9

زعيم قراصنة الكومبيوتر

مارك مايفريت Marc Maiffret، بشعره الأرجواني الإبري المظهر المكسو بطبقة من الجل، لا يبدو عليه أنه جاسوس مأجور مكلف بسرقة ما يعتقد أحد السياح الكشميريين أنه أكثر برامج الكومبيوتر العسكرية الأميركية سرية. مايفريت، المولع بارتداء السراويل السوداء والقمصان ذات الياقة المزودة بأزرار، يحبذ «الاقتداء بزي «نيكولاس كيج» Nicolas Cage ولكن بقامته البالغة خمسة أقدام وستة إنشات، يبدو أشبه بنسخة قوطية جديدة عن «بارني رابل» Barney Rubble.

لم تكن مفاجأة بالنسبة إلى هاوي الأنترنت البالغ عشرين عاماً من العمر المعروف بلقب «تشاميليون» Chameleon أن الحياة هي لعبة أرقام. لأنه بقدر ما تسعفه الذاكرة، فإن هذا الدخيل الرقمي الذي تفوق على جهابذة أمن الأنترنت، يعيش في عالم سفلي قوامه الأرقام. الأصفار والآحاد التي كنت أحركها «والتي كانت تحركني»، مترابطين معاً في لغة من الشيفرات الثنائية، تشكل أساس الأوامر التي كان يستخدمها لتزوير الطلبات التي تشكل الأساس لأنظمة التشغيل التي تعمل بمثابة الأدمغة بالنسبة للشبكات التي يخترقها.

تشاميليون هذا، المتخصص في اختراق برامج مايكروسوفت للنفاذ

إلى ثغرات أمنية، يقول: «أنا لم أتخرج من معهد ماساشوستس للتكنولوجيا بدرجة شرف. عالمي كان يتمحور حول اختراق برامج الكومبيوتر وأنظمته، بينما يتمحور عالم أخصائيي أمن الشبكات حول تحصين أنظمتهم وحمايتها ضدي وضد هجماتي، هجمات لا يعرفون عنها شيئاً».

أمّا الآن، بصفته أحد مؤسسي شركة اي. آي eEye، إحدىٰ كبرىٰ شركات الاستشارات الأمنية لشبكة الأنترنت، فقد غدا واحداً من أخصائيي أمن الكومبيوتر هؤلاء الذين كان يفوقهم ذكاءً وحنكة. ولدى مايفريت بطاقات شخصية Business Cards ـ لكن ذلك لا يعني أنه قد انساق مع الاتجاهات السائدة. برغم كل شيء، فهم يقرأون، «زعيم قراصنة الكومبيوتر». وهو والرؤوس الكبيرة المعادون لتقاليد المجتمع من أمثال، «جيريكو» jerico، «ديلدوغ» Dildog، «بانكيس» punkis، و«تويتي فيش» Tweety Fish، يقدمون الصورة الواضحة لعدم تجهيز وتأهيل التجسس الاقتصادي حتىٰ الآن من أجل شبكة الأنترنت Cyberspace.

ولكن كم يجب أن تكون مغرية بالنسبة إلى عالم الشركات التجارية في أمريكا. لقد سبق لمعظم الشركات تخزين مقادير هائلة من البيانات والسجلات الشخصية للموظفين ووثائق المعاملات التجارية للزبائن ومعلومات مالية سرية ومشاريع سرية وخطط تسويقية وتقنيات في مرحلة البحث والتطوير ـ على شبكات أجهزتها. ومن أي مكان بعيد في العالم، كان باستطاعة دخيل رقمي بارع، التسلل إلى شبكة الكومبيوتر لإحدىٰ الشركات التجارية من طريق التحايل على برنامج الشبكة وحمله على تنفيذ أوامره وليس أوامر المشرف الإداري على النظام. وبمجرد دخوله إلى

الشبكة يغدو قادراً على القفز من جهاز إلى آخر، ناسخاً الوثائق ورسائل البريد الإلكتروني السرية. عالم من الرموز والأرقام، منذ بدء العمل على سرقة المعلومات وحتى انتهائه منها، فإن الشركة لن تعرف حتى بأنها قد سرقت ـ ما لم يبح المجرم بما قام به متباهياً بفعلته.

«أعتقد» ـ يقول ديل كودنغتون Dale Coddington، مهندس أمن أنظمة الشبكات في شركة أي. آي. ديجيتال سيكيوريتي eEye Digital Security ـ «أنه كلما اتجهت الشركات نحو تخزين مزيد من المعلومات على الشبكة، فإن منافسيها سيجدونها فرصة مغرية للتعاقد مع قراصنة كومبيوتر».

وأضاف: «بما أن سجلهم لدىٰ مكتب التحقيقات الفيدرالي دون الممتاز، فليس هنالك سوىٰ فرصة ضئيلة للإيقاع بأحد قراصنة الكومبيوتر، من المدربين جيداً. وبحكم مثل هذه المخاطر الضئيلة والعائد المرتفع، فلا مناص من أن تتعرض شركة ما لسرقة معلوماتها من علىٰ شبكة الكومبيوتر. ولكن يبقى السؤال: هل ستعلم مع ذلك بما حل بها؟ منذ الأيام الأولىٰ لعصر الإلكترون (فترة الستينيات) وقراصنة الكومبيوتر يصولون ويجولون عبر «الشبكات» ـ حتىٰ قبل صياغة هذا المصطلح سايبرسبيس Cyberspace من قبل كاتب الخيال العلمي «ويليام غبسون» William Gibson في روايته نيورومانسر Newromancer. كانت الأنترنت في البداية مقتصرة على نخبة مختارة من الجامعات ومعاهد الأبحاث. وكان مصطلح «هاكر» Hacker أو قرصان الكومبيوتر، يستخدم إمّا لوصف ضربة غولف غير موفقة أو متبجِّح اكتشف أعمق أسرار تشغيل أنظمة الكومبيوتر. في كلتا الحالتين، لم يكن «الهاكر» خارجاً على

القانون. كان «الهاكر» يحوز على مهاراته عادة من خلال آلاف الساعات التي كان يقضيها في سبر أغوار شبكات الكومبيوتر الكبيرة ودراسة كيفية تناظمها مع بعضها بعضاً. لقد أدىٰ اختراع شبكة الأنترنت العالمية سنة 1989 إلىٰ تغيير ذلك كله. في البداية، كان طريق المعلوماتية السريع والواسع عبارة عن درب ريفي ضيق وعر يعج بالحفر والمطبات. لم يكن معظم الامريكيين حتىٰ سنة 1996 قد سمعوا بعد بمصطلح «ويب» Web، ومصطلح «براوزر» Browser كان يستخدم لوصف شخصٍ يتسكع في أرجاء أحد المحال التجارية بلا هدف محدد، وعدد قليل من الشركات أقامت لها مواقع علىٰ شبكة الأنترنت.

مع إطلالة فترة التسعينيات، بدأت الشركات تقر بحتمية اللجوء إلى التجارة الإلكترونية التي تقدم خدماتها إلى الزبون مباشرة، وبحلول سنة 2000 أصبح هناك ملايين من مواقع الانترنت التي يعود معظمها لشركات ومؤسسات تجارية صغيرة، إضافة إلى الجامعات ومراكز الأبحاث والتكنولوجيا والمراكز العائلية الفرعية والمتعصبين دينياً وسياسياً ومقدمي المشاهد الجنسية ومحتالي الشبكات والجماعات المؤجحة للكراهية والصحف والمجلات ودور النشر وقراصنة الكومبيوتر وقراصنة الموسيقىٰ والبرمجيات إضافة إلى مواقع الاستفسارات العامة لزيد وعمرو من الناس.

لكن الأعداد المتزايدة لمواقع الأنترنت تعني عدداً أكبر من الهجمات على هذه المواقع. في سنة 1988، أول سنة تتوافر فيها الإحصاءات، تم الإبلاغ عن 6 حوادث انتهاك لمواقع الأنترنت، استناداً إلى تقرير مركز «سيرت» Cert الذي هو جزء من معهد جامعة «كارنيجي ميلون» Carnegie Mellon لهندسة البرمجيات. بعد أربع سنوات، ارتفع

عدد هذه الحوادث إلى 773. أمّا سنة 1995 فشهدت 2412 حادثة انتهاك لشبكات الكومبيوتر، هذا الرقم الذي تضاعف بدوره إلى 9859 حادثة سنة 1999. وظل الربع الأول من العام 2000 على هذا المنوال وبوتيرة ستؤدي إلى ارتفاع العدد إلى 10,000 حادثة في ذلك العام. وهذه هي فقط الحوادث التي يتم الإبلاغ عنها. فالبنتاغون وحده يتعرض أسبوعياً لمئات الهجمات على غرار العشرات من المواقع الحكومية والعسكرية الأخرىٰ. ومواقع «موتورولا» Motorola، «نيويورك تايمز» The New York Times و«ياهو» Yahoo! هي مجرد غيض من فيض تلك الشركات التي تعرضت مواقعها للاختراق من قبل مجرمي الديجيتال الأشاوس هؤلاء.

لا يشكل التواصل الأوسع نطاقاً بين شبكات الأنترنت العالمية جزءاً من التأملات اليومية لمدمني الانترنت فحسب، إنما بات هذا التواصل العالمي يمثل طريقاً للوصول إلى المصدر الرئيسي. أخصائي أفلام الرعب ويس كرايڤن Wes Craven مخرج فيلم سكريم إيتال Scream et al وكوابيس شارع إيلم Nightmares on Elm Street يقول: «أنظر إلى أجهزة الكومبيوتر وشبكاتها العالمية الآخذة بالاتساع، على أنها بداية لمسالك عصبية إلى الوعي العالمي. بدأ الأمر بالتلغراف المستند إلى مبدأ استخدام الأرقام لنقل المعلومات، وصولاً إلى أجهزة كومبيوتر هذه الأيام. إن الطريقة التي تتقارب بها شبكات الكومبيوتر من بعضها البعض من خلال اتصالها بشبكة الانترنت، تخلق ما يشبه نظاماً مركزياً رقمياً للأعصاب. هناك دماغ آخذ بالتشكل حول القشرة الخارجية للكوكب».

مسألة معقدة ربما، لكن هذا التواصل البشري الافتراضي له ثمنه: الأمن. إن السهولة التي تم من خلالها إطلاق الموجة الهائلة من الهجمات

ضد الإنجازات التي حققتها التجارة الإلكترونية e-commerce على شبكات الانترنت في شباط/ فبراير، سنة 2000 والتي أدت إلى ما يعرف بتعطل الخدمة Dos تؤكد أن كل شخص، وصولاً إلى أكبر الشركات، هو عرضة للهجوم على مواقعه على شبكة الانترنت. ياهو Yahoo! إي تْريد E Trade، أمازون Amazon، باي. كوم .Buy. com، والعشرات من المواقع الأخرى تعرضت لعاصفة من المجموعات الإلكترونية الدقيقة electronic pockets الحاوية على رسائل مضادة للشركات التجارية. تسارعت أنفاس منظمي ومسؤولي وحدات الخدمة في الشركات لهذا الهجوم المباغت، الذي أبطأ حركة العمل إلى درجة كبيرة وأدىٰ في بعض الحالات إلى الشلل التام وإغلاق الشبكة. في مصطلحات عالم الواقع، كان ذلك معادلاً لمليون مالك جهاز كومبيوتر شخصي يقومون في لحظة واحدة بالاتصال بعشرين موظف خدمة مساعدة فنية خارج عن طوره. النتيجة: سيل لا ينقطع من النغمات التي تعطي إشارة مشغول، وحالة من اليأس مطبقة علىٰ مجموع الزبائن.

