العرب
الأحد 2021/05/09
السنة 43 العدد 12055

حروب من نوع آخر: الفدية الرقمية وقود هجمات معلوماتية

مافيا الإجرام الإلكتروني تنشط في ملاذات بعيدة عن أجهزة إنفاذ القانون

نمت شعبية برنامج الفدية بشكل ملحوظ خلال السنوات العشر الماضية لاسيما في ظل التوترات السياسية بين واشنطن وموسكو التي غذت القرصنة المعلوماتية، حيث صارت هذه الهجمات الإلكترونية التي تستهدف المال أبرز تهديد للبرامج الضارة في العالم حسب تقرير يوروبول.

قراصنة أكثر قسوة

بوسطن (الولايات المتحدة) – **طغى التوتر السياسي في واشنطن بسبب القرصنة الروسية للوكالات الفيدرالية والتدخل في السياسة الأميركية، على آفة رقمية متفاقمة مع أزمة أوسع نطاقا، وهي هجمات الفدية التي تشنّها مافيا الإجرام الإلكتروني، التي تنشط في الغالب في أماكن آمنة أجنبية وملاذات بعيدة عن أجهزة إنفاذ القانون الغربية.**

في الولايات المتحدة وحدها، سُجّل خلال العام الماضي ضرب أكثر من 100 وكالة فيدرالية وحكومية وبلدية، وما يزيد عن 500 مركز رعاية صحية، و1680 مؤسسة تعليمية، وأعداد لا حصر لها من الشركات، وفقا لشركة الأمن السيبراني إمسيسوفت. وتصل الخسائر بالدولار إلى العشرات من المليارات. لكن الأرقام الدقيقة غير محددة. حيث يتجنب العديد من الضحايا الإبلاغ حفاظا على السمعة.

طوال الوقت، أصبح أفراد عصابات برامج الفدية أكثر جرأة وغرورا حيث يعرضون المزيد من الأرواح وسبل العيش للخطر. وهذا الأسبوع، هددت إحدى النقابات بإتاحة بيانات للعصابات الإجرامية المحلية. وعرضت أخرى مشاركة البيانات التي جمعت من ضحايا الشركات مع المتداولين داخل وول ستريت. وقد تواصل مجرمو الإنترنت بشكل مباشر مع الأشخاص الذين جمعت معلوماتهم الشخصية من أطراف ثالثة للضغط على الضحايا للدفع.

قال آلان ليسكا المحلل في شركة الأمن السيبراني ريكوردد فيوتشر "بشكل عام، أصبح ممثلو برامج الفدية أكثر جرأة وأكثر قسوة".

من أين أتت برامج الفدية؟

تعتبر الحكومة الأميركية الآن برامج الفدية تهديدا للأمن القومي. وقد أنشأ مكتب التحقيقات الفيدرالي فريق عمل للتعامل مع الأمر.

ألان ليسكا:
بشكل عام، أصبح ممثلو برامج الفدية من القراصنة أكثر جرأة وأكثر قسوة

الخميس، سلّمت فرقة عمل عامة وخاصة تضم مايكروسوفت، وأمازون، ورابطة الحكام الوطنية، ومكتب التحقيقات الفيدرالي، والخدمة السرية، ووكالات مكافحة الجريمة في بريطانيا وكندا خطة عمل عاجلة من 81 صفحة إلى البيت الأبيض لتحقيق شامل على برامج الفدية، مع تعيين وزير الأمن الداخلي أليخاندرو مايوركاس لمرافقتهم في إطلاق رسمي عبر الإنترنت في الساعة الواحدة مساء بتوقيت شرق الولايات المتحدة.

تتحدث العصابات الإجرامية التي تهيمن على أعمال برامج الفدية في الغالب باللغة الروسية، وتعمل في ظل إفلات شبه كامل من العقاب خارج روسيا والدول الحليفة. إنها استمرار وتطوّر لأكثر من عقدين من السرقة الإلكترونية التي استهدفت بطاقات الائتمان والهويات ونجحت في إفراغ حسابات مصرفية.

ونمت النقابات من حيث التطور والمهارة، حيث استفادت من منتديات الويب المظلم للتنظيم والتجنيد مع إخفاء هويات الأفراد وحركاتهم باستخدام أدوات مثل متصفح تور والعملات المشفرة التي تجعل من الصعب تتبع المدفوعات (وغسلها).

