مركز الملك فيصل للبحوث والدراسات الإسلامية
King Faisal Center for Research and Islamic Studies

قدرات القرصنة السيبرانية الإيرانية

تقرير خاص

جمادى الأولى ١٤٤١هـ / يناير ٢٠٢٠م

قدرات القرصنة السيبرانية الإيرانية

تقرير خاص

المحتويات

ملخصٌ تنفيذي:

١. تملك إيران تفوقاً كبيراً في القدرات العسكرية غير المتماثلة، وتستخدم في ذلك وكلاءَها الإرهابيين، والتكنولوجيا العسكرية المنخفضة التكلفة؛ لموازنة قوى خصومها الأكثر تقدماً من الناحية التكنولوجية. وقد حدَّت العقوباتُ الدولية الناجحةُ من قدرة إيران على شراء أو تطوير تكنولوجيا متقدمة في جميع القطاعات تقريباً. ورغم ذلك، يمكنها امتلاك القدرة الإلكترونية الأساسية -التي تُتيح لها شَنَّ الهجمات أو التجسس على خصومها- وهو ما يمكن تحقيقُ الجزء الأكبر منه من خلال التعليم الذاتي والوصول إلى الإنترنت. وكما هو الحال مع أسلحة الحرب التقليدية، يمكن أيضاً تحسين القدرة الإلكترونية بمرور الوقت وتطويرها من خلال مراقبة تأثيرها على الهدف. وسنرى أن إيران لم تكتفي بتطوير مجموعة من القدرات الإلكترونية فحسب، بل تستخدمها أيضاً على نطاق واسع للتجسس والهجوم والسرقة.

٢. لقد تعرَّضت إيران في الماضي لهجمات إلكترونية مدمرة، وقد علمتها تلك الهجمات قيمة امتلاكها القدرةَ الإلكترونية الخاصة بها. في عام ٢٠١٠، أُصيبت جميع وحدات مفاعل التخصيب النووي الإيراني في نطنز بفيروس «ستاكس نت» الخفي الخطير؛ ما ألحق أضراراً بالمعدات اللازمة للبرنامج النووي. وفي عام ٢٠١٢، اكتُشف الفيروس «فلام» (وتُكتب أحياناً: فليم، أو فلايم)، على شبكات الحواسيب الإيرانية؛ وهو فيروس ذو قدرة على استخراج البيانات ومحوها سرّاً. استَخدمت إيران أيضاً «القمع الإلكتروني» لمواجهة الاحتجاجات التي انتشرت عبر الإنترنت فيما عُرِفَ بـ «الحركة الخضراء» عام ٢٠٠٩؛ ما أدَّى إلى الحد من الوصول إلى الإنترنت، وفَرْض رقابة على محتوى الويب الذي أدلى به المحتجون، أو حذفه.

٣. عادة ما تُمكِّنُ الدولُ القومية وكالةَ استخبارات من تشغيل برامجها الإلكترونية بصورة مباشرةً. ولكنْ، على النقيض من ذلك، فإن القوى العاملة الإلكترونية الإيرانية تتكون من شبكة معقدة من المقاولين، تستخدم الشركاتِ الإيرانيةَ الخاصةَ والمؤسسات الأكاديمية الداخلية لتنفيذ المهام عن طريق وُسطاء. يعمل «المديرون التقنيون» هؤلاء على المتطلبات والأهداف التي وضعتها وزارة الاستخبارات، أو الحرس الثوري الإيراني. ولا يوجد تجانس بين

مجموعات المتعاقدين هؤلاء، ويتم جمع جهودهم في بعض الأحيان لِشَنِّ الهجمات؛ ما يجعل تحديد الجناة بدقة وتعقُّبهم أمراً صعباً.