«لقد أدرك قراصنة الكومبيوتر Hackers منذ وقت طويل أنه من الممكن شن هجمات أوسع نطاقاً على مواقع خدمة التجارة الالكترونية والتسبب في تعطيل الخدمة Dos، لكن أحداً منهم لم يتجرأ على القيام بذلك قبل الآن»، يقول تويتي فيش، عضو منظمة «كالف أوف ذا ديد كاو» Culf of the Dead Cow، وهي منظمة سرية للصوص الشبكات قام أبطال عملية الهجوم على مواقع التجارة الإلكترونية Dos بإرسال تحياتهم إليها ضمن الشيفرة المستخدمة في هجومهم على أهدافهم. (أعضاء منظمة الـ ديد كاو لا علاقة لهم بذلك). وبحسب تخمينات شركة أمن الكومبيوتر

ICSA هناك مليون قرصان من قراصنة الكومبيوتر في أنحاء العالم، معظمهم من العابثين Script Kiddies أو المتبجحين Wannabes ممن لا يميزون شيفرة الكومبيوتر عن شيفرة «مورس» Morse، لكنهم من الذين يحتمون وراء سواتر الشركات معتمدين على البرمجيات السهلة والمتوفرة أمامهم من مواقع قراصنة الكومبيوتر على الأنترنت المفتوحة لتلقي استفسارات أولئك الذين يعرفون من أين تؤكل الكتف.

ولكن لا تتوقع من الشركات التجارية أن تلجأ فوراً إلى مثل هؤلاء القراصنة للتعرف إلى ما يرمي إليه منافسوها. فالثقة معدومة بين كبار مسؤولي الشركات وصغار العاملين في مجال الكومبيوتر من أمثال مايفريت، ولديهم رغبة ضئيلة في التعامل معهم. والمرة الوحيدة التي تتعامل فيها أقسام تكنولوجيا المعلوماتية في الشركات التجارية مع أمثال هؤلاء هي عندما يساء استخدام صفحة الشركة من قبل بعض العابثين Script Kiddies. عندما تتعاقد الشركات مع خبراء كومبيوتر من الخارج، فالسبب هو دراسة قضية التناظر الجدلي في علم الكومبيوتر. Computer Forensics، الذي يعتبر مجالاً آخر من مجالات الكومبيوتر الحسّاسة. وتستخدم هذه التقنية لضبط أحد الموظفين الناقمين وهو يقوم بسرقة بيانات أو لاعتقال شخص ما يقوم بالتشويش على بيانات سرية من طريق البريد الالكتروني. في عام 1998 تم التعاقد مع مايفريت لجمع الأدلة من أجل دعوى مدنية. فالعشيقة السابقة الناقمة على أحد الزبائن كانت قد سرقت الترخيص لمشبك طبي جراحي دقيق من شركته: «آروسيرجيكال أوف نيوبورت بيتش» Aro Surgical of Newport Beach في كاليفورنيا. قام مايفريت بترميز البرنامج خصيصاً لمراقبة حسابها التجاري على البريد

الالكتروني، معلقاً آماله على أن تكون متهورة بما فيه الكفاية للمضي قدماً في استخدامه. وسر مايفريت عندما رآها تفعل ذلك، متصلة من المنزل. لم يراقب مايفريت بريدها الالكتروني الصادر، لكنه كان قادراً على الاطلاع على الرسائل الواردة.

«كل عشر دقائق كان البرنامج يقوم بتفحص حسابها على البريد الالكتروني، يستخرج نسخاً عنه ويرسلها إلينا، وهو برنامج استغرق مني 45 دقيقة لترميزه. كان بإمكاننا استخدام برنامج آوت لوك بروغرام Out look program لشركة مايكروسوفت، لكني لم أرغب في إزالة أي ملفات من وحدة الخدمة، لأنها لن تحصل عندئذ على بريدها الالكتروني وسينتابها الشك».

إحدىٰ رسائل البريد الالكتروني وردت من شركة كانت قد استدرجتها، وتطرقت إلى وجود الوثيقة وإلى اهتمامهم بالحوار. تلقت آروسيرجيكال إنذاراً يمنعها من استخدام الترخيص المسروق، وكان على شركة e - Eye أن تعد فاتورة بقيمة 240 دولاراً في الساعة.

يعتقد مايفريت أن لديه القدرة الإبداعية على حل أي مشكلة تقريباً بسرعة وبلا عناء ـ والسبب يعود إلى سيرته الأولى أيام كان أحد قراصنة الكومبيوتر. لكن العديد من شركات أمن الكومبيوتر تزعم أنها لن تتعاقد مع أشخاص مثله. فعلى حد قولهم فهم يتوجسون خيفة من ماضيهم الإجرامي. آي. إس. إس. ISS شركة أمن أنترنت مقرها في أتلانتا، كانت على مدى سنوات تشجب استخدام قراصنة الكومبيوتر من قبل منافسيها. وتضمن هذه الشركة نظافة ماضي موظفيها من خلال التحريات التي تُجريها على سجلات حياتهم الماضية. ولكن سبيس روغ Space

Rogue، ناشر كتاب «هاكر نيوز نيتوورك» Hacker News Network، وعضو جمعية «لوفت هيڤي إندستريز» Lopht Heavy Industries، التي هي عبارة عن مركز لكبار لصوص الشبكات في بوسطن، يقول موضحاً أن هناك شركات سبق لها أن تعاقدت مع قراصنة كومبيوتر، لكن من دون أن تدري.

«لا يوجد هناك سجل عام لقراصنة الكومبيوتر يمكن العودة إليه للتحقق من وضع أحد الأشخاص المشتبه بانتمائهم إلى هذه الفئة»، يقول سبيس روغ، الذي أدلىٰ في العام 1998 إلى جانب أعضاء آخرين من شركة «لوفت» Lopht بشهادته أمام الكونغرس بشأن ثلاثة أخطار تتهدد شركة ناسيونال الكترونيك إنفراستركتشر National Electronic Infrostructurs. ويضيف روغ قائلاً: «كل شركة تتبجَّح قائلة: (نحن لا نتعاقد مع قراصنة كومبيوتر)، هي شركة تضلل وتخادع نفسها»

ويصف مدير شركة آي. إس. إس. كريستوفر كلاوس Christopher Klaus، التي بدأت نشاطها في سنة 1994 بمنتجٍ وحيد، الاتصال بقراصنة الكومبيوتر المأجورين، «إنه سلوك ينطوي علىٰ مخاطرة يمكن أن يقود إلى مساءلة قانونية جسيمة». هذه الشركة ذات رأس المال البالغ 3 مليارات دولار، ومقرها في أتلانتا، تتحدث عن أنها «أكبر مصدر في العالم للحلول الإدارية الأمنية للأنترنت»، زاعمة تعاملها مع 5000 زبون، من ضمنهم أكبر 21 من أصل 25 مصرفاً تجارياً و9 من أصل أكبر 10 شركات اتصال، وأكثر من 35 وكالة حكومية. وكلاوس، الذي هو نفسه قرصان كومبيوتر تائب كان ينتحل شخصية «كوُ» Coup، سيخسر كثيراً إذا ما تعامل مع هؤلاء الأشرار.

لكن آي. إس. إس. كانت قد تعاقدت في الواقع مع ستة أو أكثر من هؤلاء القراصنة الذين ذاع صيتهم في السنوات الأخيرة، والمعروفين بكونهم من الحاقدين الناقمين، ومن ضمنهم قرصان معروف باسم «برايم» Prym له علاقة بعدد من الهجمات النوعية على المواقع التجارية والحكومية والعسكرية والبيئية لشبكة الأنترنت: «أطلقوا كيڤن ميتنيك Phree Kevin Mitnick وإلا ضربنا لكم 600 علامة تجارية، «كتب مراهق أخرق في إحدىٰ المرات على صفحة غرين بيس Green Peace. (كان قرصان الكومبيوتر كيڤن ميتنيك آنذاك في السجن في قضية كبرى).

يعترف كلاوس بأن برايم كان على قائمة رواتب شركة آي. إس. إس. ولكن «قررنا سويّاً أن نترك الشركة. ولم يعد يعمل مع آي. إس. إس». وقام موظف آخر من موظفي آي. إس. إس. كان يعمل محرراً لمجلة تدعىٰ فراك Phrack تعنى بشؤون قرصنة الكومبيوتر، مع اثنين آخرين على الأقل بترميز بعض إنجازات برامج قرصنة الكومبيوتر التي خرجت عن نطاق السيطرة وهذه الإنجازات، يقول بعض أخصائيي الكومبيوتر، كانت مسؤولة عن آلاف الهجمات الناجحة على شبكات الانترنت خلال فترة ثمانية عشر شهراً. وعلى الرغم من ادعاء كلاوس أنه لم يكن يعرف شيئاً عن نشاطات قرصنة الكومبيوتر الخارجة عن نطاق القرارات المألوفة لبعض المحترفين الشباب الذين تعاقد معهم من أجل فريقه المجهول X - Team، الذي هو عبارة عن وحدة أمن خاصة داخل الشركة، فقد كانت تلك النشاطات بمثابة سر مكشوف في دوائر قرصنة الكومبيوتر لسنوات عدة. وقراصنة الكومبيوتر من أمثال مايفريت يمقتون تطبيق القوانين، ولا يثقون بالحكومة ولا يطيقون الشركات التجارية.

وعندما ينتقل أحدهم للعمل في إحدىٰ الشركات، يصبح في نظرهم منافقاً تخلىٰ عن جذوره. ورصيد هؤلاء القراصنة حتى اللحظة هو المعلومات، التي تشكل شريان الحياة بالنسبة إلى مهنتهم. من ذا الذي يرغب في مساعدة إحدىٰ الشركات على كسب المال؟ إضافة إلى ذلك، فهؤلاء الذين يأتون متمتعين بمستويات رفيعة من البراعة، غالباً ما يعيشون في عالمين مختلفين: عالمهم الافتراضي الذي هم فيه عبارة عن شخوص وهمية مبهمة تسبر أعمق أغوار مجاهل الأنترنت بحثاً عن ثغرات أمنية. يقومون بابتداع نصوص جديدة، وأحياناً ماكرة، ويتصلون بباعة البرمجيات ليحذروهم من عيوب في منتجاتهم، ويقيمون لهم مواقع على الانترنت للتعليق على مجريات الأحداث، وينشرون نسخاً مسروقة من صفحات Home Pages الشركات التجارية (متوفر على موقع WWW. Attrition. org.).

