وثائق سنودن: وكالة الأمن القومي تحضّر أمريكا لحرب المستقبل

كتبه نون بوست | 19 يناير, 2015

ترجمة وتحرير نون بوست

الكتّاب: جاكوب أبلبوم – آرون غيبسون – كلاوديو غوارنييري – اندي ميلر ماكوهن – لاورا بواترس – مارسيل روزنباخ – ليف ريج – هيلمار شمندت – مايكل سنوثيمر

عادة ما يحتاج المتقدمون لأي عمل إلى سيرة ذاتية لامعة حتى يتم قبولهم، كما أن الخبرة في العمل التطوعي بالمشاريع الاجتماعية في حال إضافتها للسيرة الذاتية ستشكّل عاملاً إيجابيًا للقبول، أما بالنسبة لبرنامج بوليتريان (Politerain) فالوظيفة تتطلب مجموعة مهارات مختلفة تمامًا، ولسان حال إعلانات الوظيفة لهذا العمل تقول "نحن نبحث عن متدربين جاهزين لتحطيم العالم".

برنامج (Politerain) هو مشروع يتم تشغيله من قبل الاستخبارات الأمريكية، ووكالة الأمن القومي (NSA)، وبشكل أكثر تحديدًا، فإن المسؤول عن هذا البرنامج هم مجموعة القناصين الإلكترونيين ومكتب تصميم عمليات الوصول (TAO) التابعين لوكالة الأمن القومي.

يجري تحضير المتدربين المحتملين في برنامج (Politerain) عن طريق إقناعهم أن الأبحاث التي

ستجري على أجهزة الكمبيوتر التابعة لطرف ثالث، يمكن أن تؤدي إلى تخريب أو تدمير جهاز الخصم، ويدرك المتدربون المحتملون بأن الهجوم على أجهزة الخصوم قد يؤدي إلى تعطيل أجهزة البث والاستقبال والخوادم وأجهزة تمكين الشبكة الخاصة بالخصم، وكل هذا يتم باستخدام برنامج يسمى باشنيت بولكا (Passionatepolka)؛ فعلى سبيل المثال، قد يُطلب من المتدرب "إيقاف تعريفات الشبكة عن بعد" باستخدام برامج مثل بيرسركر (Berserkr) التي تعمل على زرع برامج تفتح طرق ثانوية وبرامج تشغيل متطفلة، كما قد يشمل الولوج إلى جهاز الخصم استخدام برمجية أخرى تدعى بارن فاير (Barnfire)، والتي تعمل على محو نظام الإدخال والإخراج الأساسي (BIOS) من مجموعة الخوادم (السيرفرات) التي تستخدمها الحكومات بشكل أساسي ضمن منظوماتها المعلوماتية، كما يمكن أن يُسند لمتدربي برنامج (Politerain) مهمة تدمير الأقراص الصلبة لجهاز الخصم عن بعد، وفي نهاية المطاف، فإن الهدف من برنامج التدريب الداخلي هو "تطوير العقلية الهجومية" لدى المتدرب.

تم فتح برنامج التدريب منذ ثماني سنوات، ومنذ ذلك الحين أصبحت عقيدة جميع جواسيس وكالة الأمن القومي تتضمن العقلية الهجومية، كما أصبح توجّه جهاز المخابرات المركزي لا يقتصر فقط على المراقبة الجماعية لاتصالات الإنترنت، بل أصبح تحالف العيون الخمسة – وهو تحالف استخباراتي مؤلف من الولايات المتحدة وبريطانيا وكندا واستراليا ونيوزيلندا – يمتلك جواسيسًا إلكترونيين يسعون لتحقيق المزيد من الانتصارات الرقمية.

