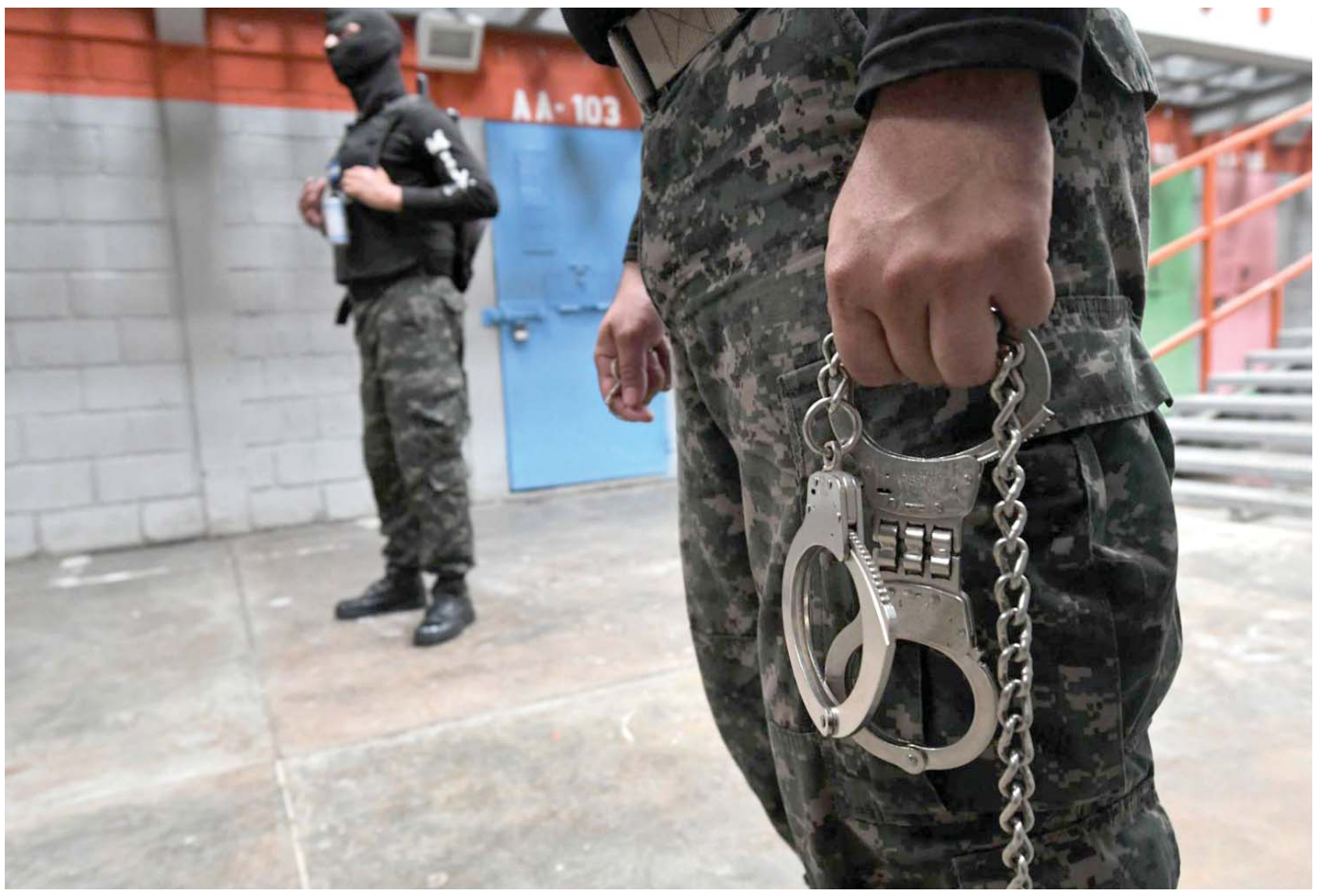
العرب
الأحد 2019/10/13
السنة 42 العدد 11496

التأهب كلمة السر في مواجهة التهديدات الأمنية المبتكرة

القانون وقيود الشركات لا يوفران المرونة الأمنية المطلوبة لمواجهة خصم يجدد أساليبه



ماذا ينفع إغلاق باب الإسطبل بعد هرب الحصان

واشنطن - تعد أقسام الأمن في الشركات بجميع أنحاء العالم أساسية. وفي حين تفتخر هذه المؤسسات بقوة أمنها، إلا أنها غالبا ما تفتقر إلى المرونة وهي سمة يمتلكها خصومها. وتشدد قدرات الخصوم المتطورة على الحاجة إلى التأهب وتوقع التهديدات التي قد تأتي في أي وقت.