إنهم في الغالب ناشطو كومبيوتر ذوو ميول فوضوية. المعلومات، التي تشكل العقيدة الأساسية للص الشبكات المخضرم، تريد أن تكون حرة. في عالم الواقع، على أي حال، توفر لهم تلك المعلومات بالذات حول قرصنة الكومبيوتر واختراق أمن الشبكات، من ستة أرقام رواتب ضخمة كمستشاري خدمة أنترنت. إن مجرد كونهم من ذوي الدخل غير المحدود ويدفعون الضرائب بانتظام ومواطنين ملتزمين بالقانون عندما يكونون بعيدين عن أجهزة الكومبيوتر، لا يعني أنهم غيّروا نظرتهم إلى الحياة.

قرصنة الكومبيوتر ليست عملية تراكمية لمجموعة من المهارات الخاصة فحسب، إنما أسلوب من أساليب الحياة، هاجس يستبد بالمرء

على نحو مقلق؛ إنها نوع جديد من فلسفات الألفية أكثر من كونها عملاً محدداً في شركة من شركات «المصادر المعلوماتية».

لا أحد يمكنه تشخيص ذلك أكثر من «ديلدوغ» Dildog، أحد أعضاء منظمة ديدكاو، الذي كان يقيم في جناحه الخاص في الفندق خلال مؤتمر ديفكون Defcon حول قرصنة الكومبيوتر في سنة 1999. فيما ابتسامة مرسومة على محياه. كان ذلك في لاس فيغاس Las Vegas في تموز/يوليو، والحرارة في الخارج تناهز الأربعين درجة مئوية، لكن «ديلدوغ» كان ينعم بالهواء البارد المنعش داخل جناحه المكيف. لقد لاقى الكشف عن برنامجه المتطور لـ «باك أوريفايس» Back Orifice وهو برنامج يكاد يشكل إهانة واضحة لبرنامج «باك أوفيس» لشركة مايكروسوفت، نجاحاً مثيراً. والبرنامج هو عبارة عن إحدى أخطر وأغرب التقنيات التي يستخدمها جاسوس الشركات التجارية. إذ بمجرد تركيبه على شبكة الكومبيوتر لإحدى الشركات المستهدفة (يمكن زرعه بشكل سوي بمجرد إرساله كأداة ملحقة بأدوات البريد الالكتروني) فإنه يفسح في المجال للمستخدم الوصول من موقع بعيد إلى كل زاوية وكل ركن من نظام الشبكة وتحليل كل نشاط من نشاطاتها وكأنه هو مدير أنظمتها. كذلك يمكنه أيضاً اكتشاف جميع كلمات السر والحركات الأساسية ونسخ جميع الوثائق والملفات والتنقل الحر من خدمة إلى أخرى من وحدة التخريم إلى ملفات البريد الإلكتروني، والإبحار عبر قواعد البيانات الحاوية على مجموعات كبيرة من البطاقات الائتمانية، ومن ثم شق طريقه إلى مخزونات هائلة من المعلومات والبيانات الشخصية التي تم تجميعها من الزبائن. وجاءت وحدة الـ «سوفت وير» Soft Ware أيضاً مزودة ببرامج

يمكنها تشغيل المايكروفونات المدمجة وكاميرات أجهزة الكومبيوتر الشخصية والتحكم بها من دون علم صاحبها. وأي شخص يمكن أن يكون تحت المراقبة وتسجيل خصوصياته في أي وقت. فلنسمها «كوربوريت كام» Corporate Cam، أو علم كومبيوتر الشركات.

ولكن ليس هذا ما حدا بـ «ديلدوغ»، الذي يكسب أموالاً طائلة في إحدىٰ شركات التكنولوجيا، لاختراع هذه التقنية. فعلى الرغم من مزاعم صانعي البرمجيات وشركات أمن الكومبيوتر وصانعي التقنيات المضادة لڤيروسات الكومبيوتر ورجال القانون أن إطلاق برنامج باك أوريفايس 2000 كان مجرد طريقة لقراصنة الكومبيوتر لإضفاء الصفة الشرعية والقانونية على انتهاكات الشبكات، فإن «ديلدوغ» يقول إنه يحاول فقط أن يشير إلى مشكلات كامنة مع برمجيات مايكروسوفت. إن شركات أمن الكومبيوتر «تخشىٰ الاعتراف بأن نظام تحرياتها متصدع وضعيف إلى درجة مخيفة»، يقول «ديلدوغ» ويضيف: «[إنهم] يعطون الناس الانطباع أن برمجياتهم تؤلب القضاء على قرصان الكومبيوتر العادي. لسوء الحظ، هذا أيضاً يستغبي أصحاب الشبكات الحساسة فعلياً من خلال دفعهم إلى الاعتقاد أن هذا البرنامج كاف لحمايتهم. أولئك الذين يثقون بهذا النظام لحمايتهم... هناك مفاجأة بانتظارهم».

حشد من المعجبين، معظمهم في العشرينيات من العمر بالزي الأسود الفاحم وآثار الوشم البادية عليهم وشعرهم الأشعث، كانوا بانتظار «ديلدوغ» في جناحه في الفندق. من أصل 3000 قرصان وعابث ومتبجِّح وعاهر (من زمرة قراصنة الكومبيوتر) وأخصائيي أمن كومبيوتر وصحفي

وعميل سري وعميل مكتب تحقيقات من الذين حضروا مؤتمر ديفكون حول قرصنة الكومبيوتر سنة 1999، كان ألفان منهم قد احتشدوا في قاعة المؤتمرات في فندق «ألكسيس بارك أوتيل» Alaxis Park Hotel لمتابعة إطلاق برنامج بي. أو. تو. كيه Bo2k. في السنة السابقة، كانت منظمة ديدكاو قد اختارت ديفكون لترويج أول نسخة من برنامجها «باك أوريفايس». هذا البرنامج الذي كتبه أحد أعضاء المنظمة. «سير دايستيك» Sir Dystic كان يعمل على مواقع «ويندوز» Windows 95 و98 من خلال ابتكار منفذ خلفي يستطيع المستخدم بواسطة إدارة العمليات كافة على تلك الأجهزة من مكان بعيد.

وكانت نسخة «ديلدوغ» المطورة والمرمَّزة قد صممت للعمل على شبكات تتناسب وبرنامج ويندوز NT، وقد موهت نفسها بطريقة متقنة للغاية. ولم يقطع أعضاء منظمة ديدكاو كل هذه المسافة إلى لاس فيغاس ليخيبوا الآمال. بدأوا المؤتمر بعرض ليزري بلغ ذروته بصوت إلكتروني يصم الآذان أشبه بالمُواء. تحلق الجمهور حول «ديلدوغ» محيياً. بعدها، وبينما شرع «ديلدوغ» ومساعدوه يشرحون مبرراً موقف مايكروسوفت إذا ما أخذت منتجاتها تعمل على «شفط» الفلسفة، جرىٰ عرض لصاقة سي. دي. روم. على الجدار وراءه، رأس بقرة يدور ويدور بشكل سريع. في نهاية العرض أطلق أعضاء المنظمة اثني عشر سي. دي. روم. تحتوي على برنامج باك أوريفايس المطور. الجمهور اندفع إلى الأمام.

صانعو البرامج المضادة للڤيروسات وممثلو شركات أمن الكومبيوتر كانوا يراقبون عن كثب، على أمل أن يتمكنوا من ضبط أحد ما ومعه

نسخة. أول من سيتمكن من اختراق البرنامج سيفوز بحقوق الشهرة والتباهي Bragging rights، وأسماؤهم ستنشر في بيان صحفي، ربما أيضاً في بعض المجلات والمقالات الصحفية، كأبطال أحبطوا النوايا الشريرة لعصابة قراصنة كومبيوتر منظمة ديدكاو.

أحد موظفي شركة (آي. إس. إس) ألقىٰ بنفسه وسط الحشد وتمكن من اختلاس نسخة. وخلال 24 ساعة، ستتمكن الشركة من اختراق أجزاء من البرنامج وإطلاق نسخة مطابقة تضاهيها. في خلال ذلك الوقت، لم يكن «ديلدوغ» على علم بذلك، ولكنه ما كان ليكترث حتىٰ ولو كان يعرف. وعلى حد زعم «ديلدوغ» في محادثة سابقة عبر الإنترنت، تقرب منه أحد موظفيه وسأله عن مقدار الرشوة التي يمكن أن تدفعه الشركة في مقابل تسريب نسخة أولية عن البرنامج، يقول «ديلدوغ»: «النقود لا تحفزنا»، وأضاف: «ولكن على سبيل الدعابة قامت المنظمة بإرسال مذكرة إلى موظف آي. إس. إس. تقول فيها إنها ستأخذ مليون دولار وشاحنة عملاقة. بعد ذلك، شعر أعضاء المنظمة بالإنزعاج لاكتشافهم أن الديسكات الأصلية المبعثرة في ديفكون قد تعرضت للإصابة بڤيروس «تشيرنوبل» Chernobyl. «أمر محرج جداً»، يعترف تويتي فيش قائلاً.

على الرغم من أن آي. إس. إس. كانت في غاية السرور لاكتشافها حقيقة أن بوسعها التجسس على البرنامج، فإن ديلدوغ كان على يقين تام من أن الشركات لن تكتفي بهندسة معاكسة له، إنما سرعان ما ستخرج بتقنية لإزالته. هذا هو السبب وهذا ما حدا به إلى إطلاق برنامجه «كمصدر

مفتوح»، ما يعني أنه سيكون بوسع قراصنة الكومبيوتر في أنحاء العالم كافة تعديل الشيفرة بما يتلاءم واحتياجاتهم. واعتماداً على خبرته السابقة، قدر ديلدوغ أن برنامج بي. أو. تو. كيه سينتشر عندئذ كالڤيروس، متشكلاً ربما في عشرات النسخ المختلفة. وقام بإحصاء أكثر من 300,000 عملية تفريغ لبرنامج باك أوريفايس الأصلي، الذي كان يعمل على ويندوز 95 و98 فقط ونشر بشكل أولي من طريق أداة ملحقة بالبريد الإلكتروني. ومن يدري كم من النسخ الأخرىٰ قد تم تداولها من صديق إلى آخر، من قرصان كومبيوتر إلى آخر، ومن متعد على الشبكة إلى أحد الضحايا؟ لكن «ديلدوغ» لم يكن يأبه لذلك. وعلى غرار «لويس مول»، مخرج الأفلام الفرنسي الذي قال يوماً: «أنا أحب الفوضى، لكنها تخرج طاقم العمل عن طوره»، كان ديلدوغ يستمتع بالفوضىٰ والتشويش، معتقداً أن السؤال كان عادة أهم من الجواب.