وتعمل برامج الفدية على تشويش بيانات المؤسسة الضحية بالتشفير. ويُترك المجرمون تعليمات على أجهزة الكمبيوتر المصابة حول كيفية التفاوض على مدفوعات الفدية، وبمجرد دفعها، يوفرون مفاتيح فك تشفير البرامج.

في العام الماضي، توسع محتالو برامج الفدية إلى الابتزاز بسرقة البيانات. قبل تشغيل التشفير، يسحبون الملفات الحساسة بهدوء ويهددون بفضحها علنا ما لم تُدفع لهم الفدية. وأصبح على الضحايا الذين دعموا شبكاتهم بجدية كوسيلة للتحوط ضد برامج الفدية الآن أن يفكروا ماليا في الدفع. في نهاية سنة 2019، كان لدى مجموعة واحدة فقط من برامج الفدية موقع ابتزاز عبر الإنترنت ينشر مثل هذه الملفات. وأصبح العدد الآن أكثر من عشرين.

يمكن أن يتحمل الضحايا الذين يرفضون الدفع تكاليف تتجاوز بكثير الفدية التي ربما تفاوضوا عليها. حدث ذلك مؤخرا لشبكة الصحة بجامعة فيرمونت. وتكبدت خسائر تقدر بنحو 1.5 مليون دولار يوميا في الشهرين اللذين استغرقهما التعافي. وكان لا بد من مسح أكثر من 5 آلاف جهاز كمبيوتر بالمستشفى وإعادة جمعها من البيانات الاحتياطية.

لم تتردد جامعة كاليفورنيا سان فرانسيسكو، التي شاركت بشكل كبير في أبحاث كوفيد – 19، في الدفع. ومنحت المجرمين 1.1 مليون دولار في يونيو الماضي. وتضررت الشركات المصنعة بشكل خاص هذا العام، حيث طُلبت فدية قدرها 50 مليون دولار من صانعي الكمبيوتر آيسر وكوانتا، وهي مزود رئيسي لأجهزة كمبيوتر أبل المحمولة.

يعتبر بعض كبار مجرمي برامج الفدية أنفسهم متخصصين في خدمات البرمجيات. إنهم يفخرون بـ"خدمة الزبائن"، حيث يوفرون "مكاتب المساعدة" التي تساعد في دفع الضحايا في فك تشفير الملفات. وهم يميلون إلى الوفاء بوعدهم. فلديهم علامات تجارية تجب حمايتها.

كيف يُنظّم المجرمون صفوفهم؟

قال موريتس لوكاس مدير الحلول الاستخباراتية في شركة الأمن السيبراني إنتل 471، في ندوة عبر الإنترنت في وقت سابق من هذا العام "إذا التزموا بوعودهم، فسيتم تشجيع الضحايا في المستقبل على الدفع. أنت تعرف بصفتك ضحية سمعتها بالفعل".

تحدد الشركة التابعة الأهداف وتخطط لها وتصيبها، وتختار الضحايا وتنشر برامج الفدية "المستأجرة" عادة من موفر برامج الفدية كخدمة. ويحصل المزود على جزء من المدفوعات، وعادة ما تأخذ الشركة التابعة أكثر من ثلاثة أرباع. وقد يحصل المقاولون الآخرون أيضا على قسط. يمكن أن يشمل ذلك مصممي البرامج الضارة المستخدمة لاقتحام شبكات الضحايا والأشخاص الذين يديرون ما يسمى بـ"المجالات المضادة للرصاص"، والتي تخفي وراءها عصابات برامج الفدية خوادم "القيادة والتحكم" الخاصة بهم. وتدير هذه الخوادم البرامج الضارة واستخراج البيانات قبل التنشيط عن بُعد، وهي عملية خفية قد تستغرق أسابيع.

في تقرير الخميس، قالت فرقة العمل إنه سيكون من الخطإ محاولة حظر مدفوعات الفدية، ويرجع ذلك إلى حد كبير إلى أن "مهاجمي برامج الفدية يواصلون العثور على قطاعات وعناصر من المجتمع غير مهيأة بشكل يرثى له لهذا النمط من الهجوم".

تدرك فرقة العمل أن السداد يمكن أن يكون السبيل الوحيد للأعمال المنكوبة لتجنب الإفلاس. والأسوأ من ذلك، غالبا ما أجرى مجرمو الإنترنت المتطورون أبحاثهم ويعرفون حد تغطية تأمين الأمن السيبراني للضحية. ومن المعروف أنهم ذكروا ذلك في المفاوضات.