ولادة الأسلحة الرقمية (D.Weapons):

وفقًا للوثائق السرية المسرّبة من أرشيف وكالة الأمن القومي عن طريق إدوارد سنودن والتي تحصلت عليها شبيغل بشكل حصري، يتبين أن الأجهزة الاستخباراتية الأمريكية تخطط لحروب مستقبلية تلعب فيها شبكة الإنترنت دورًا حاسمًا، حيث تهدف الخطة إلى استخدام الشبكة لشلّ شبكات الكمبيوتر؛ مما سيؤدي إلى السيطرة على البنية التحتية للدولة، وهذا يشمل السيطرة على الطاقة وإمدادات المياه والمصانع والمطارات وتدفق الأموال.

خلال القرن العشرين، طوّر العلماء ما يسمى بأسلحة ال. (ABC) – اختصارًا للأسلحة الذرية والبيولوجية والكيميائية -، وإن تنظيم انتشار واستخدام هذه السلحة استغرق عقودًا، وعلى الرغم من مرور فترة زمنية طويلة على اختراع هذه الأسلحة وتنظيمها إلا أنها لاتزال تعتبر منظمة بشكل جزئي؛ أما الآن فقد تم تطوير أسلحة رقمية جديدة لاستخدامها في حروب المستقبل (الحرب على الإنترنت)، وحاليًا لا يوجد أي اتفاقيات دولية أو سلطات رقابية تنظّم انتشار واستخدام هذه الأسلحة الرقمية، والقانون الوحيد الذي ينطبق حاليًا هو قانون البقاء للأقوى.

منذ عقود وفي عام 1970 توقع المنظّر الإعلامي الكندي مارشال ماكلوهان حصول هذه التطورات، حين أشار إلى إن الحرب العالمية الثالثة هي حرب عصابات المعلومات التي تتميز بعدم التفريق بين الأهداف العسكرية والمدنية، وماكلوهان أصاب كبد الحقيقة في هذا التعبير، كون جواسيس اليوم يستعدون لهذه المعركة؛ فالجيش الأمريكي والبحرية ومشاة البحرية والقوات الجوية بادرت إلى إنشاء قوات إلكترونية خاصة بها، ولكن المسؤول الرسمي الأمريكي عن القوات الإلكترونية والمسؤول

عن اتخاذ زمام المبادرة هي وكالة الأمن القومي (NSA)، وليس من قبيل الصدفة أن يكون مايكل روجرز مدير وكالة الأمن القومي يشغل بذات الوقت منصب رئيس القيادة الإلكترونية في الولايات المتحدة، حيث يعتبر الأخير كبير المحاربين الرقميين، ويترأس مجموعة مكونة من 40.000 موظف جميعهم ذوو خبرة في التجسس الرقمي وهجمات الشبكة الرقمية المدمرة.

نظم المراقبة تمثّل المرحلة الأولى فقط:

من وجهة النظر العسكرية، فإن نظم مراقبة الإنترنت هي المرحلة الأولى والابتدائية في إستراتيجية الحرب الرقمية للولايات المتحدة، حيث تُظهر الوثائق الداخلية التي تم تسريبها من وكالة الأمن القومي أن نظم المراقبة هي القاعدة الأساسية والابتدائية للهجمات الإلكترونية، وتُظهِر الوثائق أيضًا أن الهدف من نظم المراقبة هو الكشف عن نقاط الضعف في أنظمة العدو، وزرع برامج متخفية في أنظمته تساعد على اختراقها، وهذا يحقق للوكالة نوعًا من الوصول المستمر للأنظمة الإلكترونية؛ مما يساعد على تحقيق المرحلة الثالثة من الحرب والتي سُميت في الوثائق المسربة بمرحلة الهيمنة (Dominate)، وهذه المرحلة تتيح للوكالة السيطرة على النظم الحيوية والشبكات أو تدميرها عند الحاجة، وذلك اعتمادًا على البرامج المتخفية التي تحقق الوصول المستمر التي تم وضعها في المرحلة الأولى؛ علمًا بأن الوثائق تشير إلى أن وكالة الأمن القومي تنظر إلى البنية التحتية الحيوية على أنها أي منظومة تساعد على الحفاظ على تراتبية المجتمع، مثل الطاقة والاتصالات والنقل، وعلاوة على ذلك تنص الوثائق الداخلية على أن الهدف النهائي هو القدرة على ممارسة التصعيد المبرمج الفوري للحرب الإلكترونية.