في نظر قرصان الكومبيوتر، هناك أمر واحد فقط يمكن أن يكون أسوأ من التعامل مع شركة تجارية، ألا وهو تناول طعام الإفطار مع أحد رجال القانون. وكذلك عدد من المتبجحين من مداهمة أعضاء مكتب التحقيقات الفيدرالي لمنازلهم مهددين بالمذكرات القضائية ومصادرين أجهزة الكومبيوتر. «ولا يبدو أيضاً أن أعضاء مكتب التحقيقات مستعدون لإعادة ما يصادرونه»، يقول مايفريت الذي تعرض لمداهمة عملاء مكتب التحقيقات سنة 1998. «وحتى لو أعادوا ما صادروه، فإن السرعة التي تتطور بها التكنولوجيا تجعل من التكنولوجيا السابقة موضة قديمة على أي حال. وهكذا فهذا في الحقيقة أحد أساليبهم في معاقبتك دون أن يكلفوا أنفسهم عناء مقاضاتك لدىٰ المحاكم». أن النظر في أي دعوى قد يكلف

ما بين 2000 ـ 5000 دولار، وربما 20,000 دولار، للنظر في القضايا القانونية الأكثر خطورة، أو أكثر من ذلك.

فريق دفاع كيفن ميتنيك، الذي لم يدفع له سوىٰ جزء ضئيل مما يكسبه عادة للدفاع عن أحد مدمني الكومبيوتر من عاثري الحظ، قدم للحكومة كشف حساب عن 3000 ساعة عمل على مدىٰ 3 سنوات، لكنه أنفق أكثر من ضعف هذا المبلغ. وقياساً إلى أتعاب محامي لوس أنجلوس، فهذا يعني أن كشف حساب ميتنيك كان سيتجاوز المليوني دولار، لو قام بتسديده وفقاً للدفعات القانونية. لماذا تباطأت قضيته على هذا النحو؟ نظراً لأن «النيابة العامة [كانت] تحاول أن تجعل منه عبرة للآخرين»، كما يظن «جينفر غرانيك» Jennifer Granick، أحد محامي سان فرانسيسكو الذي دافع عن عدد من قراصنة الكومبيوتر.

ما الذي اقترفه ميتنيك حتى يؤول به المآل إلى خمس سنوات في السجن؟ وفقاً لمذكرة الاتهام فقد نسخ الشيفرة السرية لبرنامج أحد أجهزة الكومبيوتر وأحد أجهزة الهاتف الخليوي التي تعود ملكيتها إلى شركات موتورولا Motorola ونوكيا Nokia وصن Sun وتقدر قيمتها، بحسب زعم الحكومة بثمانين مليون دولار. في الأساس وجهت إليه تهمة التجسس الاقتصادي، قبل أن يكون هناك قانون في هذا الشأن. ويعترف ميتنيك الذي حكم عليه بالإقامة في أحد مراكز التأهيل عندما كان مراهقاً للعلاج من مرض هوس الكومبيوتر، يعترف بجمع هذه المعلومات، لكنه لم يطلع عليها أحداً على الإطلاق. فقد زعم أنه كان يريد دراستها.

«عندما كان في السجن كانت عيناه تلتمعان كلما كنا نتطرق في حديثنا إلى شيفرة الكومبيوتر، يقول «برايان مارتن» Brian Martin،

المعروف أيضاً بـ«جيريكو»، خبير موقع attrition. org.، الذي يتعقب جرائم الكومبيوتر، وعضو سابق في فريق دراسة التناظر الجدلي لكومبيوتر دفاع ميتنيك of the Mitnick defense's computer forensies team. كيف تمكن ميتنيك، المعروف بمهاراته المتواضعة في مجال الكومبيوتر ومهاراته المتميزة في مجال الحرفنة الكلامية، من تحقيق ذلك التعديل على صعيد برنامجه؟ مع موتورولا، يقول ميتنيك، كان سهلاً. في أحد الأيام، وفي طريق عودته إلى المنزل بعد انتهاء عمله، توقف عند أحد أكشاك الهاتف العمومي، وقام بعد أن انتحل شخصية مهندس بالسؤال عن الشيفرة الأساسية لأحد الهواتف الخلوية الجديدة. «بعد بضع دقائق اتصلوا بي ثانية وأخبروني أنه قد سبق نقله إلى حساب مباشر كنت قد أعطيتهم إياه، يقول ميتنيك. لكنه في الوقت الذي وصل فيه إلى المنزل كان قد حصل على تصاميم آخر منتجات موتورولا.

بالنسبة لذلك النوع من الجرائم المجردة، فقد كانت مناورات الحكومة خرقاء إلى أبعد الحدود، وكأنها تتعامل مع أحد السياح. لم يصر إلى رد طلب الكفالة الذي تقدم به متينيك، وإنما رفض سماع الدعوى.

دونالد راندولف، المحامي الذي عينته المحكمة للدفاع عن ميتنيك، يقول إنه لم يسبق له أن سمع مطلقاً بمثل ذلك خلال السنوات الخمسة والعشرين من حياته المهنية. استغرق ذلك سنة كاملة تقريباً إضافة إلى عدد من الاستدعاءات المقدمة من قبل راندولف، قبل أن تسلم جهة الادعاء الفيغاباتيس التسعة للدليل الالكتروني التي كانت قد جمعتها لكي يتمكن الدفاع من إعداد ملفه. محامو الادعاء كانوا ممتنعين عن إعطاء ميتنيك جهاز كومبيوتر صغير laptop لإعداد دفاعه. معظم دواعي التأخير

كان مصدرها ذلك الخوف غير المبرر من أن يتمكن ميتنيك، من دون مودم ـ من شفاء غليل غضبه من السجن. في الحقيقة، فقد نسب مسؤولو السجن إلى ميتنيك قدرات خارقة تليق بجيمس بوند. زج به في إحدى المرات في زنزانة انفرادية لأن مسؤولي السجن كانوا يخشون أن يتمكن من تحويل آلة التسجيل «الووكمان» إلى جهاز إرسال على موجة إف. إم. يمكن استخدامها في التنصت على مكتب آمر السجن.

عندما يعود المؤرخون القانونيون إلى قضية ميتنيك يجدون أنفسهم في حيرة من أمرهم حيال المراسيم والقرارات الأكثر غرابة للقاضي ماريانا فايلرز. مع قضية التشفير، دخلت قضية ميتنيك مرحلة جديدة. لعلها القضية الأولى التي يتم فيها مقاضاة قضية التشفير جنائياً، «يقول راندولف من سانتا مونيكا، وهي شركة مقرها كاليفورنيا اسمها «راندولف آند ليڤاناس». «ولكن كونوا مستعدين، فإنها ستغدو قضية دائمة بدءاً من الآن»، خصوصاً بعد أن كانت وزارة العدل تحوم ولفترة حول فكرة سيئة جداً تدعى «قانون الأمن الإلكتروني لشبكة الأنترنت Cyberspace Electronic Security Act. القانون كان يبعث على الخوف لعدة أسباب؛ لأنه سيمكن المحققين من الدخول خلسة إلى منزلك أو ممتلكاتك الخاصة، والبحث عبر جهازك الكومبيوتر، أو دس برامج من دون علمك بوسعها أن تتقاطع مع عناصر إدخال البيانات، مع كلمات السر، مع مراسلاتك الخاصة على موقع البريد الالكتروني وحواراتك المباشرة ـ أو إبطال برامج التشفير. لحسن الحظ، بعد أن تسرب نص الاقتراح وقوبل بعاصفة من الرفض، عمدت وزارة العدل إلى طيه بهدوء.

لكن الأمر الذي لا زال مقلقاً هو اعتماد المجرمين أكثر فأكثر على

التشفير. لسوء الحظ، فإن الحل المقترح هو أشبه باللجوء إلى التفتيش بواسطة الأقمار الصناعية عن لص سرق محفظة لاعتقاله. بالطبع، المفارقة لم يتم التفريط بها من قبل قراصنة الكومبيوتر: وزارة العدل كانت تطلب الإذن للدخول إلى أنظمة كومبيوتر الأميركيين والشركات الأمريكية والحكومة الأمريكية.

مع ميتنيك، فقد تركزت القضية حول شريحة من البيانات المشفرة التي عثر عليها في جهاز الكومبيوتر الصغير Laptop الذي كان بحوزته عند اعتقاله سنة 1995. وبما أن جهة الادعاء عجزت عن اختراق هذه الشيفرة، اشترطت تسليمها مفتاح الشيفرة مقابل عدم تسليم الدفاع ما تم اكتشافه، فوافق القاضي على ذلك. «في الأساس، كانت جهة الادعاء تبرر امتناعها، فإلى جانب حقهم الدستوري في الاطلاع على أدلة الاتهام، فإن محامي الدفاع عن ميتنيك كانوا يرغبون في معرفة ما إذا كانت هناك أدلة تشير إلى براءته عن تسليم الأدلة، يقول، راندولف. «على حد علمنا، لم يتم اللجوء إلى مثل هذا الأسلوب من قبل».

فلو كان ميتنيك مثلاً قد حصل على الشيفرة الأصلية لهاتف موتورولا الخلوي من مصدر غير موتورولا، لما كانت وجهت إليه تهمة الاحتيال من خلال الكومبيوتر (كان يمكن اتهامه بحيازة أملاك مسروقة، التي ستعتبر جنحة). وشيفرة موتورولا الأصلية، وشيفرة صن ونوكيا كانت متداولة في أوساط قراصنة الكومبيوتر على مدى سنوات.

ماذا كانت نتيجة المعاملة السيّئة التي تلقاها كيفن ميتنيك؟ المئات من الهجمات على مواقع الشركات ومواقع الحكومة والمواقع العسكرية احتجاجاً على هذه المعاملة؛ وأخذت مواقع مثل Kevinmitnic. com

وFreekevin. com تقوم بنشر آخر أخبار كيڤن ميتنيك. معظم التقارير المنشورة سخرت بالطبع من تنفيذ القانون على هذا الشكل. وقد أطلق مارتن هذه الدعابة على موقع attrition. org.: وكالة الأمن القومي، وكالة الاستخبارات المركزية ومكتب التحقيقات الفيدرالي، جميعهم يريدون أن يثبتوا أنهم الأفضل في اعتقال المجرمين. وهكذا فإن الرئيس يختبرهم بإطلاق أرنب نحو الغابة، ويأمر كلاً منهم بالإمساك به. وكالة الأمن القومي تقوم بنشر عناصر استخباراتها وتكلفهم بالإبلاغ عن الحيوانات الموجودة في الغابة وتقوم باستجواب جميع الشهود من نباتات ومعادن. بعد ثلاثة أشهر من التحقيقات المكثفة، تستنتج الوكالة أن الأرانب غير موجودة. وكالة الاستخبارات المركزية، بعد أسبوعين من عدم العثور على أية أدلة، تعمد إلى حرق الغابة بكاملها، والقضاء على كل ما فيها، بما في ذلك الأرنب. وتعلن إحدىٰ الوكالات المجهولة الهوية بأن سي. آي. إيه قامت بهذا العمل. وبعد ساعتين يخرج عناصر مكتب التحقيقات الفيدرالي من الغابة وبحوزتهم دب مهشم من شدة الضرب وهو يصرخ مستغيثاً: «أنا أرنب، أنا أرنب، أنا أرنب».

