إيفا فولفأنغل

نقرة خاطئة

ملاحقة المتسللين الإلكترونيين:
لماذا الحرب السيبرانية
تخصنا جميعا

ترجم هذا المقتطف من الكتاب: د. ضياء الدين النجار

مقدمة

أمر سهل للغاية

في خريف عام 2019 قمت باختراق مستشار أمن تكنولوجيا المعلومات للرئيس الأمريكي الأسبق باراك أوباما. عندها أتضح لي أن العالم بحاجة إلى هذا الكتاب. لأنه كان أمرا سهلا للغاية.

لقد كان اختراق بتكليف - وجاء التكليف من الضحية نفسها: إيريك روزنباخ المسمى بقيصر السيبرانية حيث كان بمسماه الوظيفي الرسمي "نائب مساعد وكيل وزارة الدفاع لشؤون الفضاء السيبراني" مسؤولاً في الفترة من عام 2011 إلى عام 2014 عن الاستراتيجية السيبرانية لوزارة الدفاع الأمريكية، ومن 2014 إلى 2017 كان رئيس أركان البنتاغون. خلال هذا الوقت واكب روزنباخ جميع التطورات الجوهرية المتعلقة بالفضاء السيبراني حيث تمكن مع فريقه من صد جميع أنواع الهجمات جزئيًا أو كليًا أو على الأقل من تحليلها بعد ذلك. في تلك السنوات كانت هناك طائفة كاملة من الأحداث: من سرقة الصين للملكية الفكرية من الشركات الأمريكية الكبيرة من خلال هجمات التلصص مرورا بالهجمات الإلكترونية الإيرانية والكورية الشمالية على البنى التحتية الحيوية وصولا إلى محاولات المخابرات الروسية التي كانت تزداد ضراوة يوما بعد يوم بمساعدة هجمات القرصنة ونشر الأخبار الكاذبة للتدخل في السياسة الأمريكية.

ومن ثم أتلقى في عام 2019 تكليفا من روزنباخ أن أكتب له بريدًا إلكترونيًا مستخدما التقنية المعروفة باسم التصيد الاحتيالي بالرمح، وهي عبارة عن رسائل بريد إلكتروني شديدة الاستهداف مفصلة تفصيلا على شخص بعينه بهدف دفع المرسل إليهم إلى الضغط على مرفق ضار. فإذا فعلوا ذلك ينتشر فيروس على حاسوبهم – والذي بحسب ما يقع عليه اختيار المخترق – يتجسس عليهم ويستولى على البيانات أو يقوم بتشفير كل شيء – أو يفعل كلا الأمرين معا.

يقوم إيريك روزنباخ الآن بتدريس الأمن السيبراني بوصفه مدير مركز بيلفر في كلية هارفارد كينيدي. الرسالة الإلكترونية المتصيدة هو واجب منزلي في إطار حلقة دراسية مكثفة في هارفارد أحضرها مرتين في الأسبوع. اسم الحلقة الدراسية "الفضاء السيبراني والعمليات المعلوماتية: الحرب، السلام والمسافة الفاصلة بينهما"، وهو اسم يخاطبني على نحو خاص لأن هذا هو بالضبط موضع اهتمامي: الحرب، السلام – وكل شيء يوجد ما بينهما في الفضاء السيبراني. لست طالبًا منتظمًا، لكن لديّ زمالة في الصحافة العلمية في معهد ماساتشوستس للتكنولوجيا. لهذا السبب يجب أن أقنع روزنباخ أولاً أنه يمكنني المشاركة في حلقته الدراسية بصفتي حائزًة على منحة دراسية. "لكن عليك القيام بكامل العمل"، هكذا كتب لي مهددًا. العمل -هذا كل ما يتوقعه من الحائزين الطموحين على زمالة وهم في منتصف حياتهم المهنية الذين حضروا الحلقة الدراسية في هارفارد معي. يبدو الأمر مشوقا بالنسبة لي، ولذا أعطي موافقتي – وهو أمر سيجر علي فعليا قدرًا هائلاً من العمل: منها مثلا قوائم قراءة طويلة إلى ما لا نهاية للتحضير لكل موعد يطلب معرفة محتوياتها من الفصل بأكمله دون سابق إنذار. معسكر تدريبي لعدة أيام ذي مضامين تقنية. طائفة من الاختبارات القصيرة وأوراق سياسية استراتيجية يتعين كتابتها. أضف إلى ذلك كتابة "إحاطات فورية" تلقائية يتعين علينا فيها أن نتولى لعب دور الضالعين في حادث سيبراني وأن ندلي ببيان، وقبل كل شيء تنفيذ عمليات محاكاة: أدوار تحاكي واقع وزارة الدفاع والتي عادة ما يلعب فيها روزنباخ دور رئيس الولايات المتحدة الأمريكية الذي يجب أن نقدم له النصح.