وتشير إحدى الوثائق المسرّبة أيضًا بأن الصراع الرئيسي التالي سيبدأ في الفضاء الإلكتروني، واستعدادًا لهذه المرحلة، تبذل الحكومة الأمريكية حاليًا جهودًا هائلة لتسليح نفسها رقميًا لمواجهة حرب الشبكات الإلكترونية، حيث إن ميزانية الاستخبارات السرية لعام 2013، أشارت أن وكالة الأمن القومي طلبت مبلغ مليار دولار من أجل زيادة قوة عملياتها الهجومية على الشبكات الإلكترونية، ويتضمن هذا المبلغ بندًا بقيمة 32 مليون دولارًا لتطوير"حلول غير تقليدية" لمواجهة الحرب الإلكترونية القادمة.

يعزو الخبراء ظهور البرمجيات الضارة في السنوات الأخيرة لأعمال وكالة الأمن القومي وتحالف العيون الخمسة، وذلك بناء على عدة مؤشرات، وتشمل البرمجيات الضارة برامج مثل ستكسنت (Stuxnet) الذي تم استعماله لمهاجمة البرنامج النووي الإيراني، وبرنامج ريجن (Regin)، وهو أحد برامج التجسس التي تستعمل تقنية حصان طروادة، والذي خلق ضجة في ألمانيا بعد أن أصاب وحدة التخزين الخارجية (USB Stick) العائدة لموظف رفيع المستوى للمستشارة الألمانية أنجيلا ميركل، كما اُستخدِم هذا البرنامج في الهجمات الإلكترونية التي أطلقها جواسيس وكالة الأمن القومي ضد المفوضية الأوروبية والمكتب التنفيذي للاتحاد الأوروبي، وشركة الاتصالات البلجيكية بلجاكوم في عام 2011.

إن الجواسيس الأمريكيين قادرين بشكل روتيني على اختراق أمن أي برنامج، وجميع مستخدمي الإنترنت معرضون لخطر هجوم البيانات الذي يمارسه هؤلاء الجواسيس، وتُسلّط الوثائق الجديدة

الضوء من جديد على كشوفات أخرى أيضًا، فالهجوم الالكتروني الذي تمت تسميته كوانتم إنسيرت (Quantuminsert) والذي شغل الأوساط الإلكترونية لفترة زمنية طويلة، تم اعتباره على أنه هجوم ذو نسبة نجاح منخفضة حسب ما تُبيّن الوثائق السريّة، وعلى الأرجح تم استبداله ببرنامج آخر يعمل على شن هجمات أكثر موثوقية مثل برنامج كوانتم ديرك (Quantumdirk)، الذي يعمل على إدخال برمجيات ضارة ضمن مواقع خدمات الدردشة مثل الفيسبوك وياهو، كما تُبيّن الوثائق أن أجهزة الكمبيوتر المصابة ببرنامج ستريت بيزار (Straitbizarre) يمكن التحكم بها لتتحول إلى أجهزة قادرة على توزيع ونشر نقاط الاتصال الإلكترونية، ويتم استخدام هذه النقاط لتلقي الرسائل من شبكة الكوانتم التابعة لوكالة الأمن القومي، والتي تُستخدَم للسيطرة والتحكم بالهجمات الإلكترونية التي تجري على نطاق واسع جدًا، كما أشارت الوثائق أن العملاء السريين استطاعوا اختراق الهواتف النقالة من خلال استغلال نقطة ضعف في متصفح سفاري من أجل الحصول على بيانات حساسة وزرع برمجيات خبيثة ضمن هذه الأجهزة.