٤. تستخدم إيران الهجمات الإلكترونية للتجسس والوصول إلى البيانات وسرقة الملكية الفكرية ونشر الدعاية. وعادةً ما تُوصف مثل هذه الهجمات الإلكترونية التي ترعاها الدولة بأنها «تهديدات مستمرة متقدمة»، على الرغم من أن معظم الهجمات الإيرانية ليست متقدمة ولا مستمرة. وعادةً ما تستخدم الهجمات الإلكترونية الإيرانية مزيجاً من الأساليب ذات المهارات المنخفضة (مثل التصيُّد الاحتيالي)(*)، بالإضافة إلى تقنيات أكثر تطوراً؛ للوصول سرّاً إلى شبكة الهدف؛ وينتج عن هذا العديدُ من الهجمات التي تبدو عشوائيةً وغير احترافية؛ ما يزيد من احتمال كشف الهدف لها؛ ومن ثم؛ فإن كل هجوم يُكتشف سيزيد من احتمالية تحسين الهدف لدفاعاته. ومع أن الحكومة الأمريكية تكتشف الجهات الفاعلة الإلكترونية الإيرانية بشكل متكرر، وتُفصح عن عدد صغير منها علناً، وتوجه إليها الاتهام، فإن الهجمات تستمر، وبفضل «التدفق الكبير» تنجح الهجمات بوتيرة مقلقة. فقد تمكنت إيران من الوصول إلى بيانات حساسة عن الأفراد من خلال الهجمات على أهداف حكومية وتابعة لقطاع الخدمات. وقد نجحت -على الأرجح- في سرقة الملكية الفكرية من بعض شركات التكنولوجيا، إلى جانب الوصول إلى بيانات الاتصال من مقدمي الخدمات.

٥. ترغب إيران في تطوير نسختها الخاصة من فيروس «ستاكس نت»، لمهاجمة وتدمير المعدات - المعروفة باسم أنظمة التحكم الصناعي -، داخلَ المنشآت البتروكيماوية التي تمثل أهميةً كبيرة لاقتصاديات خصومها. ومع ذلك، فشلت إيران حتى الآن في تطوير هذه القدرة، وبدلاً من ذلك ركزت على الإضرار بشبكات تكنولوجيا المعلومات لهذه الأهداف. يُعرف الفيروس الذي مكَّن إيران من شن مثل هذه الهجمات باسم «شمعون»، وهو برنامج ذو قدرة على مسح البيانات، وقد دمَّر أنظمةً لتكنولوجيا المعلومات في أغسطس ٢٠١٢، ونوفمبر ٢٠١٦، وديسمبر ٢٠١٨.

(*) التصيُّد الاحتيالي: هو محاولة الحصول على معلومات حساسة، مثل أسماء المستخدمين، وكلمات المرور، وتفاصيل بطاقة الائتمان، والأموال، لأسباب ضارة غالباً، وذلك بالتنكر ككيان جدير بالثقة يمكن أن يكون، دون حصر، في صورة رسائل يتم إرسالها عبر البريد الإلكتروني، أو رسائل نصية فورية، أو وسائط اجتماعية، أو مواقع إلكترونية، أو مكالمات هاتفية.

٦. تستخدم إيران أيضاً بشكل فعال أبحاث تحديد الأهداف مفتوحة المصدر، لتصميم هجمات إلكترونية أكثر استهدافاً للأفراد ولنشر الدعاية. وعلى الرغم من ذلك، فإن إيران سوف تجد صعوبة في استخدامها الخبيث لوسائل التواصل الاجتماعي؛ بسبب المبادرات الأمنية الجديدة من قبل مقدمي الخدمات، الذين يسعَوْن إلى اكتشاف حساباتها الضارة وحجبها وإزالتها.