لا تكاد توجد – إلا هنا – فرصة للتعامل في الحياة بشكل مكثف ووثيق وشامل مع ما يحدث في الفضاء الرقمي وماهية الضرر الهائل الذي ينشأ من الهجمات السيبرانية ومدى خطورة عصر الحروب السيبرانية - وقبل كل شيء: إلى أي مدى نحن عرضة للهجوم . كلنا. ليس الولايات المتحدة ، بل المجتمع ، العالم.

منذ ذلك الحين لم أتوقف عن البحث في هذا المجال النوعي والصورة تزداد شمولا يوما بعد يوم.

أضف إلى هذا منظورات جديدة، كما أن هناك فيما يتعلق ببعض الموضوعات تقييمات مختلفة، ولكن يظل برغم كل شيء أمر واحد: إنه يقيني المتمثل في الآتي: من ينظر إلى الهجمات السيبرانية الكبرى في السنوات الأخيرة والتطورات الراهنة سيرى أنه يجب علينا التحرك. وأنا لا أقصد بهذا رؤساء الحكومات والمستشارين الأمنيين فحسب.

يتضح لي مدى التأثير الهائل لهذا على كل واحد منا عندما أقوم بمهمة كتابة رسالة التصيد الإلكتروني بالحربة إلى روزنباخ. أقضي ليلة في البحث عن معلومات تخص روزنباخ وأندهش من كم المعلومات التي أعرفها بعد كل هذا الوقت عن خصوصياته وكم عدد الفرص المحتملة للهجوم عليه التي تنفتح أمامي.

بالنسبة لرسالة البريد الإلكترونية أحصل على تقدير A، وهو أعلى تقدير وفقًا لنظام الدرجات في الولايات المتحدة الأمريكية. هذا يعني، كما أوضح لي روزنباخ، أنه اعتبر رسالتي الإلكترونية جديرة بالثقة. ولو كان رسالة بريدية للتصيد حقا لكان قد ألتقط معها أيضا أحد الفيروسات.

فإذا كان من السهولة بمكان تمرير رسالة بريد إلكترونية ضارة على شخص واعٍ بالمشكلات مثل روزنباخ، فكيف يمكننا حماية أنفسنا بالأساس؟ خلال الحلقة الدراسية أصبحت فجأة واعية بعدد المرفقات التي كُنت قد فتحتها لأن الرسالة الإلكترونية الخاصة بها كان وقعها علينا يوحي بالثقة المطلقة. لا يمكن التحقق إذا ما كانت رسالة إلكترونية ما حقيقية إلا بصعوبة بالغة. فلا يتطلب الأمر إلا وجود شخص مثلي يأخذ من وقته يوما كاملا ويقوم ببعض البحث في الإنترنت – تمامًا كما فعلت مع روزنباخ. وعندها يمكنك كتابة رسالة إلكترونية شخصية ومحل ثقة سيفتحها أغلبية الناس من دون أن يحركوا ساكنا. وتزوير عنوان المرسل تمرين سهل. وشراء ما يلزم من برمجيات ضارة على الإنترنت لا يتطلب أيضًا سوى قليل من الجهد البحثي. وبهذا يكون الهجوم جاهزا.

يتم تنفيذ معظم هجمات التصيد الاحتيالي بجهد أقل كثيرا. معظمها ليست شخصية، فغالبًا ما يكفي وجود مكونات نصية متكررة الاستخدام – إلا أنها مع ذلك مشهود لها بالنجاح. الجمهور يفعل ذلك. فأي شخص يرسل ما يكفي من مثل تلك رسائل البريد الإلكترونية إلى العالم سيصطاد في وقت ما شخصًا ساذجًا. وما أن تعلق الأمر بمبالغ مالية أكبر فإن استثمار بعض الجهد وتفصيل الهجمة على المقاس المطلوب أمر يستحق الجهد. يعد هذا الأمر استثمارًا مربحًا للغاية إذا ما وضعت في اعتبارك ما تدفعه الشركات لاستعادة بياناتها المشفرة. لا يوجد في الواقع إلا أوجه محدودة من أوجه الاستثمار المتسمة بفاعلية أكبر من الاستثمار في البرمجيات الضارة. والضرر الذي يلحق بنا جميعًا هائل.

فلا يتطلب الأمر سوى نقرة واحدة خاطئة.

