحذيرات من هجمات إلكترونية هائلة تعطل الحياة بأكملها

أصبحت الإنترنت بمثابة الشريان الذي يغذي العالم، ويكمن الخطر الأكبر في استهداف القراصنة الإلكترونيين للبنية الحيوية للشبكة العنكبوتية ببرمجيات خبيثة تستهدف مواطن الضعف في أجهزة توجيه المعلومات على الشبكة، ما يهدد بتعطيل الحياة بأكملها.

سد الثغرات في إنترنت الأشياء ليس حلاً كافيًا

واشنطن – تواجه الولايات المتحدة مشكلة خطيرة في البنية التحتية، لكنها لا ترتبط بالحفر في الشوارع أو الحالة المزرية للمواصلات العامة أو الجسور المتداعية في جميع أنحاء البلاد، بل بما تفرضه تحديات الأمن الإلكتروني التي تواجهها البلاد.

وتعاني البنية التحتية الأميركية من نقاط ضعف خطيرة وملحة رغم أنها غير مرئية إلى حد كبير، ومن غير المرجح أن يتم إصلاحها خلال "خطة الوظائف الأميركية" التي أطلقتها إدارة جو بايدن والتي تبلغ قيمتها 2 تريليون دولار، لكن يمكن لنقاط الضعف هذه أن يتم استغلالها بسهولة لاختراق السيارات وأجهزة الكمبيوتر والهواتف التي تتصل كلها بالإنترنت، والأخطر من ذلك أن الهجمات قد تطال الشركات الأميركية والمستشفيات والمرافق العامة من مسافات بعيدة بفضل البرنامج الذي يساعد على تشغيل أنظمتها، ولن يكون الجيش الأميركي وحتى الوكالات وشركات الأمن الإلكتروني بمنأى عن الخطر المحدق.

> البنية التحتية الأميركية تعاني من نقاط ضعف غير مرئية، إلا أنه من الممكن استغلالها لشن هجمات إلكترونية هائلة

تنشأ مثل هذه الثغرات الأمنية من الأخطاء البرمجية، وأحيانًا يتم اكتشافها في الأجهزة، مثل ثغرة "هجوم دون انتظار" التي سميت بهذا الاسم لأنه ليس من السهل إصلاحها بمجرد اكتشافها.

وتسمح هذه الثغرة الأمنية التي يتم فيها استغلال نقاط الضعف في البرمجيات وثغراتها الأمنية غير المعروفة باختراق أجهزة الآيفون وبرامج البريد الإلكتروني وملفات موظفي الشركات، وحتى أجهزة الكمبيوتر التي تدير السدود وأنظمة التصويت ومحطات الطاقة النووية.

أقفال قديمة

يبدو الأمر كما لو أن أبواب الولايات المتحدة كلها محمية بأقفال قديمة، وتم استخراج نسخ من مفاتيحها لأي شخص لديه ما يكفي من المال لشرائها. والأسوأ من هذا أن الولايات المتحدة نفسها هي التي أتاحت هذه المفاتيح عن غير قصد للحلفاء والأعداء والمبتزين المحتملين على حد السواء.

يمثل الاختراق الأخير لشركة "سولار ويندز"، وكذلك شركات مثل "مايكروسوفت" التي فرضت إدارة بايدن بسببها عقوبات مؤخرًا على روسيا وطردت العديد من موظفي سفارتها، أحدث مثال على كيفية تمكن الدول الأخرى من اختراق البنية التحتية الأساسية للولايات المتحدة. مثل هذه الاختراقات، التي يعود تاريخها فعليًا إلى أوائل القرن الحادي والعشرين، لا تزال في الغالب أكثر من مجرد اختبارات وطرق للتعرف على مدى سهولة اقتحام تلك البنية التحتية بطريقة أكثر جدية في وقت لاحق.

ومع ذلك، يتسبب القراصنة أحيانًا في إحداث ضرر من خلال تفريغ البيانات أو محو الأنظمة، خاصة إذا فشلت الأهداف في دفع الفدية الإلكترونية. وبشكل أكثر دهاءً يمكن للقراصنة أيضًا زرع "قنابل زمنية" قادرة على الانفجار في وقت ما في المستقبل.