وتبقى اليقظة المستمرة أمرا بالغ الأهمية لمواجهة عدوّ يستغل كل الموارد المتاحة أمامه.

خصص سكوت ستيوارت، محلل قضايا الإرهاب والأمن، في مركز ستراتفور للأبحاث الأمنية الاستخباراتية، أحدث تحليلاته ليسلط الضوء على أهمية التأهب في مواجهة التهديدات الأمنية المبتكرة، لافتا إلى أن المثل القائل إن "الحاجة هي أم الاختراع"، ينطبق على الجرائم أيضا.

ويلفت ستيورت إلى أنه لا فرق في الخطر سواء أكانت المسألة مرتبطة بتهديدات الإرهاب، أم بالمجرمين وجواسيس الشركات والناشطين.

جاءت فكرة الحديث عن هذا الموضوع خلال مشاركة ستيوارت في ندوة بشيكاغو شملت تبادل الخبرات في مجال الأمن العالمي. ناقش خلالها المشاركون التحديات الخاصة التي يواجهها الأمن.

سكوت ستيوارت

يجب على المسؤولين في أقسام الأمن الاستعداد للمعركة المحتملة القادمة، بدلا من الاكتفاء بالتركيز على المعركة المنتهية

ويقول ستيوارت إن الحديث مع عدد المشاركين قاده إلى اكتشاف شيء ما وهو أنه: سواء كان العدو مجرما أو جاسوسا أو ناشطا، فإن كل تهديد يمتاز بالقدرة على التكيف مع الإجراءات الأمنية وبالإبداع من حيث القدرة على ابتكار حلول لتجاوز أي عقبة. لكنه أدرك جمود أقسام الأمن في الشركات والبرامج التي يصممونها، حيث إنهم غير مرنين؛ فالعديد من اختصاصيي الأمن سواء من الجيش أو من وحدات إنفاذ القانون (أو كليهما، مثل حالته)، ينتمون إلى خلفيات مختلفة تميل إلى التقاط العديد من السمات التي تعطل هذه المؤسسات خلال العمل فيها.

عموما، يحمل الأشخاص الذين ينتمون إلى الجيش أو وحدات إنفاذ القانون قدرة هائلة على التنظيم، لكن غالبا ما يعجزون أمام التغيير. يقول ستيوارت "حتى نكون منصفين، لا يستطيع العاملون في أقسام أمن الشركات اتباع منهجياتهم الخاصة، على عكس خصومهم. ولا يتمتع الموظفون بأي خيار لا يعني اتباع معايير الشركات وإرشادات الصناعة والعمل ضمن قيود القانون المدني والجنائي".

يمكن أن يضع غياب المرونة البرامج الأمنية في وضع حساس أمام خصم قابل للتكيف.

في النهاية، إذا أرادت أقسام الأمن البقاء في الصدارة، فعليها أن تخطط لمواجهة التهديد المحتمل بدلا من الاكتفاء بالترقب للرد على الهجوم الأخير.

مهاجمون مرنون

لا يشك أحد في مرونة المجرمين وإبداعهم. وكلما كانت المكافأة أكبر، كلما زاد إبداع المخالفين للقانون. وينطبق هذا على مهربي المخدرات الذين يلعبون لعبة القط والفأر مع قوات الأمن منذ عقود؛ اضطر هؤلاء الأفراد إلى تكييف أوضاع التهريب وأساليبه استجابة لاستراتيجيات قوات إنفاذ القانون. ويستخدم هؤلاء المهربون مجموعة من الأساليب لنقل بضاعتهم عن طريق الجو أو البحر أو البرّ أو حتى تحتها، كما تمكنوا من نقل المواد غير القانونية عبر الحدود تحت أغطية مختلفة.

لكن الحيلة والإبداع تمتد إلى المجرمين الآخرين؛ طورت بعض الجهات أجهزة لوضعها على الصرافات الآلية وغيرها من الفتحات التي تدخل فيها بطاقة الائتمان لسرقة معلومات المالك. وبالمثل، طوّرت بعض مجموعات سرقة البضائع مراقبة إلكترونية متطورة وماسحات ضوئية للكشف عن أجهزة نظام تحديد المواقع العالمي المخفية في شحنات البضائع وتشويشها. وستستخدم بعض المجموعات أجهزة التشويش على نظام تحديد المواقع العالمي لحجب الإشارة في حالة عدم تفطنها لبعض أجهزة التتبع.