ما هو حال الموظف الذي يسمح للمجرمين بالدخول إلى شبكة الشركة بنقرة طائشة متسببا بالتالي في أضرار بملايين اليوروهات؟ هذا ما أطرحه على نفسي بشكل محدد في فبراير/ شباط 2022 وأنا أقف في طابق الإدارة لشركة هيلمان للتوزيع الواقعة بمدينة أوسنابروك عبر ثلاثة طوابق ممتدة ناظرا إلى أسفل ناحية الفناء الأمامي الكبير الذي يعج بالحركة كما لو كنا في أحد أعشاش النمل؛ فهناك تقف شاحنات الشركة الضخمة التي تنقل كل يوم عددًا لا يحصى من البضائع عبر جمهورية ألمانيا الاتحادية ينتظر وصولها في عناوين مختلفة تمامًا هذا الشخص أو ذاك. قبل أسابيع قليلة فقط بدا كل شيء فعلا مختلفًا تماما هنا. توقفت حركة العمل الدائبة على غير انتظار عندما وقعت هيلمان ضحية لهجوم إلكتروني قبيل أعياد ميلاد عام 2021. فالشركة التي توظف ما يقرب من 11000 شخص في جميع أنحاء العالم ويبلغ رقم مبيعاتها السنوي 2.5 مليار يورو أخذت تفقد من ثانية لأخرى وبلا أدنى سابق إنذار اتصالها بشبكة الإنترنت.

في هذه الحالة لم تتدفق أي فدية لأن الشركة انتبهت إلى الهجوم مبكرًا – أي أنه تم اكتشافه قبل أن يتمكن المجرمون من تشفير البيانات. ومع ذلك كان الضرر هائلاً فلا ننسى أن الشركة لم تعد لبضعة أيام بالكاد قادرة على التصرف – وذلك في فترة مبيعات أعياد الميلاد. بالإضافة إلى ذلك وضعت ببضعة أسابيع بعدها عديد من الغيغابايتات من البيانات الداخلية على شبكة الإنترنت الخفية، وهو أمر مثير لاهتمام المجرمين أو المنافسين الدوليين على حد سواء.

لفت نشر البيانات أنظاري نحو الاختراق وتمكنت أخيرًا من إقناع هيلمان باستقبالي من أجل إعداد تقرير لصحيفة "دي تسايت" الأسبوعية. لم يكن الأمر سهلاً ، فمعظم الشركات تخاف خوفا عظيما من التحدث عن الهجمات. والعار العلني وبالأولى كذلك القلق من استفزاز المجرمين يجعلهم يتورعون عن قطع تلك الخطوة نحو العلن.

ولكن إذا كانت الهجمات الإلكترونية من المحرمات فسنظل دوما عرضة للهجوم. فحتى في محيطي الصغير غالبا ما أواجه هذا الموقف:

"أفضل عدم معرفة ذلك على وجه الدقة، فلن أفهم هذا الأمر على أية حال - ولن يصيبني قطعا مثل هذا الأمر." لسوء الحظ تأتيك المصيبة على حين غرة إذا لم تكن مستعدا لها. وهؤلاء بالذات هم من يتصلون بي حينئذ: »إيفا ، لقد قمت بالنقر على رسالة بريد إلكتروني بدت غريبًة بعض الشيء. فماذا عليّ يا ترى أن أفعل الآن؟"

في محيطي الشخصي وحده أصيب في غضون عام عديد من الأفراد الطبيعيين الذين التقطوا فيروسات ضارة عبر رسائل البريد الإلكتروني أو وقعوا ضحية لرسائل وهمية ، بالإضافة إلى شركتين متوسطتين خسرتا مبالغ مالية ذات خمسة إلى ستة أرقام.

أما في هيلمان للخدمات اللوجستية فمن المرجح أن تكون التكاليف أعلى بكثير. ومع هذا فإن هذه الضحية لهجوم القراصنة هي مجرد واحدة من كثيرين: فوفقًا لدراسة أجرتها رابطة "بيتكوم" الرقمية تسبب الهجمات السيبرانية أضرارا للاقتصاد الألماني تبلغ سنويا نحو 203 مليار يورو، إذ تضرب تلك الهجمات غالبية الشركات، حيث أبلغ نحو 84 بالمائة منها عن وقوع مثل تلك الهجمات.