إن حرب العصابات الإلكترونية لا تفرّق بين الأهداف العسكرية والمدنية، حيث تظهر وثائق سنودن المسرّبة، بأن جميع مستخدمي الإنترنت على مختلف انتماءاتهم يمكن أن يعانوا من أضرار في بياناتهم أو في أجهزتهم، كما أن هذه الحرب يمكن أن تؤثر على الأشخاص الغير متصلين بشبكة الإنترنت العالمية أيضًا؛ فعلى سبيل المثال إذا تم استخدام سلاح بارن فاير (Barnfire) لتدمير أو تخريب مركز التحكم في أحد المستشفيات، فإن الأخطاء البرمجية التي ستنجم، سيتضرر منها جميع الأشخاص حتى الذين لا يمتلكون هواتفًا محمولة، علمًا بأن وكالات الاستخبارات اتبعت سياسة الإنكار كمبدأ عام يحكم سياساتها الإلكترونية، حيث عملت هذه الوكالات على إحاطة الهجمات الإلكترونية بتقنيات متقدمة جدًا، تجعل من المستحيل تقريبًا تقفي أثر منفذي الهجوم.

إن التقنيات التي يمتلكها ويستعملها سلاح الاستخبارات الأمريكي، بالإضافة إلى جيش الجواسيس الذي يجنده، تقوّض عمدًا أسس سيادة القانون في جميع أنحاء العالم، وهذا النهج يهدد بتحويل شبكة الإنترنت إلى منطقة تنعدم فيها سلطة القانون، بحيث تصبح هذه الشبكة وما يرتبط بها من مؤسسات حيوية مرتعًا لاستعراض عضلات القوى العظمى التي تستخدم الخدمات السرية التي تمتلكها وفقًا لأهوائها الخاصة، بدون وجود أي وسيلة محددة لمحاسبتهم على أفعالهم.

إن إيجاد رابطة السببية ما بين برامج التجسس الإلكترونية وبين وكالة الأمن القومي، هو أمر صعب للغاية ويتطلب جهدًا قانونيًا كبيرًا، ولكن الوثائق الجديدة تظهر بعض المؤشرات التي يمكن أن تساعد في إيجاد الرابط؛ فمثلاً تصميم لوحات مفاتيح الكتابة في الكومبيوترات والأجهزة الذكية التي تسمى كويرتي (QUERTY)، كانت جزءًا من أرشيف سنودن المسرّب حيث تم تصنيفها على أنها برامج تسجيل معلومات (keylogger)، وتعمل هذه التصاميم على تسجيل كل الحركات التي يقوم بها الضحية خلسة، بهدف إخضاعها للتفتيش والتدقيق في وقت لاحق، وعلى الرغم من أن هذه البرامج والتصميمات لا توحي بأنها تشكّل أي خطر حاد وحقيقي، إلا أن الشيفرة الأساسية الواردة ضمن هذه البرامج تكشف بعض التفاصيل المثيرة للاهتمام، كونها توحي بأن برامج تسجيل المعلومات مثل ال(keylogger) يمكن أن تكون جزءًا من ترسانة كبيرة من البرمجيات التي تنتمي إلى برنامج فخر المحارب أو (Warriorpride)، وهو برنامج يصنّف ضمن فئة تشفير اللغات (برامج

الاسبرانتو) ويتم استخدامه من قبل جميع الوكالات الشريكة في تحالف العيون الخمسة، وكان مخصصًا بشكل أساسي لاختراق أجهزة الآيفون، والوثائق المسرّبة عن وكالة الأمن القومي تشمل عينات من التعليمات البرمجية لبرامج تسجيل المعلومات (keylogger)، والتي يمكن أن تساعد على إنشاء دفاعات مناسبة ضد هذا النوع من البرامج.