لصوص الشبكات متنبهون دائماً من مكتب التحقيقات الفيدرالي. فعندما تلقى مايفريت اتصالاً من السائح المزعوم خالد إبراهيم، عضو حركة الأنصار، (وهي مجموعة انفصالية هندية متشددة مدرجة على قائمة وزارة الخارجية التي تضم أخطر ثلاثين منظمة إرهابية في العالم)، كان يفترض أن إبراهيم يعمل لمصلحة مكتب التحقيقات الفيدرالي. تكمن أسباب عديدة وراء عدم اضطلاع القانون بمهمة مكافحة الجرائم الرقمية. الأفضل والأكثر نجاحاً يعمدون إلى الاستقالة من وظائفهم والعمل في

شركات التكنولوجيا التي تدفع لهم ثلاثة أضعاف ما كانوا يتقاضون. (أنت لا تسمع أبداً عن عالم تكنولوجيا يترك وظيفة تدر عليه دخلاً يتجاوز المائة ألف ليلتحق بوظيفة في مكتب التحقيقات الفيدرالي).

منفذو القوانين هم أيضاً أمام حقائق عالم الأنترنت. على عكس مسرح الجريمة في عالم الواقع، لا يسعك أن تسرق مجمل شبكة الكومبيوتر لموقع بريد إلكتروني ضخم مثل موقع «ياهو»! الوسائل التقليدية للتعامل مع الجريمة التي أثبتت نجاحها ضد الإرهاب وجرائم الشوارع، لا تجدي نفعاً في مجاهل عالم الأنترنت. ومع ذلك، فإن مكتب التحقيقات يبذل قصارى جهوده على هذا الصعيد؛ فهو يرسل العملاء التقليديين لتعقب جرائم الكومبيوتر. وهؤلاء العملاء لا يميزون عنوان موقع عالمي على الويب URL من جسم مجهول UFO، وهذا ما يجعل مكتب التحقيقات يظهر من خلال ضوء معتم على موقع الشبكة. «مكتب التحقيقات يخرج من دون دليل عندما يتعلق الأمر بقراصنة الكومبيوتر»، يقول مارتن: «مفهومهم عن استراتيجية الجريمة يتمثل في تعقب الشائعات على الأنترنت على أمل أن يكون أحد القراصنة من الحماقة بحيث يعترف بشيء ما».

هذا هو الأسلوب الذي اتبعه مكتب التحقيقات لتعقب الشخص الذي يعتقد أنه قام بهجوم شباط 2000 وأدىٰ إلى تعطيل خدمات الشبكة. بعد أسبوع من الموجة الأولىٰ من الهجمات، اعتقد مكتب التحقيقات أنه وجد ضالته: فتىٰ في العشرين من عمره ذو وجه تملؤه البثور، يمتلك مهارات متواضعة في مجال الكومبيوتر، يعتقد المحققون أنه أقام حاجزاً إلكترونياً من خلال عمله في مجال المساعدة الفنية في إحدىٰ شركات

صناعة قطع الغيار في ديربورن ـ ميتشيغان. على الرغم من أن التقديرات كانت تتجه بقوة نحو هوية المتهم، فإن اللصوص، والمتسمرون على الشبكة والقراصنة وأولئك الذين كانوا يتخذون مواقع سرية على شبكة الانترنت، كانوا يرتكبون ما يسمى بـ «التباهي المتسلسل»: مستمدين شهرتهم من الهجمات على أقنية حوار اللصوص. العديد منهم انتحل مستهتراً اسم «مافيابوي»، أحد الأسماء المحتملة التي وردت في سلسلة من التقارير الإخبارية حول التحقيق. كان هنالك العشرات من عناصر المافيابوي يصولون ويجولون في أنحاء الانترنت خلال الأيام والأسابيع التي أعقبت الهجمات التي أدت إلى تعطل الخدمة Dos. لكن أحد المتبجحين من قراصنة الكومبيوتر تميز عن البقية؛ «بيغ فارمر»، المعروف أيضاً بـ «يوروستايلن»، و«بين فارمر»، كان قد أرسل رسالة إلى مارتن عبر البريد الإلكتروني على موقع attrition (قال بأنه نصير) مباشرة بعد أول موجة من الهجمات متفاخراً بإنجازاته. وعندما عجز عن الإجابة عن أسئلة بسيطة تتعلق بالهجمات، جرى استبعاده مثل غيره من الحمقى الطامحين إلى بريق الشهرة.

عندما قام المتهمون الحقيقيون بإطلاق سيل من مجموعات الرسائل الإلكترونية على مدى أسبوع ـ (أمازون، تشارلز سكواب، داتيك، زدينت، ولايكوس، من جملة المواقع الأخرى ـ) وسع بيغ فارمر من نطاق اتصالاته، وبدأ بإرسال الرسائل من أمريكا بشكل مباشر إلى عشرات الصحفيين على أمل أن يصغي أحدهم إليه. لكن أحداً لم يفعل. وكان بيغ فارمر، الذي انتحل هذا الاسم لأن والديه يمتلكان مزرعة لتربية الخنازير وزراعة الفاصولياء والذرة، قد قال في حوار مع بعض أصدقائه المزعومين

على شبكة الإنترنت IRC: أرسلت بريداً إلكترونياً إلى خمسة عشر صحفياً على أمل أن أتلقىٰ رداً ولكنهم لم يتجاوبوا فهم أفادوا بأنني غير شرعي، ولكني سأريهم. وقد زعم بوقاحة أنه سيضرب الـ سي. إن. إن. CNN وتايم وورنر Time warner في اليوم التالي، وقد هوجما بالفعل.

عندما سأله مارتن بعد الموجة الأولى من الهجمات عن سبب قيامه بذلك، أجاب بيغ مارتن: «إذا ما لاحظت الأهداف، تجد أنها جميعها شركات تعمل في مجال الدعاية والإعلان، وهذا كان محاولة لإثارة الذعر في نفوس المساهمين في شبكة الأنترنت» ولكن من دون دليل قاطع، لا يمكن لمارتن أن يكون واثقاً. بعدها قام بإيصال البريد الإلكتروني الذي كان بيغ فارمر قد أرسله إلى جيمس إم. آتكنسون، مؤسس مجموعة غرانيت آيسلاند غروب Cranite Island Group في غلوستر، ماساشوستس، وهي شركة متخصصة في مكافحة الرقابة الفنية آتكنسون، وإضافة إلى قيامه بعمليات تنصت سرية على الشركات، فهو أيضاً متعقِّب محترف لقراصنة الكومبيوتر. نظراً لعلاقات آتكنسون الوثيقة مع رجال القانون، فقد كان على معرفة بالعملاء الذين ليس لديهم أدلة على بيغ فارمر. وأن مكتب التحقيقات يتخبط في تحقيقاته في قضية الشخص الذي عطل الخدمة Dos بسبب هجماته. كل ما كان عليه أن يبدأ به هو بريد بيغ فارمر الالكتروني والذي كان شكل وصمة عار. لم يكن هنالك ثمة أدلة لإجراء تحقيق. لكن أنكتسون قرر تكريس بضعة أيام من وقته ليرى إذا كان بوسعه تقديم مساعدة.

لم يستغرق منه كثير وقت لتحديد دليل عناوين ملفات بيغ فارمر،

وصفحة رئيسية كاملة على موقع أمريكا أون لاين AOL مع صور لشاحنة حبوب وسيارة محدَّثة.

أتكنسون، الذي قام بإجراء مئات التحريات في مشاريع كهذا المشروع، لم يكن متخصصاً في إلقاء القبض على المجرمين الرقميين Digital Criminals. كانت شركته تركز على عمليات التنصت والتحري من خلال مراقبة الخطوط الهاتفية وحماية الشركات التجارية والوكالات الحكومية ضد التحريات أو عمليات التجسس التقنية اللامشروعة.

«استغرقت مني لمعرفة هوية ذلك الشخص 23 دقيقة»، يقول أتكنسون. «الطريقة التي تتمكن من خلالها التعرف إلى هوية أولئك العابثين، تتلخص في البحث عن أدنى الهفوات أو أتفه الزلات التي يرتكبونها. عندما تمكن بيغ فارمر من الوصول إلى رجال الإعلام، ترك وراءه أثراً قاد إلى التعرف عليه».

على موقع أميركا أون لاين AOL، وجد أتكنسون صورة لسيارة حمراء قانية من طراز 1999 بعجلات من الكروم ـ والأهم من ذلك، بزجاج نوافذ قاتم. كان بيغ فارمر قد أزال رقم اللوحة من الصورة، لكنه أبقىٰ على لمعان السيارة. وكان بمقدور أتكنسون استخلاص صورة لهدفه عن طريق التقاط صورة لسيارته بكاميرا رقمية ماركة سوني، واستخدام الفلاش في وضح النهار. كان بيغ فارمر قد تلقىٰ مخالفة بسبب زجاج سيارته القاتم، وهو أمر بدا بأنه يعتز به، حيث حاول ومن دون طائل أن ينقل صورة سيارته بطريقة المسح Scan إلى صفحته الرئيسية الخاصة، لكن الملف تعرض للتلف. من ملف يحتوي على 680 كيلوبايت، لم يتبق سوى 630ك. قام أتكنسون بإسقاط كامل الموقع على محطة سيليكون

غرافيكس Silicon Graphics الخاصة به وعمل على استعادة أجزاء الوثيقة التالفة وترميمها. وكان فارمر قد أزال اسمه وعنوانه عن قسيمة المخالفة. ولكنه لم يزل رقم القسيمة ورقم اللوحة والتاريخ والوقت. فقام أتكنسون بالاتصال بشرطة ولاية ميتشيغان، وفي غضون 90 دقيقة زوده أحد الضباط باسم أحد الأشخاص المحتملين وعنوانه وبقية المعلومات المتعلقة به.

«تفاخر بيغ فارمر بشأن هجماته السابقة واللاحقة»، يقول أتكنسون. «يبدو أنه كان يفعل ما بوسعه ليلفت إليه الانتباه». وبينما كانت جانيت رينو تصرخ من وراء الكواليس مطالبة بعقد مؤتمر صحفي للإعلان عن اعتقال أحد الأشخاص، تلقىٰ مكتب التحقيقات أكثر من اثني عشر استدعاءً للشهادة وقام باستدعاء بيغ فارمر للاستجواب، لكن عملاء مكتب التحقيقات ومحامو وزارة العدل سرعان ما أدركوا أن كل ما كان لديهم هو مجرد متبجح قديم من قراصنة الكومبيوتر في العشرين من عمره كان قد أضاع وقتهم.

كان بيغ فارمر يقرأ كل ما تقع عليه عيناه عن الهجمات التي أدت إلى تعطل نظام الخدمة Dos من خلال وسائل الإعلام، ثم يسارع في الحال إلى التباهي بذلك مباشرة على موقع الشبكة من خلال قنوات الحوار Chat Channels ومواقع البريد الالكتروني. لو كان التفاخر جريمة، لكان بيغ فارمر يقضي الآن حكماً بالسجن مدىٰ الحياة. عوضاً عن ذلك، فقد سمح له بالمغادرة.