التأثير المدمر

اخترقت كل من روسيا والصين وكوريا الشمالية وإيران البنية التحتية لهذه الدولة من أجل سرقة أسرار الشركات أو سرقة المعلومات الشخصية أو إحراج الوكالات الفيدرالية أو جني الأموال أو التأثير على الانتخابات. أما الحكومة الأميركية فليست سوى ضحية بريئة لمثل هذه الأعمال، على الرغم من أنها كانت رائدة في هذا المجال، ولا تزال تواصل ريادتها في العمليات السيبرانية في الخارج.

وتتمتع هذه الدولة كذلك بتاريخ طويل في صنع الأسلحة التي استخدمت لاحقًا ضدها.

وعندما يتحول الحلفاء فجأة إلى أعداء، مثل الحكومة الإيرانية بعد الإطاحة بالشاه في ثورة 1979 أو المجاهدين في أفغانستان بعد انتهاء حربهم ضد الجيش الأحمر في عام 1989، تتغير الأسلحة أيضًا. وفي حالات أخرى، مثل القنبلة الذرية أو المركبات الجوية المسيرة، تتفوق المعرفة بأحدث التطورات التكنولوجية، مما يؤدي إلى سباق تسلح.

ومع ذلك، في كل هذه السنوات لم يتم استخدام أي من هذه الأسلحة بمثل هذا التأثير المدمر ضد الولايات المتحدة مثل تكنولوجيا الحرب الإلكترونية.

وفي عام 2009 بدأت أجهزة الطرد المركزي، القادرة على تخصيب اليورانيوم الإيراني إلى مستوى إنتاج الأسلحة، تتعطل. في البداية لم يهتم المهندسون هناك كثيرًا بالمشكلة. كانت أجهزة الطرد المركزي عالية السرعة عرضة لأعطال متكررة. وكان على الإيرانيين استبدال ما يصل إلى واحد من كل 10 منهم بشكل منتظم. لكن هذه المرة بدأ عدد الأعطال في التكاثر ثم التكاثر مرة أخرى، بينما بدأت أجهزة الكمبيوتر التي تتحكم في أجهزة الطرد المركزي تتصرف بشكل غريب أيضًا.

وفي عام 2010 فحص مختصون في أمن الكمبيوتر من بيلاروسيا أجهزة الكمبيوتر الإيرانية واكتشفوا تفسير كل الأعطال. ووجدوا أن الجاني المسؤول عن ذلك هو فايروس تمكن من اختراق أعماق تلك الأجهزة من خلال سلسلة من ثغرات "هجوم بلا انتظار".

وكان ذلك الفايروس الملقب بـ "ستاكس نت" الأول من نوعه. ومن المسلم به أن فايروسات الكمبيوتر كانت تخلق الفوضى تقريبًا منذ فجر عصر المعلومات، لكن هذا كان شيئًا مختلفًا. لا يمكن لـ"ستاكس نت" إتلاف أجهزة الكمبيوتر فحسب، بل أيضًا الآلات التي تتحكم فيها أجهزة الكمبيوتر، مما أدى في هذه الحالة إلى تدمير حوالي 1000 جهاز طرد مركزي.

وهذا الفايروس طورته وكالات الاستخبارات الأميركية بالتعاون مع الإسرائيليين، وثبت أن "ستاكس نت" ليست سوى وابل واحد في الحرب الإلكترونية التي لا تزال مستمرة حتى يومنا هذا.

لم يمض وقت طويل قبل أن تطور الدول الأخرى إصداراتها الخاصة من "ساكس نت" لاستغلال نفس النوع من هذه الثغرات.

وتصف نيكول بيرلروث، مراسلة نيويورك تايمز، في كتابها "ذيس إز هاو داي تيل مي ذا وورلد إندز" (هكذا يحدثونني عن نهاية العالم) بالتفصيل كيف تصاعد سباق التسلح الإلكتروني الجديد. وقد استغرق الأمر من إيران ثلاث سنوات فقط للرد على"ساكس نت" من خلال إدخال برامج ضارة إلى شركة النفط السعودية أرامكو، مما أدى إلى تدمير 30 ألفاً من أجهزة الكمبيوتر الخاصة بها. وفي عام 2014 نفذت كوريا الشمالية هجومًا مشابهًا على شركة "سوني بيكتشرز" رداً على فيلم تخيل اغتيال زعيم هذه الدولة، كيم جونغ أون. وفي الوقت نفسه، ووفقًا لتقرير بيرلروث، استهدف القراصنة الصينيون الشركات الأميركية للاستحواذ على الملكية الفكرية، بدءًا من تقنية الليزر وتوربينات الغاز عالية الكفاءة إلى خطط طائرات أف – 35 وصيغ طلاء كوكا كولا و"بنجامين مور".