البداية كانت بمجموعة قراصنة (Hackers):

تشير الوثائق المسرّبة أن قسم مركز العمليات عن بعد (ROC)، والذين تتم الإشارة له برمز (S321)، يقع في مقر وكالة الأمن القومي في فورت ميد بولاية ماريلاند، في الطابق الثالث من أحد المباني الرئيسية في حرم وكالة الأمن القومي، والفريق العامل ضمن المركز يُعد حاليًا أهم فريق بالنسبة للوكالة، وهو الفريق المسؤول عن العمليات السرية، وتضيف الوثائق لأن بداية قسم (ROC) كان بمجموعة من قراصنة الإنترنت غير المهنيين، أما حاليًا فإن إجراءات التعيين في المركز أصبحت أكثر منهجية، كما تم الكشف عن أن شعار مركز (ROC) هو "بياناتك الخاصة هي بياناتنا، ومعداتك الخاصة هي معداتنا"، المركز يتضمن عملاء يعملون من خلال الجلوس الدائم أمام شاشات حواسيبهم، ونظام العمل داخل المركز تناوبي ليغطي كامل اليوم طيلة أيام الأسبوع.

كما توضح الوثائق أن هدف وكالة الأمن القومي بالهيمنة على الشبكة العالمية يتضح بشكل خاص من خلال عمل قسم (S31177)، والذي يسمى باسم (فريق التجاوز)، ومهمة هذا القسم تتمثل باقتفاء أثر الهجمات الإلكترونية الأجنبية، ومراقبتها وتحليلها وفي أفضل الأحوال محاولة نسخ التقنيات التي تستعملها، وهذا النوع من الأقسام التي تعمل على مكافحة الاستخبارات الإلكترونية، يعتبر من أهم أقسام منظومة التجسس الحديثة.

الاعتماد على تقنيات الدول الأخرى:

بالإضافة إلى قيام أرشيف سنودن السري بالكشف عن قدرة الولايات المتحدة الخاصة في تنفيذ الهجمات الإلكترونية، فإنه يكشف أيضًا عن قدرات الدول الأخرى؛ ففريق التجاوز لديه حق الوصول والاستخدام لأرشيف سنوات العمل الميداني الأوّلي الموجود ضمن وكالة الأمن القومي، والذي يتضمن قواعد بيانات عن الهجمات الإلكترونية التي تم تنفيذها من قبل البلدان الأخرى، وتظهر الوثائق أن وكالة الأمن القومي ومعاونيها من تحالف العيون الخمسة، استطاعوا الاستفادة من الهجمات الإلكترونية التي تشنها الدول الأخرى، حيث وظّفت تقنيات هذه الهجمات لاستخدامها الخاص في السنوات الأخيرة، وتشير إحدى الوثائق المسرّبة العائدة لعام 2009 أن اختصاص أقسام الهجمات الإلكترونية هو "اكتشاف وفهم وتقييم الهجمات الأجنبية"، كما تشير وثيقة أخرى إلى أن هذه الأقسام تعمل على سرقة أدوات الهجمات الأجنبية واعتماد التقنيات الحديثة لتحديد الأهداف ومهاجمتها.

في عام 2009، قامت وحدة تابعة لوكالة الأمن القومي باكتشاف اختراق للبيانات لدى عاملي وزارة الدفاع الأمريكية، وقام القسم بتتبع عنوان الآي بي (IP) للمخترقين، وتبيّن أن مركز العمليات يعمل في أسيا، وفي نهاية التحقيقات نجح عملاء وكالة الأمن القومي بتعقب نقطة الهجوم القادمة من الصين، كما استطاعوا سرقة المعلومات الاستخباراتية التي تحتفظ بها الاستخبارات الصينية الناجمة

عن الهجمات الصينية الأخرى، بما في ذلك بيانات سرية تمت سرقتها من الأمم المتحدة، وإن هذا الأسلوب الذي تنتهجه وكالة الأمن القومي الذي يقوم على ترك مهمة الاختراق وجمع البيانات لأجهزة الاستخبارات الأخرى، ومن ثُمّ سرقة هذه البيانات واستغلالها، هو أسلوب تقني متقدم جدًا وله مخاطر جمة؛ فالوكالة تعتبر جميع البلدان التي ليست جزءًا من تحالف العيون الخمسة أهدافًا محتملة لاستخدام هذه التقنية الغير تقليدية.