ساعدت هذه الدرجة من الذكاء الجنائي في دفع متوسط مدفوعات الفدية إلى أكثر من 310 آلاف دولار العام الماضي، أي بزيادة 171 في المئة عن 2019، وفقا لما ذكرته بالو ألتو نتوركس، وهي مؤسسة من فريق العمل.

ليس من المستغرب أن نرى صناعة التأمين الإلكتروني التي ما زالت حديثة العهد تتأرجح. قال مايكل فيليبس، كبير مسؤولي المطالبات في شركة ريزيليونس إنشورنس والرئيس المشارك لفريق العمل، إن أقساط التأمين ارتفعت بنسبة 50 إلى 100 في المئة خلال العام الماضي. ففي المتوسط، يمكن أن تتجاوز مدفوعات مطالبات التأمين الإلكتروني الآن 70 في المئة مما دُفع في أقساط التأمين، مما دفع بعض شركات التأمين إلى التخلي عن هذا النوع من التأمين تماما، كما تظهر تقارير الصناعة.

ستتطلب الاستجابة متعددة الجوانب لبرامج الفدية التي اقترحتها فرقة العمل نوعا من التعاون الدبلوماسي والقانوني وإنفاذ القانون المتضافر مع الحلفاء الرئيسيين الذين تجنبتهم إدارة ترامب، مما يعوّض ما يسميه المؤلفون الاستجابة الحالية "غير المنسقة والمفككة".

الوقوف في وجه العملية

قال فيليب راينر الرئيس المشارك لفريق العمل، والمدير التنفيذي للمنظمة غير الربحية للأمن والتكنولوجيا "لا يوجد حل سحري، ولكن إذا أردنا تغيير مسار هذا النوع من الهجوم فيجب على حكومة الولايات المتحدة أن تتعامل معه بسرعة".

يحث التقرير على ضرورة تسمية مطوري برامج الفدية والشركات التابعة لهم والأنظمة التي تمكّنهم وفضحهم (ليس التعرف عليهم سهلا دائما) ومعاقبتهم.

كما يدعو إلى الكشف الإلزامي عن مدفوعات الفدية و"صندوق استجابة" فيدرالي لتقديم المساعدة المالية للضحايا على أمل أن يمنعهم، في الكثير من الحالات، من دفع الفدية، مع تنظيم أكثر صرامة لأسواق العملات المشفرة لتصعيب غسل عائدات برامج الفدية على المجرمين.

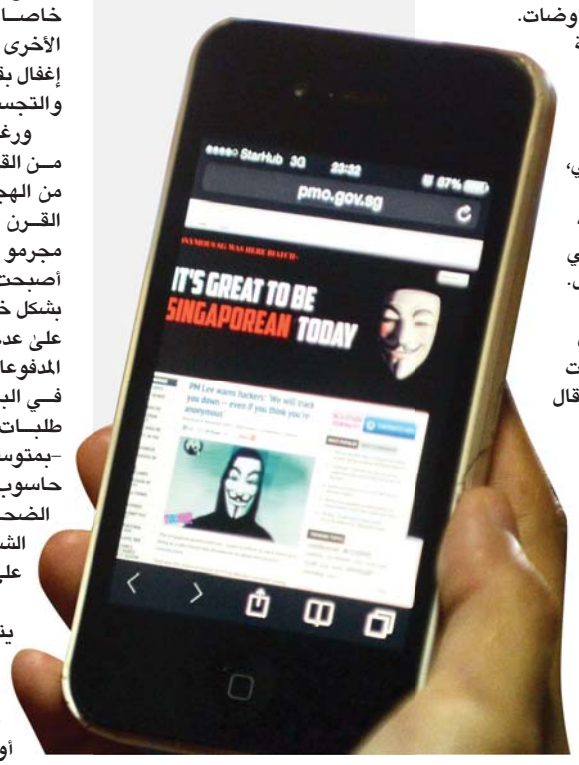
كما تدعو فرقة العمل إلى شيء قد يكون مثيرا للجدل: تعديل قانون الاحتيال وإساءة استخدام الكمبيوتر في الولايات المتحدة للسماح للقطاع الخاص بحظر النشاط الإجرامي عبر الإنترنت أو تقييده، بما في ذلك شبكات الروبوتات، وشبكات أجهزة الكمبيوتر الزومبي التي جرى الاستيلاء عليها والتي يستخدمها مجرمو برامج الفدية لزرع العدوى.