٧. تواصل إيران تحسين قدرتها على الهجوم الإلكتروني، وتُطور قدراتها التقنية، وتبتكر في عمليات استهدافها. ولأن الأهداف التقليدية أصبحت أكثر وعياً بالإجراءات المتعلقة بأمان تكنولوجيا المعلومات، فإن إيران تهاجم الآن المنظمات الأضعف في سلاسل الإمداد لهذه الأهداف. تُطلِق إيران هجماتها على نطاق واسع للحصول على معلومات أو العثور على «ثغرة» لإلحاق أضرار بأهدافها الأساسية أو السرقة منها. وتُوجَّه غالبية الهجمات الإلكترونية الإيرانية إلى أجهزة الكمبيوتر، على الرغم من أن لديها قدرة أساسية على سرقة البيانات من أجهزة الهواتف المحمولة. ومع أن هذه القدرة محدودة، إلا أنها تحولت بالفعل إلى الاستهداف الدولي بدلاً من الاستخدام المحلي الإيراني السابق. يُضاف إلى ذلك أن إيران ستواصل بالتأكيد تطوير الفيروس «شمعون» ونشره. وهي تعمل لامتلاك القدرة على تنفيذ هجوم لسرقة معلومات من مُورِّدي أنظمة التحكم الصناعي، تُمكِّنها من الوقوف على المزيد من نقاط الضعف في هذه المعدات. قد تكون إيران تتلقى أيضاً مساعدة من روسيا، يدعم ذلك مذكرة تفاهم ثنائية إلكترونية عامة، والكشف عن النشاط الإلكتروني الروسي غير المعتاد الذي كُشف أمره في الشرق الأوسط.

١. المقدمة:

١,١. تهدف هذه الورقة إلى جمع البحوث العامة حول النشاط الإلكتروني الحكومي المنسوب إلى إيران؛ من أجل استخلاص استنتاجات حول قدرتها الحالية. يوجد عدد كبير من البحوث حول النشاط الإلكتروني الإيراني، ولا تسعى هذه الورقة إلى تكرار البحوث الحالية أو الزيادة عليها، فقد أجرى بعضها كبارُ خبراء الأمن الإلكتروني في العالم؛ لكنها تسعى إلى النظر في مدلول هذا النشاط من منظور استراتيجي، وتقديم ملخص له، دون مطالبة القارئ بالإلمام بخلفية تقنية. وقدرَ الإمكان، ستسعى الورقة إلى تجنُّب المصطلحات الفنية المعقدة؛ ذلك الفخ الذي وقع فيه الكثير من الأوراق المكتوبة حولَ بعض الجوانب الإلكترونية.

٢,١. ستشير هذه الورقة دائماً إلى «الهجمات الإلكترونية»؛ وهي تعني: اختراقاً غيرَ مُصَرَّحٍ به لشبكة كمبيوتر أو جهاز من قبل جهة خارجية. وعادةً ما يبدأ الهجوم، أو الاختراق، من خلال الحصول على بيانات تسجيل دخول المستخدم، ويكون ذلك باستخدام «التصيُّد الاحتيالي»، الذي يحثُّ فيه المهاجمُ المستخدِمَ على اتباع رابط في رسالة بريد إلكتروني من مصدر يبدو موثوقاً. يُوجِّه الرابط إلى خادم الويب الخاضع لسيطرة المهاجمين؛ إما لسرقة بيانات الاعتماد من خلال شاشة تسجيل دخول تنتحل صفة جهة موثوقة، أو عن طريق تنزيل برمجيات خبيثة أو فيروسات ضارة على جهاز المستخدم. ويمر «التصيُّد الاحتيالي الموجه» بالخطوات نفسها، لكنْ، مع تفاعل خاضع لبحث وتحسين أكثر؛ على سبيل المثال، عن طريق إرسال رسالة بريد إلكتروني تنتحل صفة شريك تجاري مُحدِّد للهدف، تدور حول موضوع مألوف. ويتطلب هذا النوع من التصيُّد الاحتيالي معرفةً أكبر حول الهدف، ولكن فرص نجاحه أكبر. وسنرى كيف تُشَنُّ هذه «الهجمات» لسرقة المعلومات لأغراض استخباراتية، أو للوصول إلى مزيد من المعلومات، أو إتلاف المعدات المادية، أو نشر الدعاية. وتُوصف الهجمات الإلكترونية التي ترعاها الدولة عادةً بأنها «تهديدات مستمرة متقدمة»، على الرغم من أننا سنرى أن العديدَ منها ليس متقدماً ولا مستمرّاً.