صعوبة التتبع تعني صعوبة الاستهداف:

تظهر الوثائق أن وكالة الأمن القومي نجحت باكتشاف العديد من حوادث التجسس على البيانات على مدى السنوات الماضية، وكانت معظم هذه الهجمات قادمة من الصين وروسيا، كما أن السياسة التي تنتهجها الوكالة ساعدت مكتب تصميم عمليات الوصول (TAO) على تعقّب عنوان الآي بي (IP) الخاص بخوادم (سيرفرات) التحكم الرئيسية المستخدمة من قبل الصين؛ مما ساعد المكتب على كشف الأشخاص المسؤولين عن هذه الهجمات داخل صفوف جيش التحرير الشعبي، ويشير عملاء وكالة الأمن القومي إلى أن الوصول لهذه المعلومات لم يكن سهلاً على الإطلاق، كون الهجمات الصينية كانت صعبة التتبع كونها تعتمد على سياسية تغيير عناوين الآي بي (IP)، وأن صعوبة التتبع تؤدي إلى صعوبة الاستهداف، ولكن في النهاية، تشير الوثائق بأن التتبع نجح من خلال استغلال ثغرات جهاز التوجيه المركزي.

وتضيف إحدى الوثائق المسرّبة أن الأمور ازدادت صعوبة عندما سعت وكالة الأمن القومي لتحويل التتبع إلى استهداف، كون الاستهداف ألزم العملاء على الخوض في بيانات طويلة ومملة وهائلة الحجم، ولكنهم في النهاية نجحوا باختراق كمبيوتر مسؤول عسكري صيني رفيع المستوى؛ مما أدى إلى حصولهم على معلومات عن الأهداف الصينية في الولايات المتحدة وفي البلدان الأخرى، كما أن العملاء استطاعوا أيضاً الحصول على شيفرة المصدر للبرنامج الصيني الذي عمل على اختراقهم.

إن البيانات السابقة لا تعني بأن جميع عمليات الاختراق ضد الولايات المتحدة كانت فاشلة، كون الوثائق المسربّة تشير أيضًا إلى وقوع عمليات اختراق صينية ناجحة؛ فقبل بضع سنوات قامت وكالة الأمن القومي بتقييم الأضرار الناجمة عن الاختراقات الإلكترونية لحكومة الولايات، وأشارت النتائج بأن وزارة الدفاع الأمريكية وحدها سجلت أكثر من 30.000 حادثة اختراق معروفة، ومن ضمنها تم اختراق أكثر من 1600 جهاز كمبيوتر متصل بشبكة وزارة الدفاع، وتشمل البيانات العسكرية الحساسة التي تم الحصول عليها نتيجة لهذه الاختراقات، جداول التزود بالوقود الجوي، ونظام تخطيط الخدمات اللوجستية العسكرية، وأنظمة ملاحة الصواريخ التابعة لسلاح البحرية، ومعلومات عن الغواصات النووية والدفاع الصاروخي وغيرها من المعلومات السرية لمشاريع الدفاع.

بالطبع فإن الرغبة في الحصول على المعلومات لم تفتن الصين وأمريكا وروسيا وبريطانيا فقط؛ فقبل سنوات، اكتشف عملاء الولايات المتحدة عملية قرصنة كان منشأها في إيران، كما تم اكتشاف موجة مختلفة من الهجمات منشأها في فرنسا.