بالطبع، لو لم يكن هنالك قراصنة كومبيوتر يتفاخرون بجرائمهم، لما كان لي عمل أقوم به، «يقول رجل معروف بالأحرف الأولىٰ من اسمه: جيه 3 «J3». يتعقب جيه 3 قراصنة الكومبيوتر في مخابئهم السرية،

يراقب أقنية المراسلة على شبكة الانترنت Internet Relay Chot، متحرياً آخر المعلومات عن اختراق نظام المكالمات الهاتفية Phreaking، الاتصال بأرقام لوحات الإعلانات والتحري عن مواقع شبكة الانترنت التي تقدم برامج عن اختراق كلمة السر ودليل إرشادات عن كيفية القيام بذلك. بالنسبة لـ جيه 3 لم يكن هذا مجرد هواية، بل مهنة. شركة أمن الكومبيوتر ISCA قامت بالتعاقد معه ليعمل بصفة جاسوس شبكات. عندما يتلقى معلومات عن أية ثغرة أمنية، يقوم بتسريب المعلومة إلى الهيئة الفنية لشركة أمن الكومبيوتر، بحيث تتمكن الشركة إما من تطوير نظام دفاعي أو تقوم بتحذير صانعي البرمجيات قبل أن يصار إلى استغلال هذه الثغرة. «وإذا ما وقعت على الملف السري لإحدىٰ الشركات منقول على أحد مواقع شبكة الأنترنت، أو أن لصوص الشبكة لهم جذورهم في إحدىٰ الشبكات، أو أن أحد المواقع التجارية الذي يتضمن قاعدة بيانات البطاقات الائتمانية لصاحب الموقع قد تم اختراقه»، يقول جيه 3: «عندها أقوم بالاتصال بالشركات لتحذيرها».

مع ذلك، فقراصنة الكومبيوتر لا يزالون يتوافدون من كل حدب وصوب، والاجراءات القانونية لم تحقق سوىٰ قدر ضئيل من النجاح في اكتشاف أولئك القراصنة. هذا يظهر أنه على الرغم من النزاع القائم بين لصوص الشبكات فهي تحتاج إلى دعائم الشركات التجارية في أمريكا، فالمسألة تحتاج إلى وقت قبل أن يتحول أولئك اللصوص نحو الانترنت للتزود بالمعلومات القيمة عن الأبحاث العلمية من الشركات المنافسة. ولا يتطلب الأمر من ويليام جيبسون كثير خيال للتنبؤ لمعرفة بأن الأنترنت سيكون الميدان التجاري لمعركة المستقبل.

لقد أدى نشوء قواعد بيانات هائلة وابتكارات على صعيد تقنيات فرز المعلومات إلى ظهور ما يسمى بالتخمة المعلوماتية. ومع انتشار الانترنت أخيراً، بوسع القرصان البارع الكشف عن أسرار إحدىٰ الشركات على الفور ببضع نقرات على لوحة المفاتيح. مثل هذه المعلومات كانت وعلى مدى عقود محفوظة في أماكن سرية آمنة بعيدة عن متناول يد العابثين، حتى أولئك الذين قاموا بوضعها، أو كانت محفوظة بعيداً في خزائن يعلوها الغبار في مقرات الشركات. لقد أدى التحول نحو أجهزة الكومبيوتر الشخصية الصغيرة والخدمات المحلية خلال فترة التسعينيات إلى توزع هذه البيانات في كل حدب وصوب. تحمل أجهزة الكومبيوتر اليوم نصف مليار حساب مصرفي ونصف مليار حساب بطاقة ائتمانية و200 مليون ملف ائتماني (ملف واحد تقريباً لكل أمريكي تجاوز الثامنة عشرة)، ومئات الملايين من أرصدة الرهونات العقارية والأرصدة التقاعدية والفواتير الطبية وغير ذلك. هذا فقط من جانب المستهلك. هنالك أيضاً الآلاف من شبكات الكومبيوتر التجارية التي يمكن الوصول إليها من الخارج عبر خطوط الهاتف، كونه ينبغي على الموظفين أن يكونوا قادرين على إجراء اتصال هاتفي من مكان بعيد. لكن السماح بدخول البعض وإبقاء البعض الآخر خارجاً، أثناء القيام بنشاطات أساسية كالبريد الالكتروني والإبحار عبر الانترنت، هو عمل ينطوي على تحد. لم يتمكن أمن الكومبيوتر على الرغم من تقنياته المتعاظمة من وضع حد لقراصنة الكومبيوتر هؤلاء. وإذا كان للشركة موقع على الأنترنت، فهو عرضة للانتهاك من قبل أحد لصوص الشبكات عبر صفحة الشركة الرئيسية مباشرة.

هذه هي الطريقة التي تمكن من خلالها فتىً في الصف الأول الثانوي لم يتجاوز العشرين من عمره من سكان ضواحي أمريكا من اختراق أهم مركز أبحاث نووية في بومباي ـ الهند ـ في أيار 1998. كان يتابع ريبورتاجاً تلفزيونياً حول تجارب الهند النووية التي قامت بإجرائها تحت سطح الأرض، ولسبب أو لآخر ولدت لديه هذه المشاهد امتعاضاً واستياءً دائمين. لم يكن يعرف السبب بالتحديد. برغم كل شيء، فقد كان صغيراً جداً ليتذكر هيروشيما وناغازاكي وأزمة الصواريخ الكوبية. لم يتمكن حتى من تحديد موقع الهند على الخارطة. بلد بائس من بلدان العالم الثالث عاجز تقريباً عن سد رمق أبنائه بالذات، يدخل في سباق تسلح نووي مع باكستان والصين. كلما كان يمعن أكثر في التفكير بذلك، كلما طار صوابه أكثر. وهكذا قرر أن ينتقم من الهنود. وسوف يقوم بذلك من دون أن يغادر غرفته. على موقع الأنترنت العالمي حيث كان هذا اللص الظريف الشاب يمضي معظم أوقاته، انتحل لنفسه اسم تي. ثري. كيه ـ ناين t3k-9 الذي يلفظ (تيك ناين) Tech-9. كان بارعاً بشكل خاص في فك رموز كلمات السر ومعطيات التشغيل Log-ins التي تشكل مفاتيح الولوج إلى أنظمة الكومبيوتر. في هذا اليوم بالذات تسلق السلم إلى الطابق العلوي بخطى متثاقلة حاملاً بين يديه وجباته القرصنية المفضلة من شوكولا البوب تارت والكوكا كولا وحلوى الجوبريكر (حلوى مستديرة قاسية) ـ ثم توجه نحو غرفة النوم حيث كان يضع جهاز الكومبيوتر ويستمع إلى أصوات المودم الحادة.

بدأ عمله بالدخول إلى الموقع مستخدماً محرك البحث Infoseek ثم وضع نظام البحث على وضعية إن أتوميك in atomic المساوية لطباعة

عبارة: India, atomic research (الهند، أبحاث ذرية). أحد أول المواقع التي ظهرت على الشاشة كان موقع «مركز بهابها للأبحاث الذرية» BARC في الهند، والذي كان قد قرأ عن دوره الحيوي في مساعدة الهند على تطوير القنبلة الذرية.

شق طريقه نحو موقع BARC ثم قام بإدخال نظام فك الشيفرة (جون ذا ريبر دي. إي. إس إنكريبسبشن كريكر سوفت وير) John the Ripper Des Encryption Craker Soft Ware الذي كان قد حمَّله من الأنترنت والذي يحتوي على آلاف مؤلفة من البرامج المعقدة لقراصنة الكومبيوتر والأدلة «الإرشادية» المتوفرة على مواقع الانترنت وأقنية المحادثة لقراصنة الكومبيوتر. جهاز فك الشيفرة الذي يعمل عن طريق إنشاء برنامج إدخال معطيات مزيف بحيث تعتقد BARC أنه كان يستقبل اتصالاً من جهاز صديق. بعدها، وعن طريق القوة العضلية المحصنة، شرع جهاز فك الشيفرة في تحليل كل مجموعة من مجموعات الأحرف والأرقام حتى نجح في مهمته.

بادئ ذي بدء، انطلق البرنامج عبر كافة المجموعات المدونة بأحرف بسرعة الضوء الرقمي ـ 22، bb، aa، ط، a ـ وبعدها، ad، ac، ab، وهكذا كان تيك ـ ناين tek-9 قد أضاف أيضاً قوائم كلمات خاصة معدَّلة وفق الطلب تحتوي على أحرف وكلمات كان قد أدخلها في البرنامج خلال دورة أسفاره. بعد 45 دقيقة من بدء العمل، دهش تيك ـ ناين عندما تبين بأنه قد نجح في اختراق إحدىٰ كلمات السر. لقد وجد نفسه داخل شبكة الأبحاث الذرية الأولىٰ في الهند. جحظت عيناه من الدهشة. أخذ يدقق في كلمة السر: ANSI اسم لأحد الأشخاص، أخذ

يفكر، إنها إشارة التفعيل prompt بالذات التي تحض على ضرورة إدخال معطيات جديدة. لم يصدق ما جرىٰ. لم يعتمد الفتى على القواعد التقليدية في اختيار كلمات السر والتي كانت بمثابة سلاسل معقدة من الأرقام والحروف التي يصعب اختراقها نظراً للوقت الطويل الذي يستغرقه ذلك والمجازفة الكبيرة المنطوية على احتمال أن يُكشف أمره.

الخطوة الأولى التي قام بها تيك ـ ناين كانت تحميل كافة كلمات السر وأسماء معطيات التشغيل. بعدها، قام بإنشاء مخرج خلفي يؤمن له مدخلاً إلى النظام دون أن ينكشف أمره.

بعدها، قام باستشارة خارطة الشبكة التي كانت مفتوحة أمام الاستخدام العام. اتجه نحو وحدة تخديم الموقع وأخذ يحدق في رسائل البريد الإلكتروني المدونة في الجيك ـ سبيك Geek - Speak العلمي ـ بعدها، أخذ يتصفح بعض الوثائق المتعلقة بفيزياء الجزيئات. مادة مضجرة، فكر قائلاً. قرر الخروج من الموقع طالما أن الظروف مواتية لذلك، بعد أن قام بإنزال عدد من رسائل البريد الإلكتروني ووثيقة علمية للاحتفاظ بها كتذكار. بعد ذلك، وبعد أن قام بإلغاء معطيات دخول البرنامج لضمان عدم تعقبه من قبل أحد، خرج من البرنامج.

