حروب المخابرات الالكترونية

2017-07-06مؤيد جبار حسن

القبو7 او (VAULT7) هو سلسلة من الوثائق التي بدأ موقع ويكيليكس نشرها في 7 اذار عام 2017، وفيها شرح وكشف للأنشطة التفصيلية وقدرات وكالة الاستخبارات المركزية الامريكية في المراقبة والحرب الإلكترونية. تتضمن الملفات، المؤرخة من 2013-2016، تفاصيل عن قدرات البرامج الخاصة بالوكالة، مثل القدرة على التنازل عن السيارات والتجسس عبر أجهزة التلفزيون الذكية، ومتصفحات الويب (بما في ذلك غوغل كروم وميكروسوفت إدج وموزيلا فيريفوكس وأوبيرا سوفتوار) وأنظمة التشغيل لمعظم الهواتف الذكية (بما في ذلك دائرة الرقابة الداخلية أبل وجوجل)، فضلا عن أنظمة التشغيل الأخرى مثل مايكروسوفت ويندوز، ماك، لينكس.

ولقد تنبأ جوليان اسانج بهجمات الكترونية تطال العالم قبل حدوثها بأشهر، مما يدلل على مصداقيات التسريبات التي قام بها موقعه على الانترنت، مع عدم اغفال الغاية من تلك التسريبات التي قد تخدم الطرف الاخر، او وكالة الاستخبارات الامريكية.

تتكون القبو7 من عدة اجزاء، كل جزء منها يحمل في طياته عمل مخابراتي امريكي لإطلاق برامجيات خبيثة هدفها التجسس على العدو وتدمير معلوماته، والعدو هنا قد لا يكون بالضرورة منافس ايديولوجي كروسيا او كوريا الشمالية او منافس اقتصادي كالصين الشعبية، بل يمكن ان يكون مواطنون امريكيون وشركات كبرى امريكية. والهدف قد يكون اختباري او لإيصال رسالة لأطراف اخرى معينة، وفيما يلي سرد لها:

الجزء الاول وثائق تحمل اسم "عام الحسم" أطلقت في 7 آذار/2017، وتتألف من 818 7 صفحة على شبكة الإنترنت، يزعم أنها من مركز الاستخبارات السيبرانية، لم يذكر موقع ويكيليكس المصدر، لكنه قال إن الملفات "عممت بين القراصنة والمقاولين الحكوميين السابقين في الولايات المتحدة بطريقة غير مصرح بها، وقدم أحدهم ويكيليكس بأجزاء من الأرشيف". واثارت حينها نقاشا عاما حول أمن الأسلحة النووية، واستخدامها وانتشارها والسيطرة الديمقراطية عليها، لأن هذه الأدوات

تثير تساؤلات مفادها أن الحاجة ماسة إلى مناقشتها علنا، بما في ذلك ما إذا كانت قدرات القرصنة التابعة لوكالة المخابرات المركزية تتجاوز صلاحياتها مشكلة الرقابة العامة على الوكالة. فردت الاخيرة من خلال بيانا قالت فيه: "يجب أن يشعر الجمهور الأمريكي بالقلق العميق اذ ان إفصاح ويكيليكس يهدف إلى إلحاق الضرر بقدرة المجتمع الاستخباراتي على حماية أمريكا من الإرهابيين أو غيرهم من الخصوم، فهذه الإفصاحات لا تعرض الموظفين والعمليات الأميركية للخطر فحسب، بل أيضا تجهز خصومنا بالأدوات والمعلومات ليلحقوا بنا الضرر".

الجزء الثاني نشر في 23 اذار 2017 تحت اسم "الشيء المظلم". يتضمن هذا المنشور وثائق لعدة جهود لوكالة المخابرات المركزية لاختراق أجهزة إيفون وماك الخاصة بشركة أبل. وقد رفضت الاخيرة قرارا للحكومة الأميركية حرصا منها على خصوصية زبائنها واحتمال تعريض أمنهم للخطر، بعد أن لجأت واشنطن إلى المحكمة لإجبار الشركة على إنشاء باب خلفي في نظام تشغيل آيفون، حيث سيتمكن أي شخص يمتلك القدرة من فك تشفير أي آيفون، ومن ثم سيصبح من الممكن استخدام ذلك المرة تلو الأخرى في عدد من الأجهزة، رغم تأكيد مكتب التحقيقات الاتحادي أنه سيستخدم هذه الأداة مرة واحدة في تحقيقاته.

الجزء الثالث نشرته ويكيليكس في 31 اذار 2017 بعنوان (الرخام)، وقد احتوى على 676 ملف مشفرة المصدر لإطار عمل وكالة المخابرات المركزية. يتم استخدامها للتشويش على البرمجيات الخبيثة في محاولة لجعل حتى شركات مكافحة الفيروسات أو المحققين لا يمكن فهم تعليماتها البرمجية أو سمة مصدرها. رغم ما يشاع وسط مستخدمي الحاسوب، بل والقائمين على صيانته، وحتى لدى بعض المختصين أن ثمة علاقة بين بعض شركات مضادات الفيروسات العالمية وبين صناعة برامج الفيروسات، وبمعنى أوضح يتهمها البعض بأنها المسؤولة عن صناعة هذه الفيروسات من أجل ترويج بضاعتها ولو كان الثمن تدمير أجهزة كثيرة.

الجزء الرابع في 7 نيسان 2017 نشرت ويكيليكس هذا الجزء الذي يطلق عليه اسم "الجندب"، ويحتوي على 27 وثيقة. مضمون تلك الوثائق يوضح استخدام وكالة المخابرات المركزية لبرمجيات خبيثة مخصصة لأنظمة التشغيل ميكروسوفت ويندوز.