وأثبت الجواسيس في مجال الصناعة قدرتهم على توظيف طرق مختلفة للحصول على المعلومات التي يحتاجونها.

يمكن أن تكون الطرق التي يتخذونها تقليدية مثل التسلل إلى مكان يمنع عليهم الدخول إليه، ويمكن أن يشنوا حملة تصيد احتيالي أو قرصنة كما يستطيعون تجنيد موظف من الداخل يمكنه الوصول إلى المعلومات التي يحتاجونها.

وأظهر جواسيس الشركات وأولئك الذين يجندونهم القدرة على التكيف لمواجهة التغييرات التي تطال السياسات والإجراءات الأمنية.

للحصول على أدلة تؤكد ما ذكر، لا تنظر إلى أبعد من شركة أبل؛ بعد أن اكتشفت الشركة جاسوسا كان يحاول تنزيل المعلومات الحساسة عبر منفذ "يو.أس.بي"، قررت تعطيل هذه المنافذ الموجودة على الأجهزة التي يدخل إليها الموظفون.

وأجبر ذلك العميل الثاني على التكيف والتقاط صور للمستندات الحساسة الظاهرة على شاشة الكمبيوتر باستخدام هاتفه المحمول.

الجماعات المسلحة

يخصص ستيوارت حيزا هاما للجماعات المسلحة، مشيرا إلى أنها تحمل سجلا يبرز مرونتها وقدرتها على انتهاز جميع الفرص المتاحة. ولا يوجد دليل أوضح من تاريخ الهجمات على الطائرات؛ التجأ الماركسيون والكوبيون المناهضون لكاسترو والكارتلات الكولومبية والسيخ والجهاديون وحتى ضباط المخابرات الكورية الشمالية والليبية إلى اختطاف الطائرات أو تفجيرها.

ومن المفاتيح البارومترية والخلايا الإلكترونية إلى قنابل الأحذية والملابس الداخلية، وظّف أولئك الذين يرغبون في مهاجمة الطائرات مجموعة من التكتيكات لتمرير أجهزتهم القاتلة عبر نقاط التفتيش وتفعيلها.

ويقف الباحث الأميركي عند تفجيرات الحادي عشر من سبتمبر مشيرا إلى أنه خلال التخطيط لهذه الهجمات، درس تنظيم القاعدة نظام الفحص الأمني الذي تعتمده شركات الطيران وبحثت عن طرق لاستغلال نقاط الضعف التي يعاني منها.

وفي صباح الـ11 من سبتمبر 2001، اختطف الجهاديون 4 طائرات باستخدام سكاكين الجيب، حيث لم تمنع القواعد الأمنية الركاب من حمل هذه الأدوات إلى الطائرة في تلك الفترة. وتحدث زعيم تنظيم القاعدة أيمن الظواهري في الذكرى الـ18 لهجمات 11 سبتمبر، وحث أتباعه على شن هجمات ضد المصالح الأميركية والغربية، وشجعهم على الابتكار في هذا المجال.

ويتمتع الناشطون بهذه القدرة على التكيف؛ خلال العقد الماضي، وسّع البعض أنشطتهم المباشرة بطرق تجاوزت التركيز على شركة مستهدفة معينة. وتحولوا إلى الضغط على المؤسسات المالية والموردين والعملاء وغيرهم ممن يتعاملون مع الشركة المعنية. كما يعتمدون تطبيق عدد من الأساليب المباشرة المختلفة لإبقاء انتباه الأمن الذي يستهدفونه مشتتا مثل التجمع أمام منزل المدير التنفيذي.

مواجهة الخصوم

مثل أي تهديد، تتمثل خطوة مواجهة الخصم الأولى في الاعتراف بوجود المشكلة، ثم اتخاذ خطوات لمعالجتها. في هذه الحالة، يعني ذلك فهم ضرورة تعديل البرامج والسياسات والإجراءات الأمنية حتى تصبح مرنة بما يكفي لتوقع التهديد المتغير باستمرار. لكن تعديل الإجراءات الأمنية بعد الهجوم لا يكفي، إذ يجب على المسؤولين في أقسام الأمن الاستعداد للمعركة القادمة بدلا من التركيز على المعركة المنتهية. يتطلب هذا تحديد منبع التهديد حتى تتمكن الدوائر الأمنية من اتخاذ خطوات استباقية لتفادي المهاجمين المحتملين والتخفيف من التهديد بدلا من مجرد الرد على هجوم حدث بالفعل.