قمت بعديد من الرحلات البحثية من أجل هذا الكتاب - رحلات حقيقية إلى روسيا وأوكرانيا وبريطانيا العظمى وهولندا والولايات المتحدة الأمريكية، بالإضافة إلى القيام برحلات افتراضية عبر الزمن: لقد غصت في أعماق تاريخ الحروب السيبرانية والجريمة الإلكترونية مع الباحثين الأمنيين وأعدت عبر نقاشات امتدت لأيام طوال صياغة أحداثها بأدق تفاصيلها. إنه تاريخ لا يزال شابا لكنه لا يقل إثارة في أحداثه. لقد اخترت لهذا الكتاب بعضًا من أكبر الأحداث السيبرانية وأكثرها إثارة للاهتمام في السنوات الأخيرة وتتبعت آثارها حتى يومنا هذا على نحو مكثف. لقد قابلت متسللين من جميع المشارب، وزرت ضحايا، ورافقت الباحثين الأمنيين في عملهم الدؤوب كمخبرين.

والنتيجة المتوصل إليها مقسمة إلى أربعة أجزاء: في الجزء الأول أرافق المجرمين السيبرانيين، وفي الجزء الثاني أتعامل مع القرصنة الحكومية وبداية الحرب السيبرانية، وفي الجزء الثالث أبيّن كيف خرجت الحرب السيبرانية عن السيطرة بعواقب قد تصل جزئيا إلى درجة تهديد حياة مَن لا ناقة لهم في الأمر ولا جمل، وفي الجزء الرابع أبحث القضايا المتعلقة بالسبب في كوننا عرضة للهجوم على هذا النحو ومَن يمكنه أن يقدم لنا يد العون.

سيتثبت لديك مثلي بمزيج من الدهشة والإحباط أن التمييز بين الهجمات الإجرامية وهجمات الدولة ليس قاطعا دائمًا وأن هناك أشكالًا مختلطة لأن إحداهما يستفيد من الآخر والعكس بالعكس. وهو ما يجعل الأمر أكثر خطورة بمكان لأن هناك حقيقة تمتد عبر كل مراحل تاريخ أمن تكنولوجيا المعلومات متمثلة في التالي: حتى الاختراق الحكومي المفترض فيه أن "خيّر" في الحرب على المجرمين يُضعف في المحصلة النهائية أمن الجميع.

ولكن ماذا يمكننا أن نفعل؟ نحن بحاجة إلى سد الثغرات الأمنية – سواء في الشركات الكبيرة أو على مكتبنا في المنزل – ومن أجل هذا علينا التعامل مع الثغرات في أنظمتنا التي تفتح الطريق أمام المهاجمين ومع الكيفية التي يتم بها هذا الأمر. وهذا ما سنفعله في هذا الكتاب. وسنكشف عن "الثغرات" التنظيمية، بل أيضا النفسية منها. كشف "الثغرات" لأن هذا هو أحد التوجهات: الاتجاهات: المجرمين والقراصنة الحكوميين يستغلون ثقتنا. وستندهش مما يمكن لمَن يطلق عليه خبيرة الهندسة الاجتماعية – وهي بالتأكيد متخصصة في المكر والإيقاع بالآخرين – أن تحققه إذا جاز التعبير – دون عنف، وبدون فيروسات تماما.

في غمار انهماكي بالتحرير الختامي لهذا الكتاب ينفجر صوت أحد المتصلين بخبر مروّع مفاده الآتي: إنه يتصل من عند اليوروبول وإن مكتب التحقيقات الفيدرالي كما يقول الرجل على هاتفي المحمول يشارك في الاستماع لأنني مطلوبة بوصفي جزءًا من عصابة دولية عتيدة الإجرام. ليضيف أنه سيقوم الآن بحظر حسابي المصرفي وإن بطاقة هويتي هي الأخرى لم تعد منذ تلك اللحظة سارية المفعول. من المحتمل أن يكون قد وقع حادث عنف في سيارة استأجرتها حيث وجدت مهشمة بالكامل ومغطاة بالدماء عند حافة أحد ضواحي برلين مضيفا أنه عبر حساباتي يجري غسيل للأموال. لحسن الحظ يبدو أنه يعتقد أنه ليس لدي أي علاقة بأي من هذا ولكن على ما يبدو أن شخصًا ما سطا على بياناتي – إلا أنه مَن يكون هذا الشخص؟ يقول إنه يريد مساعدتي، غير أنه يتعين عليّ أولا وقبل كل شيء أن أثبت للسلطات أن ما لديّ من مال ذو أصل قانوني. فيقول لي: "افتح الكمبيوتر المحمول وابحث عن برنامج تيم فيوار Team Viewer الذي يتحكم بجهاز الكمبيوتر عن بعد ".

لقد خمنت الآن المسار الذي يتجه إليه الحديث: كان المتصل مجرما سيبرانيا. حاول أن يدلس عليّ محاولا إقناعي بأن أدعوه إلى الدخول إلى جهاز الكمبيوتر الخاص بي باستخدام أحد البرامج حتى يتمكن من إفراغ حسابي بحجة مساعدتي.