٢. النشاط الإلكتروني الإيراني:

١,٢. قبل البدء، يجب أن نأخذ بعين الاعتبار خصائص الأمن القومي الإيراني وسياسة إيران الخارجية. فمنذ ثورة ١٩٧٩، اتبعت إيران مساراً سياسيّاً تصادميّاً مستمرّاً تقريباً مع الدول القومية الأخرى؛ فحكومتها مزيج من الثيوقراطية والديمقراطية الموجهة، التي تُنتج سياسةً أمنية يحكمها مزيجٌ من العوامل المتنافسة والمتداخلة: أيديولوجية الثورة الإسلامية، وإدراك التهديدات للنظام، والمصالح الوطنية الطويلة الأمد، والاحتكاك الداخلي بين الفصائل والمؤسسات السياسية[١]. تسعى إيران إلى تعزيز مكانتها الدولية، ولكنْ، ليس لديها حلفاء حقيقيون لهم مكانة دولية ذات شأن. دعمت قيادتها السياسية اندماج إيران في الدبلوماسية الدولية، لكنَّ المرشد الأعلى خامنئي والمؤسسات المتشددة الرئيسة؛ مثل الحرس الثوري الإيراني، يعارضون أي تغيير في الموقف الأمني للأمة. وفي الوقت الذي تهتم فيه إيران اهتماماً سطحيّاً بالجهود الدبلوماسية، تنفق ما يقرب من مليار دولار سنويّاً لدعم أعمال الإرهاب[٢]؛ إذ تُعَدُّ إيران الدولة الأكثر نشاطاً في رعاية الإرهاب منذ التسعينيات الميلادية المنصرمة.

٢,٢. تملك إيران تفوقاً كبيراً في القدرة العسكرية غير المتماثلة، وذلك نتيجة للعقوبات الدولية الناجحة التي حدَّت من قدرة إيران على شراء أو تطوير التكنولوجيا العسكرية. ولمّا لم يكن في إمكانها أن تتنافس مع تقدُّم الطيران العسكري، ركزت، بدلاً من ذلك، على تكنولوجيا الصواريخ الباليستية للوصول إلى خصومها. وقد أُوقف الاستثمار في بحرية المياه الزرقاء العالمية باهظة الثمن لصالح «أسراب» من طائرات الهجوم الرشيقة صغيرة الحجم. وبدلاً من الاستثمار في القوات البرية التقليدية، جمعت إيران جيوشاً من الوكلاء الإرهابيين والجماعات شبه العسكرية؛ مثل حزب الله، وفيلق القدس التابع للحرس الثوري الإيراني، والتي تتخصص في تنفيذ المهمات الخارجية، كما وفرت إيران التدريب والتمويل والأسلحة

---

(١) سياسات إيران الخارجية والدفاعية، خدمة أبحاث الكونغرس، ٨ أكتوبر ٢٠١٩.
https://fas.org/sgp/crs/mideast/R44017.pdf

(٢) مكافحة الإرهاب العالمي في إيران. تصريحات لناثان أ. سيليس، القائم بأعمال وكيل وزارة الأمن المدني والديمقراطية وحقوق الإنسان. سلسلة محاضرات مكافحة الإرهاب بمعهد واشنطن لسياسات الشرق الأدنى، واشنطن العاصمة، ١٣ نوفمبر ٢٠١٨.

للجماعات المتطرفة والمتمردين[٣]. ومن ثم؛ تُعَدُّ القدرة الإلكترونية امتداداً منطقيّاً وفعالًا لمساعي إيران الحالية لامتلاك القدرات غير المتماثلة. في عام ٢٠١٥، شهد مدير الاستخبارات القومية الأمريكية -آنذاك- جيمس كلابر أمام الكونغرس الأمريكي بأن إيران «تعتبر برنامجها الإلكتروني واحداً من العديد من الأدوات للقيام بانتقام غير متماثل - لكنه متناسب - ضد الخصوم السياسيين»[٤].