يعدّ التركيز على تكتيكات المخالفين أفضل طريقة للتعرف على مصادر التهديد. في مركز ستراتفور، يشير المحللون إلى ضرورة الانتقال من التركيز على هوية الخصوم إلى كيفية عملهم. ويعدّ الأمر مهمّا نظرا إلى قدرة مجموعة متنوعة من الجهات الفاعلة على تبني التكتيكات التي يستخدمها الآخرون. كما يضمن التركيز على الكيفية بدلا من الهوية، التفطنَ إلى علامات الهجوم الوشيك.

يسمح التركيز على التكتيكات للمسؤولين الأمنين بمراقبة الاتجاهات الجديدة وبناء توقعات تفصّل التهديدات القادمة. تعلم أمن المطار هذا الدرس في سنة 2009، بعد أن جاء جهادي ادّعى توبته إلى نائب وزير الداخلية السعودي للشؤون الأمنية الأمير محمد بن نايف. في أغسطس 2009. زعم الجهادي أنه ينوي طلب العفو من الأمير، إلا أنه فجّر عبوة ناسفة مخبأة في أحشائه. فشل الإرهابي في اغتيال الأمير، لكن القاعدة لاحظت نجاحها في إخفاء عبوة ناسفة. وسعت إلى تهريب المتفجرات على متن طائرة متجهة إلى ديترويت في ديسمبر 2009 في ملابس أحدهم الداخلية. لكنها فشلت. ولم يكن ذلك بفضل أمن المطار، إذ لم تنفجر المواد الناسفة وتمكن الركاب من السيطرة على الإرهابي.

يكمن الحل الآخر الذي يمكن أن يساعد على هزيمة المهاجمين المحتملين في حرمانهم من القدرة على تنظيم عمليات المراقبة، حيث منح الخصوم حرية في مراقبة المعدات والإجراءات الأمنية مما ساعدهم على التخطيط لهجماتهم.

لذلك، يجب تدريب موظفي الأمن على التعرف على علامات المراقبة العدائية واتخاذ إجراءات لإيقافها. كما تشمل الشركات مناطق يجب أن يتواجد فيها شخص لمراقبة الأنشطة التي تجري فيها مباشرة. يساعد هذا على استباق الهجمات، ولا يجب إبقاء الأنظمة مجرّد آلية تسجل النشاط لمراجعته بعد وقوع الحادث.

ويخلص ستيورات إلى أن قيود الشركات والقانون لن يوفرا المرونة التي يحتاجها أفراد الأمن لمواجهة الخصم الذي يجدد أساليبه. حيث يعدّ توقع كيفية حدوث الهجوم التالي ووضع برامج استباقية لتعطيله، أمرا أساسيا إذا أرادت الشركات أن تبقى متقدمة على منافسيها. ويبقى أي إجراء آخر بمثابة إغلاق باب الإسطبل بعد هرب الحصان.

برمجيات خبيثة تتجسس على الدبلوماسيين بأساليب غير معتادة

سيرجيو غاتلان

اكتشف باحثون في شركة إسيت لأمن تكنولوجيا المعلومات في براتيسلافا برامج ضارة جديدة مصممة لاستهداف الشخصيات الدبلوماسية والحكومية. استخدمت هذه البرامج في الهجمات ضد الأفراد الناطقين بالروسية لمدة 7 سنوات على الأقل.

تسلّحت برامج التجسس الخبيثة التي أطلق عليها الباحثون اسم "أتور" ببعض الميزات المبتكرة بما في ذلك استخدام الوحدات المشفرة والاتصالات القائمة على شبكة تور الخفية وبرامج المساعدة المصممة خصيصا لـ"جي. أس.أم" (النظام الموحد للاتصالات المتنقلة).

وقالت محللة البرمجيات الخبيثة في شركة إسيت، زوزانا هروموكوفا "يركز المهاجمون الذين يستخدمون أتور على البعثات الدبلوماسية والمؤسسات الحكومية". وأشارت إلى أن "هذه الهجمات بدأت منذ سنة 2013 على الأقل. وهي موجهة إلى المستخدمين الروس، وخاصة أولئك الذين يهتمون بخصوصياتهم".

ويشير الصحافي المحلل سيرجيو غاتلان، المتخصص في الأمن الإلكتروني، إلى أن أتور صمم باستخدام هياكل نمطية، مع وحدات تم تطويرها خصيصا من أجل التسلل وجمع البيانات وتجنب البرمجيات المضادة للبرامج الضارة.