لو أبقىٰ ذلك لنفسه، لما كان عرف بأمره أحد، ولما كانت كبرى منشآت الأبحاث النووية في الهند قد عانت، خلال الأيام التي تلت، من وصمة العار التي نجمت عن توغل حوالي مائة ممن يعيثون فساداً عبر شبكاتها وكأنهم عصابة في حالة من الهرج والمرج. لكن تيك ـ ناين لم يتمكن من الحفاظ على صمته. لقد قام بما يمكن أن يقوم به أي قرصان كومبيوتر معتدّ بنفسه. أخذ يتحدث عن إنجازه بتفاخر ومباهاة. قام

بالكشف عن ملف كلمات السر بكامله لمركز بارك، ـ كلمات السر الـ800 بكاملها والأسماء المدخلة في معطيات البيانات ـ على إحدى قنوات هؤلاء القراصنة. على الفور، بدأ قراصنة الكومبيوتر بالوصول إلى هذه المعلومات ومهاجمة مركز بهابها. في غضون أيام، كان هناك أشخاص من كافة أنحاء العالم يصولون ويجولون عبر أنظمة الكومبيوتر لمركز أبحاث بهابها، يحذفون ملفات وينسخون رسائل بريد إلكتروني، ومن ضمنها ملف يتساءل عن شرعية أحد التفجيرات، مزيلين الموقع من على الشبكة ومستبدلينه بسحابة من الدخان الذري وتحيات ساخرة. لو أن تيك ـ ناين كان سائحاً أو جاسوساً تجارياً، وليس ولداً صغيراً وجد بحوث الفيزياء عسيرة ومضجرة، من يدري ما الذي كان يمكن أن يقوم بنقله إلى برنامجه. حتى هذه النقطة، فإن الشركات التجارية أظهرت قدراً من الإبداع أقل مما أظهره تيك ـ ناين، على الرغم من كونها قد بدأت بمراقبة وتتبع حركات منافسيها على شبكة الأنترنت: «نحن نعرف أن منافسينا يتعقبون موقعنا على الشبكة لأننا نتعقب مواقعهم». يقول مايكل ريندا، أحد مدراء مشاريع الانترنت في شركة آلايد سيجنال Allied Signal، «وبالطبع نحن نرد عليهم بالمثل». لقد جعلت الشبكة من تعقب معطيات إحدى الشركات المنافسة أمراً يسيراً جداً: أسعارها، قوائم زبائنها، موردوها، موزعوها ومعلومات حول منتجاتها الجديدة، لأن الشركات عالقة بين مهمتين متناقضتين: تزويد الزبون والشريك بالمعلومات المتوفرة على الانترنت، وفي نفس الوقت، حماية معلوماتها الخاصة.

بوسع شركة ديبون Dupont أن تؤمن على موقعها الخاص لأي شخص يملك جهاز كومبيوتر ومودم Modem قائمة بكل مصنع ومنشأة

غزل تستخدمها الشركة في إنتاج نسيج كول ماكس Cool Max، الذي يستخدم في الألبسة الرياضية. «إنهم يدرجون أسماء المصانع ومنشآت الغزل والنسيج وعناوينها وأسماء مدرائها»، تقول ماري آلين بايتس من قسم بايتس لخدمات المعلوماتية في واشنطن دي. سي. «بإمكانك الاتصال بالموردين ـ هل يدفعون لك ما فيه الكفاية، مطالبين إياك بإنتاج أقمشة جديدة، ومهددين إياك بنقل عملياتهم إلى شانغهاي؟ إذا أردت تصنيع منتج منافس، فأنت تحاول التقرب من مدراء المصنع عن طريق التحدث إليهم عن أمور عامة. لا أدري ما جدوى الكشف عن مثل هذه المعلومات بالنسبة لديبون».

الشائعات المتوافرة على الشبكة هي حول قراصنة كومبيوتر يتم التعاقد معهم من قبل الشركات التجارية لسرقة معلومات خاصة أو أموال، لكن الحالات التي تخرج إلى دائرة الضوء هي حالات نادرة. تتعرض الشركات لمثل هذه الانتهاكات لمواقعها على الانترنت بطرق أخرى على أية حال. حتى وقت قريب، كانت الشركات تحتفظ بملفات كاملة للموظفين وسلسلة تقاريرهم المباشرة على مواقعهم على الشبكة، إلى جانب النشرات التعريفية بتاريخ الشركة وخلاصات نشاطاتها. بوينغ، في موقعها على الشبكة، قامت بإدراج أسماء موظفيها في جميع الأقسام؛ المئات من العمال، ومن ضمنهم أولئك الذين كانوا يعملون في مجال التكنولوجيا المستخدمة في مكوك الفضاء. موقع الشركة الفضائي على شبكة الانترنت كان يعد بمثابة منجم ذهب للشركة المنافسة الراغبة في استدراج تلك الكوادر التي تحمل في جعبتها الكثير من المعلومات الحساسة والتعاقد معها»، يقول روبرت دي. آروف من شركة أبحاث

آرون/ سميث أسوشييتس Aaron/Smith Associates في أتلانتا. «وأنت تعرف إلى من تتحدث بالنسبة لكل شخص. بوسعك الاتصال برئيسهم وشق طريقك عبر المخطط التنظيمي للمؤسسة والاطلاع على المعلومات حول أحد المدراء، سيرته الذاتية وكيفية التعامل معه». عادت بوينغ إلى رشدها وسحبت هذه المعلومات.

بالنسبة إلى قرصان كومبيوتر مثل تشاميليون، فإن الوصول إلى مواقع المعلومات الحصينة يتطلب قدراً أكبر من الموهبة والبراعة. قبل أن يتخلص مايفرت من إدمانه الحاد على القرصنة التي تهدف إلى الخروج بمقدار وفير من المعلومات المسروقة من مواقع الانترنت، كان يمضي معظم أوقاته مقفلاً الباب على نفسه داخل غرفته في منزله الكائن في إحدى ضواحي جنوب كاليفورنيا والذي يعيش فيه مع والدته وشقيقته، ملازماً جهاز الكومبيوتر على مدى 36 ساعة متواصلة من النشاط المحموم، سابراً أغوار الشبكات للاطلاع على آخر الأساليب والتقنيات ووحدات خدمة الانترنت وبرمجياتها وتقنياتها وأساليب التشفير وفك التشفير والتحادث مع الفتيات من خلال البريد الالكتروني والرسائل الفورية، ومن ضمنها إحدى العلاقات الخيالية التي يقول بأنها آلت إلى نهاية كارثية، والتحليل الدقيق للأعداد السابقة من مجلة فراك Phrack، المتعلقة بقرصنة الكومبيوتر.

لم يكن لينسحب من عالمه الخيالي هذا إلا عندما كان يغالبه النعاس إلى درجة لا يعود معها قادراً على فتح عينيه. كان ينسحب زاحفاً فوق السجادة نحو إحدى زوايا الغرفة ثم يتكور على نفسه فوق غطاء سميك على أرض الغرفة عله يفوز بسنةٍ من النوم. «كنت أفضل النوم على أرضية

الغرفة لأنني نادراً ما كنت أخلد إلى نوم حقيقي»، يستذكر مايفريت قائلاً: «المدرسة كانت خارج نطاق اهتماماتي». لقد انقطع عن الحضور. اليوم المقسم إلى 24 ساعة فقد معناه بالنسبة له. حياته باتت مقسمة إلى قسمين لا ثالث لهما: الانترنت والنوم.

لم يكن تشاميليون معروفاً بمهاراته الفنية وتقدير الناس له كأحد «الرواد» أو بحسب المعجم الرقمي للانترنت، قرصان كومبيوتر من مرتبة 3l33t وحسب، بل كان ينظر إلى نفسه أيضاً على أنه أحد شعراء القرن الحادي والعشرين الالكترونيين وناشطيه السياسيين. عندما قام باختراق أحد مواقع الانترنت التابعة لوزارة الدفاع الأمريكية المخصص للذكاء الصناعي، كتب قائلاً: إنه لأمر مضحك أن ينطلق الناس في حياتهم باحثين عن الحقيقة، ومع ذلك، فعندما يجدونها يتمنون لو أنهم لم يبحثوا عنها. الحقيقة هي ڤيروس والناس لا يريدون أن يصابوا به. عش وتعامل مع الحقيقة، لأنك لا بد مواجهها عاجلاً أم آجلاً». على سبيل الدعاية، سرب تشاميليون معلومة برمجية تعبر عن هذه الفكرة النقدية لملفات مجهولة X-Files في كل مرة يحاول فيها أحدهم الدخول إلى الصفحة.

ابتسم له الحظ للمرة الأولى عندما كان في السابعة عشرة من عمره، ومن سخريات القدر أنها جاءت لقاء شيء لم يفعله. في ذلك الوقت، كان تشاميليون يعمل مع عصابة من قراصنة الكومبيوتر تدعى «نويد» Noid، كان قد اخترق معها العشرات من الشبكات التجارية متربصاً بشبكات الكومبيوتر بهدف سرقة معلوماتها، وعابثاً عبر وحدات التخريم والملفات للاطلاع على كيفية عمل الأشياء، يقول مايفرت: الخبر المدوي على صعيد أمن الكومبيوتر كان يدور آنذاك حول مجموعة من قراصنة

الكومبيوتر تدعىٰ «أساطين تحميل الملفات» Masters of downloading Files قامت بسرقة جزء من برنامج عسكري يدعى DEM أو مدير معدات الشبكات لأنظمة معلومات الدفاع. وكالة أنباء سي. بي. إس. CBS سعت للتحدث إلى أساطين تحميل الملفات MOD، ولكن نظراً لكون أعضائها متمركزين في أوروبا، فقد أشاروا على سي. بي. إس. بالتحدث إلى تشاميليون. بما أنه لم يكن راغباً في أداء هذا الدور لوحده، فقد تمكن تشاميليون من إقناع زميله في الغرفة «أحد قراصنة التنصت على المكالمات» ممن يقومون بالتلاعب بالنظام الهاتفي للحصول على ما يريدون ـ ثم توجها معاً إلى الاستديو. بهدف التمويه على شخصيتيهما، عمدا إلى إخفاء ملامح وجهيهما وتعديل نبرة صوتيهما. لكن تشاميليون لم يكن لديه أدنىٰ نية في البوح بأي شيء صحيح قد يتسبب بإدانتهما عن بعد. وهكذا أخذ يكذب. «لم أزعم أبداً أنني سرقت البرمجيات؛ قلت إن مجموعة أساطين تحميل الملفات MOD هم من قام بذلك، لأن هذه هي الحقيقة. لكنني قلت إنني كنت عضواً في هذه المجموعة. رجل، ثم رجل، يا لها من كذبة حمقاء!»

بعد وقت قصير، تلقى تشاميليون الإشارة بورود اتصال مباشر له على الشبكة. أحدهم ويدعى إبراهيم قال له إنه يريد البرنامج. ظل يلاطف تشاميليون ويتودد إليه محاولاً إقناعه بأنه سيدفع له مبلغاً محترماً من المال لقاء ذلك. «في البداية اعتقدت بأنه أحد العابثين الراغبين في إزعاجي، وهو أمر يحدث دائماً على الـ آي. آر. سي. IRC،» يقول تشاميليون. «سايرته في ما يرمي إليه، رغم اعتقادي بأنه كان أمراً تافهاً. ولكن فيما بعد طلب مني التدقيق في أحد صناديق البريد» على مسافة

ثلاث بلدات من المكان الذي كان تشاميليون يعيش فيه في آيرفين، كاليفورنيا.