الجزء الخامس في 14 نيسان 2017 نشرته ويكيليكس تحت عنوان "قفير النحل". استنادا إلى برنامج سي آي أيه للفيروس السري الذي تستخدمه وكالة المخابرات المركزية لنقل المعلومات من أجهزة الكمبيوتر المكتبية المستهدفة والهواتف الذكية إلى وكالة المخابرات المركزية، وفتح تلك الأجهزة لتلقي أوامر أخرى من مشغلي وكالة المخابرات المركزية لتنفيذ مهام محددة.

الجزء السادس نشر في 21 نيسان 2017، التي أطلق عليها اسم "الملاك الباكي". وهي أداة للقرصنة وضعتها وكالة الاستخبارات المركزية، وتستخدم لاستغلال سلسلة من أجهزة التلفاز الذكية لغرض جمع المعلومات السرية. وبمجرد تركيبها في أجهزة تلفزيون فإن تلك الأداة تمكن الميكروفونات المدمجة وربما كاميرات الفيديو المدمجة في تلك التلفزيونات لتسجيل محيطها، ثم يتم تخزين البيانات المسجلة إما محليا في ذاكرة التلفزيون أو إرسالها عبر الإنترنت إلى وكالة المخابرات المركزية. ويزعم أن كلا من وكالة المخابرات المركزية والمخابرات الحربية البريطانية تعاونت لتطوير تلك البرمجيات الخبيثة وتنسيق عملهم في حلقات العمل المشتركة للتنمية. إن التعاون بين أجهزة الاستخبارات هو واحد من أهم المجالات في العلاقات الخاصة بين الولايات المتحدة وبريطانيا.

الجزء السابع في 28 نيسان 2017 نشرت ويكيليكس الجزء المسمى بـ "الخربشات". ويستهدف الوثائق المسربة والمشفرة المصدر، عبر أداة تهدف إلى تتبع الوثائق التي تسربت إلى المبلغين والصحفيين من خلال تضمين علامات الويب في الوثائق السرية لتتبعها.

الجزء الثامن في 5 ايار 2017 نشرت ويكيليكس الجزء 8 "أرخميدس". وفيه قام مشغلي وكالة المخابرات المركزية باستخدام فايروس أرخميدس لإعادة توجيه شبكة الإنترنت المحلية (لان) وجلسات مستعرض ويب من الكمبيوتر المستهدف من خلال جهاز كمبيوتر تسيطر عليها وكالة المخابرات المركزية قبل يتم توجيه الجلسات للمستخدمين. ويعرف هذا النوع من الهجوم باسم الرجل في الوسط.

الجزء التاسع في 12 ايار 2017 نشرت ويكيليكس "بعد منتصف الليل" و "القاتل". وهي برامج ضارة تثبت على جهاز الكمبيوتر الشخصي المستهدف وتتنكر كملفات اخرى. وتؤدي إلى توصيل الحاسوب

المستهدف بجهاز السيطرة والتحكم (C2) في وكالة المخابرات المركزية، والتي من خلالها يتم تحميل وحدات مختلفة لتشغيل.

الجزء العاشر في 19 ايار 2017 نشر بعنوان "أثينا". وفيها كل شيء عن البرمجيات الخبيثة التي وضعتها وكالة الاستخبارات المركزية في اصدار مايكروسوفت ويندوز 10، وفيها كل من البرامج الضارة "أثينا" الأساسية والبرمجيات الخبيثة الثانوية اسمه "هيرا" تشبه من الناحية النظرية إلى جندب و أفيرميدنيت البرمجيات الخبيثة باستثناء بعض الاختلافات الهامة.

خلاصة الامر ان الولايات المتحدة خاضت العديد من الحروب التقليدية مع اعدائها وكذلك جربت السلاح النووي لتنهي به الحرب العالمية الثانية، ونجحت في تركيع الامبراطورية اليابانية. اليوم الوضع يختلف، وساحات المعارك أصبحت فضاء سبرانيا والاسلحة فيها فايروسات الكترونية ليس لها وزن او كتلة، كما ان حدود البلد توسعت لتضم كيانه المعلوماتي الضخم، وهنا ازدادت المخاطر والتحديات امام صانع القرار السياسي والامني والعسكري، كيف يمكن حماية أمن الوطن امام هجمات قد تطاله عبر الانترنت مثلا، فداخليا تعرض الموقع الإلكتروني الرسمي لجهاز الأمن الوطني العراقي إلى الاختراق، إضافة إلى موقعي وزارتي الشباب والبلديات، مما تسبب في توقفها وظهور عبارات كتبها المخترق تنتقد المحاصصة والفساد الإداري، وخارجيا حدث قبل أيام وهاجم القراصنة العالم ببرامجيات خبيثة تصيب الحواسيب وتطلب الفدية لعتقها.

لذا يبدو ان الولايات المتحدة تحاول ان تكون القطب الاوحد في مجال الحرب الالكترونية، وتتغلب على باقي المنافسين على الساحة، من خلال اطلاق حزمة من البرمجيات المؤذية، كبالون اختبار، لما هو اكبر واكثر تأثيرا. ليس هي وحدها في الساحة، فهناك روسيا وباقي الدول الاوربية الكبرى، كذلك اسرائيل الصغيرة في حجمها الكبيرة في فعلها، والتي تدور حولها الشبهات في اصابتها البرنامج النووي الايراني في مقتل من خلال (فلاشة ذاكرة usb) تحتوي على فايروس مهلك.

* مركز الفرات للتنمية والدراسات الإستراتيجية/2004-2017
www.fcdrs.com