تحويل الدفاع إلى هجوم:

تعمل وكالة الأمن القومي بالتعاون مع الوكالات الأخرى في تحالف العيون الخمسة، على مراقبة

الهجمات الخارجية التي تستهدف أمن الدول المشتركة بالتحالف، حيث تم تصميم نظام الحراسة (Tutelage) الذي يعمل على تحديد الاختراقات والتأكد من أنها لن تصل إلى أهدافها، وأحد الأمثلة الواردة في وثائق سنودن عن هذا النظام يشير إلى قيام نظام الحراسة (Tutelage) باعتراض البرمجيات الضارة التي تعرف باسم (LOIC) والتي تستخدمها حركة المجهولين (Anonymous) لتعطيل المواقع المستهدفة، حيث كان هذا النظام قادرًا على تتبع عناوين الآي بي التي يتم إجراء الهجوم منها، وعمل بعدها على حجب هذه العناوين لحرمان المعتدين من إجراء الهجوم مرة أخرى.

وفضلاً عن تعطيل الهجوم فإن وكالة الأمن القومي قادرة على تحويل دفاعاتها إلى هجوم، بطريقة تسمى "الهندسة العكسية وإعادة توظيف البرمجيات"، وينطوي هذا النظام على برامج خبيثة تستخدم ملايين الكمبيوترات التابعة للمستخدمين العاديين عبر برامج تم تثبيتها سرًا عليها، وهذه الأجهزة يتم التحكم بها عن بعد واستعمالها كجزء من هجمات "جيش الزومبي" لشل أجهزة الهدف؛ فإذا تبين أن الجهاز الهدف يقع داخل الولايات المتحدة، يتم إرسال المعلومات إلى مكتب التحقيقات الفيدرالي (FBI)، ولكن بالمجمل فإن جميع الأجهزة المصابة بالبرمجيات الخبيثة حول العالم يمكن استغلالها لتنفيذ هجوم معاكس من قبل وكالة الأمن القومي، ويسمى هذا البرنامج في وثائق الوكالة ب.(Defiantwarrior)، وطبعًا فإن هذا البرنامج يهدد أجهزة المستخدمين العاديين، ويجعلها عرضة للاستهداف المعاكس من قبل الهدف، بمعنى آخر، بدلاً من توفير الحماية لمستخدمي الإنترنت المدنيين، تعمل الوكالة على استخدامهم كدروع بشرية من أجل إخفاء هجماتها.

إن العاملين المتخصصين في وكالة الأمن القومي لديهم أدوات قوية وجبارة قادرة على الوصول حتى إلى أفضل الشبكات حماية، كما تعمد الوكالة لإعطاء هذه الأدوات أسماء قوية ورنانة وعدوانية، فمثلاً تمت تسمية أحد البرامج باسم ترنيمة المطرقة (Hammerchant) وهذا البرنامج يتيح للوكالة تسجيل المكالمات الهاتفية التي تجري عبر الإنترنت (الصوت عبر بروتوكول الإنترنت VoIP)، ويوجد برنامج آخر يسمى ثعلب الأسيد (Foxacid) والذي يسمح لعملاء الوكالة بإضافة وظائف إلى البرامج الخبيثة الصغيرة التي تم تثبيتها مسبقًا في أجهزة الكمبيوتر الهدف، وشعار هذا المشروع هو ثعلب يصرخ وهو يذوب في الأسيد، وطبعًا فإن وكالة الأمن القومي رفضت التعليق على التفاصيل التنفيذية لهذه المهمات لكنها أصرّت على أنها لم تنتهك القانون من خلالها.