وعلى مر السنين أصبحت روسيا بارعة بشكل خاص في التكنولوجيا الجديدة، حيث تدخل قراصنة يديرون الكرملين في الانتخابات الرئاسية الأوكرانية عام 2014 في محاولة لدعم مرشح يميني متطرف. وفي العام التالي أغلقوا شبكة الكهرباء في أوكرانيا لمدة ست ساعات. وفي البرد القارس في ديسمبر 2016 أوقفوا التدفئة والطاقة في كييف، عاصمة أوكرانيا. ولم تكن أوكرانيا فقط التي تم استهدافها، بل تسبب القراصنة الروس في إصابة إستونيا بالشلل، وتدخلوا في استفتاء خروج بريطانيا من الاتحاد الأوروبي، وكادوا يغلقون ضوابط السلامة في شركة نفط سعودية.

ثم بدأت روسيا في تطبيق كل ما تعلمته من هذه الجهود على مهمة اختراق الشبكات الأميركية. وفي الفترة التي سبقت انتخابات عام 2016 استغل القراصنة الروس المعلومات المسروقة من عضو الحزب الديمقراطي جون بوديستا وشقوا طريقهم إلى الأنظمة الانتخابية على مستوى الولاية. وفي وقت لاحق شنوا هجمات ببرامج فدية ضد البلدات والمدن الأميركية، واخترقوا المستشفيات الأميركية، بل ودخلوا إلى محطة وولف كريك للطاقة النووية في كانساس.

لم تقف الولايات المتحدة مكتوفة الأيدي أمام مثل هذه التوغلات؛ إذ اخترقت وكالة الأمن القومي شركات صينية مثل "هواوي"، وكذلك عملائها في دول مثل كوبا وسوريا. ومن خلال خطة أطلق عليها اسم "نيترو زيوس" كانت الولايات المتحدة مستعدة لإزالة عناصر البنية التحتية الرئيسية في إيران إذا فشلت المفاوضات حول الاتفاق النووي. ورداً على اختراق شركة "سوني" دبرت واشنطن انقطاعاً للإنترنت استغرق 10 ساعات في كوريا الشمالية.

وكما كشفت التسريبات من المخبر إدوارد سنودن في عام 2013، أنشأت وكالة الأمن القومي نظام مراقبة كاملا من خلال شبكات اتصالات مختلفة، واستطاعت أن تخترق حتى الهواتف الخاصة لزعماء في جميع أنحاء العالم مثل الألمانية أنجيلا ميركل. وبحلول عام 2019، وبعد أن عززت ميزانيتها السنوية إلى ما يقرب من 10 مليارات دولار وأنشأت 133 فريقًا للبعثة السيبرانية يعمل بها 6 آلاف موظف، كانت القيادة الإلكترونية في البنتاغون تزرع برامج ضارة في شبكة الطاقة الروسية وتخطط لأضرار أخرى.

وكانت وكالة الأمن القومي تخزن أيضًا كنزًا دفينًا من ثغرات "هجمات دون انتظار" لاستخدامها المحتمل ضد مجموعة من الأهداف. ولكن بعد ذلك تم اختراق وكالة الأمن القومي.

وفي عام 2017 سربت جماعة تُدعى "شادو بروكرز" 20 من أقوى ثغرات "هجمات دون انتظار" الخاصة بالوكالة. وفي شهر مايو من العام نفسه بدأت هجمات "وانا كراي"الإلكترونية فجأة تضرب أهدافا متنوعة مثل المستشفيات البريطانية وشركات الطيران الهندية ومحطات الوقود الصينية والمرافق الكهربائية في جميع أنحاء الولايات المتحدة. ومن المحتمل أن يكون الجناة كوريين شماليين، لكن الكود نشأ في الأصل في وكالة الأمن القومي، ووصلت فاتورة الخسائر إلى 4 مليارات دولار.