٣. أصول القدرة الإلكترونية:

١,٣. تعلمت إيران درساً ممتازاً في فنون الحرب الإلكترونية الناشئة؛ وذلك في عام ٢٠١٠ عندما انتشر الفيروس الخبيث السري «ستاكس نت»[٥]، في جميع وحدات مفاعل إيران للتخصيب النووي في نطنز، ساعد البرنامج في التعرف بالتفصيل على شبكات الكمبيوتر الخاصة بالمنشأة، بما في ذلك أنظمة التحكم الصناعي المتصلة، واستهدف بالتحديد وحدات التحكم المنطقية القابلة للبرمجة، والتي توفر التحكم في العمليات الكهروميكانيكية، وقد تسبب في تحطيم أجهزة الطرد المركزي سريعة الدوران. ويُعتقد أن «ستاكس نت» تسبب في أضرار جسيمة في البرنامج النووي الإيراني وأدَّى إلى تأخيره. الرد الإيراني الكامل على فيروس «ستاكس نت» غير معروف، لكنْ، من المؤكد أنه سيؤدي إلى تكاليف كبيرة ووقت إضافي لإصلاح الأضرار التي حدثت داخل أنظمة تكنولوجيا المعلومات، والتي سيتطلب الكثير منها عزلاً لتطهير البرنامج، بل قد يصل الأمر إلى تدميره. وبالقدر نفسه من التكلفة سيكون من الضروري تغيير المعدات الصناعية، تلك المعدات التي لا تحصل إيران عليها إلا من خلال شبكات بطيئة وسرية الانتشار. وسيكون هناك أيضاً مطاردة باهظة الثمن لمصدر البرنامج: من أدخله إلى المنشأة؟ وكيف أدخله؟

---

(٣) مشروع مكافحة التطرف. الحرس الثوري الإيراني.
https://www.counterextremism.com/threat/islamic-revolutionary-guard-corps-irgc

(٤) بيان حول سجل التهديدات الإلكترونية في جميع أنحاء العالم، لجنة الاختيار الدائمة بمجلس النواب، جيمس ر. كلابر، مدير الاستخبارات الوطنية، ١٠ سبتمبر ٢٠١٥.
https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf

(٥) مكافي: ما هو «ستاكس نت»؟
https://www.mcafee.com/enterprise/en-gb/security-awareness/ransomware/what-is-stuxnet.html

٢,٣. في عام ٢٠١٢ تمكنت شركة الأمن الإلكتروني ومكافحة الفيروسات «كاسبرسكاي»[٦] من التعرف على قطعة برمجية خبيثة على شبكات الكمبيوتر داخل إيران، لها القدرة على استخراج المعلومات سرّاً من أجهزة غير مُؤَمَّنة، ومن بين هذه المعلومات وثائق ومحادثات على وسائل التواصل الاجتماعي، وضغطات المستخدمين على لوحة المفاتيح. هذا البرنامج الضار الذي أُطلق عليه فيما بعد اسم «فليم»، كان له القدرة أيضاً على محو المعلومات. ويُحتمل أن يكون «فليم» نشطاً داخل إيران منذ عام ٢٠١٠.