بالطبع لم أفعل لأنني لم أكن غير مستعد للأمر، وبدلاً من ذلك تحججت بكثير من الأعذار التقنية لتفحص حال المتصل ومعرفة ما في جعبته.

يجب أن أعترف: لقد كنت في نهاية الأمر مبهورا إلى حد ما لأنه كان يتمتع بطاقة إقناع هائلة وكان لديه عن كل شيء إجابة. لقد تم توصيلي عدة مرات إلى "موظفين" ذي رتب وظيفية أخرى قدموا أنفسهم دائمًا بأسمائهم الكاملة وأرقام عملهم ولعبوا وصولا إلى مستوى الكمال لعبة "الشرطي الجيد والشرطي السيئ".

لم أعد بالطبع بعد ما أجريته من بحث من أجل هذا الكتاب ضحية مناسبة للعصابة. ومع ذلك اتضح لي أنهم قد استثمروا كثيرا وأن هذا ربما سيؤتي ثماره. وأنا أعلم على نحو مباشر من إحدى الضحايا كيف ستستمر القصة إذا لم تكن مستعدًا: في غمار بحثي قابلت امرأة شابة خسرت مبلغًا من خمسة أرقام لصالح بعض المجرمين.

إذا كنت تتساءل الآن كيف يمكن أن يحدث ذلك، فيرجى أن تقرأ الفصل الخاص بالهندسة الاجتماعية: إنه أمر حيوي تمامًا مثل المكالمة الهاتفية في غمار مرحلتي الأخيرة من الكتابة. لذلك هناك في جميع مجالات هذا الكتاب إشارات إلى التطورات الراهنة: في غمار الحرب الروسية العدوانية على أوكرانيا عادت مجموعة قرصنة تابعة لجهاز المخابرات الروسية، كانت قد ظلت لفترة طويلة بعيدة عن الأنظار أو عملت في الخفاء وهي المسؤولة عن بعض أخطر الهجمات السيبرانية في التاريخ، إلى نشاطها من جديد وأظهرت من خلال هجوم على مفاعل كهرباء – لحسن الحظ أنه كان فاشلا – أنها لا تزال تمثل خطرًا كبيرًا، وبالذات بالنسبة للبنى التحتية الغربية. تتسارع الأحداث أيضًا في مجال تطوير برامج التجسس الحكومية وإمكانية إساءة استخدامها: فمن بين أمور أخرى تظهر عمليات البحث الحالية المتعلقة ببرنامج التجسس بيغاسوس Pegasus كيف يتم في الديكتاتوريات وضع المنظمات غير الحكومية والصحفيين وشخصيات المعارضة في بؤرة قمع الدولة. تساعد الأسلحة السيبرانية التي منبعها أوروبا الأنظمة القمعية في قهر الأصوات الناقدة – وفي عام 2021 كانت ألمانيا بطل العالم في تصدير برمجيات التجسس حيث ذهبت هذه البرمجيات على نحو يكاد يكون حصريا لأنظمة غير ديمقراطية.

حتى المجرمين الذين رافقتهم في الجزء الأول يزدادون إبداعًا. يخسر عدد متزايد من الناس أموالهم لأن المجرمين يتفننون بطرق مختلفة في الوصول إلى حساباتهم المصرفية. تقرأ على نحو شبه يومي عن هجمات جديدة على الشركات بخسائر بالملايين بواسطة برمجيات انتزاع الفدية. وهنا تظل القاعدة على حالها: نقرة واحدة خاطئة تكفي.

عندما سألت على تويتر قبيل نشر هذا الكتاب عن الأشياء المهمة التي يجب أن تأتي في مقدمة الكتاب نصحوني – أيها القراء الأعزاء – بتحذيركم على طريقة "مدينة الكتب الحالمة" لصاحبها فالتر موريس الذي صدّر كتابه بأنه ليس قصة "لذوي البشرة الرقيقة والأعصاب المرهفة – والذين أود فورا أن أوصيهم بطرح الكتاب جانبا من جديد"[1]. في الحقيقة ربما أنت أيضًا قد ترتجف عند قراءة كتابي ، لكنني أود أن أحذرك من التالي: عدم قراءته قد يكون أمرا خطيرًا أيضًا. لأنك ستفقد علما قيما يحميك من الهجمات السيبرانية. وعلى النقيض من كتاب فالتر موريس فإن كل ما يدور حوله هذا الكتاب بلا استثناء وقائع حقيقية يا حبذا لو لم تغمض أمامها عينيك.