وحتى لا يتم تجاوزهم قام القراصنة الروس بتحويل اثنين من الثغرات الخاصة بوكالة الأمن القومي إلى فايروس يسمى "نوت بتيا"، مما تسبب في إحداث المزيد من الضرر. وكان الهدف في البداية تدمير أوكرانيا، وانتشرت هذه البرامج الضارة بسرعة في جميع أنحاء العالم، مما تسبب في إحداث خسائر لا تقل عن 10 مليارات دولار عن طريق إغلاق شركات مثل "ميرك" و"ميرسك" و"فيديكس" وعملاق النفط الروسي "روزنيفت" لفترة وجيزة.

وفي عام 2021 كتبت كيم زيتر، الصحافية الاستقصائية والمؤلفة الأميركية، في كتابها "كاونت داون تو زيرو داي" (العد التنازلي ليوم الصفر) أنه "يمكن الحصول على الأسلحة السيبرانية بسهولة من أسواق مشبوهة، أو اعتمادًا على مدى تعقيد النظام المستهدف، ويتم بناؤها حسب الطلب من البداية على يد مبرمج مراهق ماهر"، ثم تنتشر مثل هذه الأسلحة حول العالم قبل أن تعود في أغلب الأحيان إلى المرسل.

وعاجلاً أم آجلاً، ستعود مثل هذه الأسلحة إلى حيث تم إنشاؤها أول مرة.

واستنكر دونالد ترامب التدخل الروسي في انتخابات عام 2016. لكن مساعديه لم يبذلوا جهدا إضافيا لطرح أمثلة كافية على التدخل السيبراني الروسي لأن الرئيس لم يكن مهتمًا بذلك.

وفي عام 2018 قام ترامب بإلغاء منصب منسق الأمن السيبراني الوطني، مما ساعد مستشار الأمن القومي جون بولتون على تعزيز سلطته داخل الإدارة. وفي وقت لاحق أقال ترامب كريستوفر كريبس، الذي كان مسؤولاً عن حماية الانتخابات من الهجمات الإلكترونية، لتأكيده على نزاهة الانتخابات الرئاسية لعام 2020.

وسلط هجوم "سولار ويندز" في نهاية العام الماضي الضوء على الضعف المستمر لسياسة الأمن السيبراني في هذه الدولة وإنكار ترامب لهذه الحقيقة. وحتى بعد أن تمت مواجهته بأدلة من وكالات مخابراته على تورط روسي واصل الرئيس الإصرار على أن الجناة كانوا صينيين.

وعزز اليمين المتطرف الموقف المنكر من قبل الرئيس لأسباب حزبية. ومن الغريب أن المعلقين اليساريين حاولوا بالمثل السخرية من فكرة تورط الروس في اختراق "بوديستا" والتدخل في انتخابات 2016 وعمليات اقتحام سيبريانية أخرى، على الرغم من الأدلة الدامغة المقدمة في تقرير مولر ونتائج لجنة الاستخبارات في مجلس الشيوخ، وحتى أدلة المصادر الروسية.

حرب الكمبيوتر

لكن هذا الإنكار لليمين واليسار يحجب فشل إدارة ترامب، وهو الأكثر أهمية. هذا الفشل ظهر أيضاً من خلال عدم القدرة على العمل مع روسيا والصين لتنظيم هدنة في تصعيد التوترات الإلكترونية العالمية.

وبسبب هجوم "ستاكسنت" على إيران اقترحت حكومة بوتين بالفعل في عدة مناسبات أن على المجتمع الدولي أن يوقع معاهدة لحظر حرب الكمبيوتر وأن على موسكو وواشنطن أيضًا ترتيب شيء مماثل على المستوى الثنائي. تجاهلت إدارة باراك أوباما مثل هذه المبادرات، ولم ترغب في تقييد قدرة دولة الأمن القومي على شن عمليات إلكترونية، وهو ما يحب البنتاغون وصفه باستراتيجية "الدفاع إلى الأمام".

وخلال سنوات عهدة ترامب، حتى عندما كان يسحب الولايات المتحدة من صفقة للحد من الأسلحة مع الروس، كان يشدد على علاقته الرائعة مع فلاديمير بوتين. وبدلاً من حماية الرئيس الروسي مرارًا وتكرارًا –بغض النظر عن الأسباب الشخصية والمالية والسياسية للقيام بذلك– كان بإمكان ترامب استخدام مهاراته "العظيمة" في التعامل مع فن الصفقة لإحياء مقترحات بوتين الخاصة بعقد هدنة إلكترونية.