إن اقتحام شبكة وكالة الأمن القومي يشكّل حافزًا هائلاً للكثيرين، فبرامج الشبكات الخاصة التي تمتلكها والمفاتيح وكلمات السر وبرامج الطرق الثانوية لها قيمة عالية جدًا، كونه يمكن من خلالها – من الناحية النظرية – الاستيلاء على الحسابات المصرفية، واحباط عمليات الانتشار العسكرية والتحكم بالطائرات المقاتلة وإغلاق محطات توليد الكهرباء، وهذا يعني بالمحصلة الهيمنة على الشبكة العالمية، لذا فإن الوكالة حريصة من خلال دفاعاتها على تحصين شبكتها بأكثر الطرق أمانًا، وهذا يشكل بالنسبة لها أولوية على جميع العمليات التي تمارسها، وهذا ما يجعل عالم المخابرات الرقمية مصابًا بالفصام؛ فوظيفة وكالة الأمن القومي هي الدفاع عن الشبكة ولكنها في ذات الوقت تعمل على استغلال الثغرات الأمنية، وبمعنى آخر فإنها تلعب دور المفتش واللص بذات الوقت، وهذا يتفق مع الشعار الدائم الذي يتبعه الجواسيس في كل مكان: "اكشف أسرارهم، واحمِ

أسرارك".

الحصول على البيانات المسروقة:

من الأمور المضحكة في العالم الاستخباراتي بأنه أثناء انشغال الجواسيس بالتجسس يعمل جواسيس آخرون على التجسس عليهم، لذا تسعى وكالة الأمن القومي بشكل روتيني على تغطية آثارها بوضع آثار وهمية محلها، فمن الناحية التقنية، يعمل العملاء بعد اختراق أجهزة الكمبيوتر على تصدير البيانات التي تم جمعها، ولكن هذه البيانات لا يتم تسليمها مباشرة إلى عنوان الآي بي الخاص بالوكالة، بل يتم توجيهها إلى ما يسمى بكبش الفداء، وهذا يعني أن المعلومات المسروقة يمكن أن تنتهي على خوادم (سيرفرات) أخرى، مما يجعل أصحاب هذه الخوادم يبدون على أنهم الجناة.

بطبيعة الحال، فإن عمليات تخبئة المعلومات لا تقتصر على الكومبيوترات، حيث يمكن أن تستخدم الهواتف المحمولة لسرقة المعلومات، فالضحايا الذين لا يدرون بما يحصل، يحملون البرامج الخبيثة التي تم تحميلها على هواتفهم سرًا ويخرجون بها من مكتب العمل، ومن ثم يتم استرجاع المعلومات عن بعد عندما يعود الضحايا إلى المنزل بعد العمل.

على الرغم من أن عملاء وكالة الأمن القومي الرقميين لن يقلقوا في حال تم اكتشاف أفعالهم، كونهم يعملون لصالح وكالة قوية، ولكنهم مع ذلك يحرصون على عدم ترك أي أثر قد يستعمل ضدهم في المحاكم، وبالطبع فإن عدم وجود أدلة سيؤدي إلى انتفاء العقوبة، كما أن عدم وجود رقابة برلمانية أو اتفاق دولي يجعل من محاسبة وكالات الاستخبارات عن أفعالهم أمرًا مستحيلاً.

أخيرًا، على الرغم من أن إدوارد سنودن كشف كيفية عمل وكالات الاستخبارات في جميع أنحاء العالم، بقيادة وكالة الأمن القومي، إلا أننا لا ندري بعد إلا القليل عن خطورة الأسلحة الإلكترونية الحديثة، وأن المسؤولين عن وكالات الاستخبارات يبذلون قصارى جهدهم لضمان استمرار الفراغ القانوني في مجال جرائم الإنترنت، ويعبّر سنودن عن ذلك بقوله "إن الدفاع عن أمن المعلومات (لدى وكالات الاستخبارات) أصبح أقل أولوية من جرائم اختراق أمن المعلومات"، ويرى سنودن أنه يتعين علينا إنشاء معايير دولية جديدة لتحكم سلوك الجرائم الإلكترونية.

المصدر: دير شبيغل

رابط المقال : https://www.noonpost.com/5070/