وعثرت شركة إسيت على 8 وحدات (تعرف أيضا باسم البرامج المساعدة)، وتشمل برنامج تثبيت، وبرنامج مراقبة، ومسجل صوت، ومصور شاشة، ومسجل كلمات سر، ومحمل ملفات، ووحدة اتصال.

ولفت غاتلان، في متابعته لهذه القضية، في موقع "بلبينغ كمبيوتر"، إلى أنه أثناء تحليل حالات عدد من ضحايا أتور، اكتشفت شركة إسيت أن البرامج نقلت إليهم عبر وحدة إرسال تستخدم أساليب تشفير متعددة وتقنيات تساعدها على التخفي داخل الأجهزة المصابة. ويحقن هذا البرنامج نفسه في معظم العمليات التي تجرى على الأجهزة التي تعرضت للاختراق، باستثناء تلك التي تتضمن برامج شركة سيمانتك المتخصصة في مجال الأمن وإدارة المعلومات والعديد من عمليات نظام التشغيل.

بعد ذلك، يفعّل أتور آلية المراقبة وجمع البيانات عبر تحميل البرامج المساعدة التي تظهر كملفات مكتبة الربط الديناميكي المشتركة في نظام مايكروسوفت ويندوز.

وحسب شركة إسيت، يستهدف أتور عمليات محددة من بينها العمليات المرتبطة بالشبكات الاجتماعية الروسية وبعض الأدوات المساعدة على التشفير الرقمي، والبرامج التي تعالج إعدادات الشبكة الخاصة الافتراضية، وخدمات تشفير البريد الإلكتروني مثل هاشميل، وبرنامج تروكربت الذي يستعمل في تشفير الملفات والأقراص.

تخزّن البرامج المساعدة "مضغوطة ومشفّرة"، وتفعّل عندما تتلقى إشارة من المرسل الذي يحمّل البرامج الإضافية. وتعدّ هذه محاولة لإخفاء هذه البرمجيات لأنها دائما ما تظهر مشفرة.

برنامج «أتور» الخبيث صمم باستخدام هياكل نمطية، مع وحدات تم تطويرها خصيصا من أجل التسلل وجمع البيانات وتجنب البرمجيات المضادة للبرامج الضارة

وقال تقرير أعدته شركة إسيت إن أتور يحمل آليات تمكنه من إضافة برامج مساعدة إضافية جديدة، ومن تحديث نفسه. كما يستطيع أن يغير مواقع الملفات التابعة له لحمايتها.

ويتمثل البرنامج المساعد الأبرز الذي يحمله أتور في آلية لمراقبة الجهاز، وتشمل وحدة تستخدم البيانات الوصفية التي تم تجميعها من أجهزة الهاتف والتخزين والـ"مودم" المتصلة بالجهاز. كما يستخدم هذا البرنامج المساعد الآليات التي تم تطويرها خلال الثمانينات للتسلل إلى الأجهزة المتصلة بالمنافذ التسلسلية في الكمبيوتر المصاب.

وتعتقد إسيت أن هذا البرنامج المساعد يستخدم لاستهداف أجهزة الـ"مودم" والهواتف القديمة واسترداد العديد من معرفات المشتركين والأجهزة مثل هوية مشترك الجوال الدولية والهوية الدولية للأجهزة المحمولة.

وقالت هروموكوفا، "يمكن أن يوظف ذلك لتأسيس قاعدة لسرقة المزيد من البيانات. إذا عرف المهاجمون نوعية الجهاز المتصل، فيمكنهم صياغة مكوّن برنامج مساعد إضافي يمكنه سرقة البيانات من هذا الجهاز وإدخال تغييرات عليه، بما في ذلك تغيير برامج الجهاز الثابتة".

وسمح استخدام أتور لتقنيات الاتصال التي توفرها شبكة تور على إبقائه مخفيا، حتى بعد استخدامه في هجمات ضد أهداف بارزة منذ سنة 2013 على الأقل. وعلى الرغم من أنهم كانوا قادرين على تحليل حالات البعض من الضحايا، فالباحثون في إسيت لم يتمكنوا من تحديد كيفية وصول البرامج الضارة الأولى وحجم البيانات الكاملة التي صممت لجمعها.

وأضافت شركة إسيت "تشير إصدارات البرمجيات في البرامج المساعدة إلى وجود برامج إضافية أخرى لم نجدها بعد. ومع ذلك، يوفر بحثنا نظرة عميقة تبرز وجود هذه البرامج الضارة، ويؤكد الحاجة إلى تتبع عمليات المجموعة التي تقف وراء هذه البرامج الضارة".