ولكن مع الصين، ارتكبت إدارة ترامب خطأ أكثر خطورة.

وبسبب سلسلة من السرقات الإلكترونية الصينية، ليس فقط سرقة الملكية الفكرية وإنما أيضا سرقة الملايين من ملفات التصاريح الأمنية للموظفين الفيدراليين، توصلت إدارة أوباما إلى اتفاق مع بكين في عام 2015 لوقف التجسس المتبادل في الفضاء الإلكتروني.

وقال أوباما حينها "لقد اتفقنا على أن الولايات المتحدة والحكومة الصينية لن تجريا أو تدعما عن قصد سرقة الملكية الفكرية الالكترونية، بما في ذلك الأسرار التجارية أو غيرها من المعلومات التجارية السرية من أجل تحقيق منفعة تجارية. سنعمل معًا ومع الدول الأخرى لتعزيز قواعد أخرى لهذا المجال".

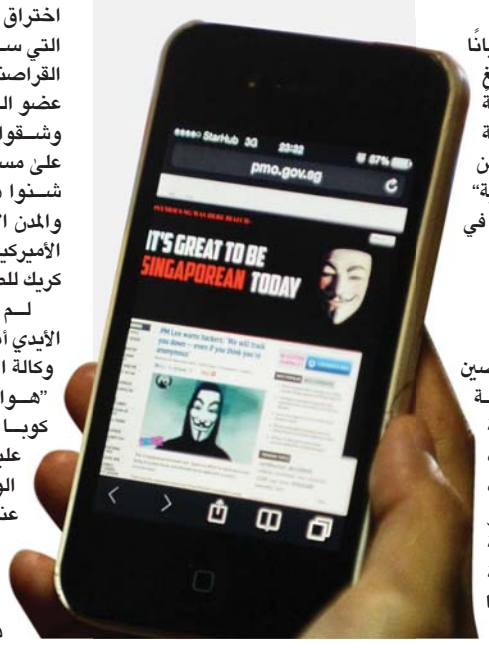
وفي أعقاب تلك الاتفاقية تراجعت التدخلات الصينية في البنية التحتية الأميركية بنسبة مذهلة بلغت 90 في المئة. ثم تولى ترامب منصبه وبدأ في فرض رسوم جمركية على البضائع الصينية. وهذه الحرب التجارية مع بكين ستدمر المزارعين والمصنعين الأميركيين، بينما تزيد من فواتير المستهلكين الأميركيين، حتى في الوقت الذي جعل فيه الرئيس من الصعب على الشركات الصينية شراء المنتجات والتكنولوجيا الأميركية. ومن ثم لجأت الصين مرة أخرى إلى قراصنتها لاكتساب المعرفة التي لم يعد بإمكانها الحصول عليها بشكل شرعي. وفي عام 2017 استولى هؤلاء القراصنة أيضًا على المعلومات الشخصية لما يقرب من نصف الأميركيين من خلال اختراق وكالة تقارير الائتمان "إكويفاكس".

وكجزء من تصميمه على تدمير كل ما حققه أوباما، بالطبع، تجاهل ترامب تمامًا اتفاقية تلك الإدارة لعام 2015 مع بكين.

وعمل رجل الأعمال الأميركي لاري هول سابقا في وزارة الدفاع، ولكنه الآن يبيع شققًا فاخرة في مخبأ نووي فاخر مصمم لحماية الأغنياء من النهاية المحتملة لكوكب الأرض، في وسط كانساس تبلغ مساحته 15 طابقًا تحت الأرض، ويسميها "سيرفايفال كوندو".

وتناهز تكلفة أصغر الوحدات السكنية 1.5 مليون دولار، ويحتوي المجمع السكني على صالة ألعاب رياضية وحمام سباحة وميدان للرماية في مساحته المشتركة تحت الأرض. وعندما سئل عن سبب قيامه ببناء هذا المبنى قال هول "أنت حقاً لا تريد أن تعرف السبب".

> ثغرة «هجوم دون انتظار» ليس من السهل إصلاحها بمجرد اكتشافها، وتستغل نقاط ضعف البرمجيات وثغراتها الأمنية غير المعروفة



كيم زيتر:
يمكن الحصول على أسلحة سيبرانية بسهولة من أسواق مشبوهة، ثم تنتشر مثل هذه الأسلحة حول العالم