عندما وصل إلى هناك، حدق داخل الصندوق. الرسالة الوحيدة التي كانت موجودة هناك كانت عبارة عن تبليغ بوجوب ترك العمل Pink slip. رسالة مصدقة. هذا يعني بأنه كان ملزماً بالتوقيع عليها إشعاراً منه بالاستلام. وهذا يعني أيضاً أنه إذا كان صاحبنا أحد رجال التحري السريين، فإن تشاميليون سيقع في ورطة كبيرة. كان هو ورفاقه في عصابة نويد في غاية الانشغال مؤخراً، كونهم قد شوهوا عدداً كبيراً من مواقع الانترنت خلال الأسابيع الأخيرة. «لقد انهمكنا في فورة من الاختراقات لعشر أو اثني عشر موقعاً، من ضمنها مواقع للجيش والقوى البحرية والقوى الجوية. «اللعنة، لقد دهمنا موقعاً لكل صنف من صنوف أسلحة الجيش الثلاثة»، يقول تشاميليون. لكنه كان يدرك أيضاً أن علاقاته مع إبراهيم كانت علاقات شرعية مئة بالمئة، من جانبه على الأقل. «حتى لو كان أحد أعضاء مكتب التحقيقات، لم أكن لأعطيه برامج أو أي شيء»، يقول تشاميليون.

وهكذا قام بفتح الصندوق، أمسك بالتبليغ، توجه نحو الكونتوار ووافق على تلقي حوالات بريدية بقيمة 500 دولار. كان مدوناً على الظرف رقم الصفحة لأحد العملاء في شيكاغو. مزق تشاميليون المغلف وألقى به في سلة المهملات.

حسن، قد يكون الشخص سائحاً، فكر تشاميليون قائلاً، أو لعله عضو في مكتب التحقيقات. مهما يكن، فقد قام بتعبئة الحوالات البريدية وصرفها من أحد المصارف في نهاية الشارع، «لن أقوم بخداع أحد

مطلقاً، ولكني لم أجد غضاضة في القيام بذلك مع أحد السياح. إضافة لذلك، فقد كان ذلك المبلغ يمثل ثروة بالنسبة لي آنذاك»، يقول تشاميليون. لقد أخذ القسط الأكبر من غنيمته واشترى لعبة نينتاندو 64 لشقيقته المتخلفة عقلياً، حيث إن الأطباء قالوا لي «إن أي لعبة ستكون مفيدة لها». استخدم باقي الغنيمة للتجول بسيارته في أنحاء المدينة وركوب الطائرة إلى سان خوسيه لزيارة صديق. في هذه الأثناء، ثابر إبراهيم على محاولاته الاتصال به على الـ آي. آر. سي. IRc، نظراً لكون الرسائل باتت أكثر تهديداً. «أعطيتك مالاً، فماذا تريد أكثر من ذلك؟ لا أريد أن أكون مرغماً على العودة إلى جماعتي لإخبارهم بأنك قد سرقتنا»، كتب إبراهيم قائلاً.

تحت وطأة الخوف، توقف تشاميليون عن مغامراته على الشبكة. لكن هذا لم يمنعه من الاستيقاظ بشكل مفاجئ وفوهة مسدس تدغدغ صدغه.

الخـاتمة

يسرنا أن نفيد بأن إبراهيم وعصابة من الأشرار لم يكونوا من داهم منزل مايفريت وسبّب الذعر لشقيقته وفاجأ والدته في الحمام وأيقظه تحت تهديد المسدس.

لقد كان مكتب التحقيقات الفيدرالي.

قام عناصر مكتب التحقيقات بمصادرة معدات كومبيوتر مايفريت التي تساوي نحو 3,000 دولار «لم يرجعوها لي مطلقاً ولم أتهم بأي جريمة»، يقول مايفريت. وهو يعتقد أنهم كانوا عاكفين على مراقبته لعدة أشهر، «يتحرون عن الأشخاص الذين كان على اتصال بهم على شبكة الانترنت»، ولكنه غير واثق في ما إذا كانت نشاطاته مع نويد أو ابراهيم هي ما جذب انتباههم. بعد بضعة أسابيع من هذه المداهمة، استعار مايفرت جهاز كومبيوتر صغيراً Lap top من أحد الأصدقاء.

لأشهر تلت، حاول إبراهيم إقامة الاتصال من جديد. لكن مايفريت أخذ عهداً على نفسه ألا يتحدث إليه مطلقاً بعد الآن.

مايفرت، على غرار العديد من أقرانه الأمريكيين من المراهقين، لم يكن ليأخذ إبراهيم على محمل الجد، وهو يهزأ بالسلطة.

إنه شخص عنيد. هو يقوم باستنتاجاته الخاصة. لا يحب أن يُملي عليه أحد ما ينبغي أن يقوم به. إنها الصفات التي تجعل منه قرصان كومبيوتر من الطراز الرفيع، وتجعل منه أيضاً جاسوساً تجارياً يتسم نشاطه بدرجةٍ عاليةٍ من المُخاطرة، يقول مايفرت، الذي تشهد شركته الأمنية الصغيرة، eEye فترة من الازدهار:

أخبرني تيك ناين أول قرصان كومبيوتر تمكن من اختراق مركز الأبحاث النووية الهندي، إنه لا يستطيع انتظار اليوم الذي ستدفع له الشركة فيه 100,000 دولار لاختراق شبكات أخرى. ولكن هل يمكن الوثوق بأنه لن يقوم بإفشاء أسرار إنجازاته على سبيل المفاخرة والمباهاة؟

كريم فاضل، جاسوس المعارض التجارية الذي شعر بعقدة الذنب حيال ما فعله، ترك شركة بيكتشرتل، واستغل، كما فعل مايفرت، الطفرة التي شهدتها تقنية الانترنت خير استغلال، قبل منصباً في مجال الاستخبارات التجارية مع شركة تقع على الطريق الدائري المحيط بواشنطن دي. سي. ويقول إنه لا يستبعد تطبيق الأساليب التي تعلمها في بيكتشر تل.

جان هيرنغ، نجم السي. آي. إيه. السابق الذي أسس أول وحدة تجسس تجارية في موتورولا، لا يزال مستمراً في تقديم خدماته

الاستشارية وتقنيات جمع المعلومات من المصادر المفتوحة. إنه متحدث دائم في المؤتمرات التي ترعاها هيئة أخصائيي الاستخبارات التجارية SCIP، المنظمة التي شكلها لنشر التعاليم الاستخبارية لجيله التجاري.

ليز لايتفوت تركت شركة تيلتك Teltech لتتسلم عملاً كمديرة أبحاث لمعهد غارتنر Gartner Institute، منشأة في مينيا بوليس متخصصة بإنتاج برامج شهادات Certification programs لتحسين الوثائق وشهادات الكادر التجاري الفني.

إيد أو مالي، عميل مكتب التحقيقات السابق الذي قام بتحذير وكالة الاستخبارات المركزية الفرنسية DGSE من قانون الجاسوسية الاقتصادية، يدير مركزاً خاصاً به للاستخبارات التجارية.

ما الذي أصاب بطل السي. آي. أيه. المغامر ديوي كلاريدج؟

قام بنقل مهاراته وخبراته إلى القطاع الخاص بعد استقالته من الوكالة. إنه الآن تاجر سلاح تخصصُه: صواريخ.

آڤيري دنيسون كانت ساخطة على ڤيكتور لي لإخلاله بشروط الاتفاق التي كانت تقضي بأن لا يشهد بأي حال من الأحوال ضد الشركة، ولكن عندما اعترف لي على منصة الشهود بأنه كان قد أزال علامات السرية عن الوثائق التي أرسلها إلى تايوان، أسهم في تقويض دعوى الحكومة. مصيره تحدد خلال المرحلة الاستكشافية للمحاكمة المدنية التي كانت أڤيري ماضيةً فيها ضد فور بيلارز. تلك كانت هي الثغرة التي عرف المحامون عندها بأن لي كان قد رفض تسليم الورقتين الأخيرتين من رسالة من ست صفحات إلى يانغ، وكان قد صاغ رسالة أخرى: «شراء الكتب

أمرٌ يسير»، كان قد كتب قائلاً: «ولكنَّ الحصول على سر أو وثيقةٍ سرية، أمرٌ أكثر صعوبة».

عقوبته: ستة أشهر في مركزٍ للتأهيل وتحت الإقامة الجبرية.

والأمر الذي فاقم من العار الذي لحق به أنه سيتكفل بنفقاته (كلفة سوار الكاحل الالكتروني كانت 4,35 دولاراً في اليوم). الأسوأ من ذلك، أن آڤيري عيَّنته شريكاً في الدفاع في حكم الـ40 مليون دولار الذي ربحته ضد فوربيلارز، الشيء الذي حاول تجنبه (إضافة إلى السجن) منذ البداية.

«آمل أن يكون لي يتصبب عرقاً». يقول زويلينغر.

«لقد نال جزاء ما اقترفت يداه».

بعد الحكم، عادت سالي يانغ أدراجها إلى تايوان لتلحق بزوجها. بي، واي، يانغ عاد إلى غرفته في كليڤلاند ليقضي بقية عقوبته وحيداً. بالإجمال، فقد أمضى سنتين تحت الإقامة الجبرية في أمريكا، بينما قامت آڤيري بالإجهاز على شركته في الصين. الحكم المدني كان بمثابة حركة درامية مثيرة بعد التصويت بالإدانة في المحاكمة الجنائية. الأمر الذي تمخض عن حكم بـ40 مليون دولار ضد آل يانغ ولي وفوربيلارز إنتربرايزز. في هذه الأثناء، كانت كلا القضيتين قيد الاستئناف.

بعض خبراء القانون يعتقدون بأن هنالك فرصة جيدة لاستئناف الحكم الجنائي.

مارك زويلننغر ترك وزارة العدل وانتقل للقطاع الخاص. هو الآن يعمل مع شركة كيركلاند وإيليس، رئيساً لقسم جرائم الانترنت.

نانسي لوك وإيريك دوبلبير ما زالا يدفعان الأمور قدماً بشأن عملية

طلبات الاستئناف ليانغ وابنته. وهما أيضاً مكلفان بعدد هائل من قضايا الياقة البيضاء.

مارك باري منهمك في مشروع مشترك مع رايثيون، مُنشئاً غرفة عمليات بكلفة 7 ملايين دولار ومديراً لأجهزة استخبارية لشركته سي ثري آي أناليتكس في نيويورك. سوف يحبذ إهداء هذا الكتاب لعمته شيرلي وعمه برايان باري، الذي حاول خلال طفولته تعليمه أن أحداً لا يحب الإنسان النَّمام... بعد فوات الأوان. أحمد الله أنني لم أُصغ إليكم أيها الناس.

آدم إل. بينينبرغ يحبذ إهداء هذا الكتاب مع كل الحب لوالده، الذي رحل عن هذه الدنيا خلال مرحلة الكتابة، وإلى والدته العاكفة بلا شك على تحديث موقعها على شبكة الانترنت.

آدم ال. بينينبرغ ومارك باري

مدينة نيويورك أيار 2000