ومن بين كل تهديدات الأمن السيبراني التي تؤثر في الشركات، كانت برامج الفدية التهديد الأكثر شيوعا بداية من العام 2020، كما كان لها أكبر تأثير في زيادة عدد الضحايا وبخاصة على سمعتهم التجارية وأنظمتهم المالية. وهكذا، فإن هجمات انتزاع الفدية أصبحت تستحق اهتماما خاصا اليوم، وربما أكثر من الأنواع الأخرى من الهجمات؛ رغم أنه لا ينبغي إغفال بقية التشكيلات الهجومية الرقمية والتجسس الإلكتروني.

ورغم ظهورها في أواخر الثمانينات من القرن الماضي، إلا أن الموجات الأولى من الهجمات الضخمة تعود إلى أوائل القرن الحادي والعشرين. استفاد مجرمو الإنترنت من أن العملات المشفرة أصبحت أكثر انتشارا، وهو أمر مفيد بشكل خاص عندما يتعلق الأمر بالحفاظ على عدم الكشف عن هويتهم عند تلقي المدفوعات. وكانت هذه الهجمات موجهة في البداية إلى عامة الناس، إذ كانت طلبات الحصول على مبالغ صغيرة –بمتوسط بضع مئات من الدولارات لكل حاسوب محظور– ولم تتطلب التفاعل مع الضحايا. وتطورت بعد ذلك لاستهداف الشركات وزادت من مقدار كل طلب على الفدية.

ومن أجل تنفيذ هجماتهم، يتبع مجرمو الإنترنت عموما الخطوات نفسها: أولا، اقتحام نظام معلومات الضحية من طريق ثغرات البريد الإلكتروني، أو العيوب في المواقع الإلكترونية أو نظم الوصول من بعد؛ ثانيا، اقتحام نظام معلومات الضحية من طريق البريد الإلكتروني. ثم، الاندساس مرة واحدة في شبكة الهدف، وانتشار وتركيب بهدف السيطرة على نظام المعلومات.

أفراد عصابات برامج الفدية أكثر جرأة وغرورا حيث يعرضون المزيد من الأرواح وسبل العيش للخطر



الحكومة الأميركية الآن تعتبر برامج الفدية تهديدا للأمن القومي، وقد أنشأ مكتب التحقيقات الفيدرالي فريقا للتعامل مع الأمر

منذ نهاية عام 2019 وظهور مجموعة "ماز"، وهي تشكيل عصابي إلكتروني دولي، أصبحت هجمات برامج الفدية إلى جانب سرقة البيانات والابتزاز لضمان عدم الكشف أمرا شائعا وأدت إلى مفاوضات مباشرة بين المهاجم والضحية. هذا النوع من الهجمات منتشر الآن. ففي تقريرها عن التهديد الذي تشكله برامج الفدية في فرنسا في عام 2020، سجلت الوكالة الوطنية الفرنسية لأمن أنظمة المعلومات (أنسي) زيادة بنسبة 255 في المئة في الهجمات المبلغ عنها مقارنة بعام 2019.

وكانت لهذه الهجمات أهداف كثيرة. وقد استهدفت هذه الهياكل مجموعات كبيرة على وجه الخصوص، ولكن الهياكل الأصغر حجما استُهدفت أيضا. وفي حين لم تحظَ سوى الاعتداءات على السلطات المحلية أو المستشفيات بتغطية إعلامية واسعة، فإن العديد من الهجمات الأخرى استهدفت كل القطاعات من دون أن تلفت النظر. وكانت هذه الهجمات ذات طابع انتهازي في الغالب، ومع ذلك كان من المقرر أن يكون بعضها على وجه التحديد لضمان دفع فدية. يختار مجرمو الإنترنت أهدافهم استنادا إلى ملاءة الشركة المستهدفة أو حالتها التشغيلية أو هشاشة نظم معلوماتها. وعلى نحو متزايد، أدت الأرباح الناتجة من هذه الهجمات والشعور بالإفلات من العقاب –بسبب قدرة السلطات المحدودة على معاقبة مجرمي الإنترنت– إلى ظهور نظام عمل منظم داخل الجريمة السيبرانية.

وردا على العدد المتزايد من الهجمات، اتخذت الشركات تدابير وقائية تزيد من صعوبة القيام بأعمال تجارية لمجرمي الإنترنت ما جعل أنظمة الحجب أقل عرضة لانتزاع الفدية. وهذا هو الحال بصفة خاصة بالنسبة إلى الشركات الكبيرة، رغم أن الشركات الأصغر حجما تظل في الكثير من الأحيان ضعيفة للغاية.