٣,٣. وقبل «ستاكس نت» و«فليم»، مباشرةً تلقت إيران درساً آخر في الحرب الإلكترونية؛ وقد تلقته هذه المرة بينما هي في صدامٍ مع شعبها. إذ نشأت حركةٌ سياسية في إيران بعد الانتخابات الرئاسية الإيرانية عام ٢٠٠٩، طالب فيها المتظاهرون بإقالة محمود أحمدي نجاد من منصبه في أعقاب ما اعتبروه تزويراً للانتخابات. وأصبح هذا الحراك يُعرف باسم «الحركة الخضراء». وقد واجهت قوات الأمن الإيرانية الاحتجاجات بقوة، ورغم ذلك، واصل الشباب الإيراني الاحتجاج من خلال استخدام المحتوى على شبكة الإنترنت ووسائل التواصل الاجتماعي، وظهرت ساحة المعركة الجديدة هذه على «الإنترنت» كاشفةً عن نقطة ضعف رئيسة في قدرة الدولة الإيرانية على الاستجابة[٧]. تحولت الحكومة إلى «القمع الإلكتروني» للاحتجاجات؛ ما أدى إلى الحد من الوصول إلى الإنترنت، مع فرض الرقابة على المحتوى الذي ينشره المحتجون على شبكة الإنترنت، أو حذفه.

٤,٣. يحتاج النظام الإيراني إلى إيجاد أفراد قادرين على القيام بهذا النوع من النشاط الأمني الجديد؛ وكان من المستحيل تدريب المسؤولين الحكوميين على المهارات اللازمة للرد على نطاق واسع لمواجهة تلك القضية العاجلة؛ لذلك اتجهت إيران إلى أفراد من القطاع الخاص للقيام بهذا العمل الإلكتروني الانتقامي، وظهرت مجموعات عديدة تعمل تحت سيطرة الحرس الثوري الإيراني ووزارة الاستخبارات. وبدأت قدرة إيران الإلكترونية الجديدة في التبلور.

---

(٦) تعرف على «فليم»، «برمجيات التجسس الخطيرة التي تسللت إلى أجهزة الكمبيوتر الإيرانية.
Wired Magazine, Kim Zetter, 28 May 2012, https://www.wired.com/2012/05/flame/

(٧) الحرب الإلكترونية الإيرانية: قمع الدولة والانتقام الدولي.
Compass: The Gallatin Research Journal. Shannon Kandell, 2018

٤. القوى الإيرانية الفاعلة في مجال الإلكترونيات:

١,٤. خلص بحث أجرته مجموعة «إنسيكت»[٨] إلى أنه في أعقاب احتجاجات «الحركة الخضراء» وهجمات «ستاكس نت»، أرادت إيران إنشاء منظمة إلكترونية رسمية، لكنها لم تكن قادرةً على بناء «قوة عاملة موثوق بها سياسيّاً ودينيّاً». فغالبية المرشحين المؤهلين لمثل هذه المنظمة سيكونون من الشباب، ممن ليسوا مؤيدين للحكومة، ويحركهم المزيد من المكاسب المالية أكثر من الأيديولوجية الدينية أو السياسية. ووفقاً لمجموعة «إنسيكت»، كان الحل «نهجاً متدرجاً، مع إيجاد شبكة من الأشخاص يرتبطون بشكل غير رسمي بالحرس الثوري الإيراني والحكومة الإيرانية، ويكونون موالين للنظام، ويُظهرون الالتزام الديني الكافي». يعمل أصحاب هذه الطبقة الوسطى بوصفهم وسطاء، يترجمون الأولويات الاستخباراتية إلى مهام إلكترونية محددة، ويتواصلون بشأنها، ويسندونها بعد ذلك إلى مقاولين متعددين. وقد خلص بحث «إنسيكت» إلى أنه «في بعض الأحيان يتنافس المقاولون بعضهم مع بعض، وأحياناً يعملون معاً، ولكن لا يُدفع لهم إلّا إذا تحقق الهدف المرجو». ونتج عن ذلك نوعٌ من الترتيبات التي يديرها المقاول الذي تُسخِّره الحكومة. هذه الترتيبات تجعل المتعاقدين يتنافسون للحصول على العقود وتحقيق النفوذ لدى الحكومة الإيرانية.

٢,٤. وتُقَدِّر مجموعة «إنسيكت» بأن هناك أكثر من ٥٠ منظمة تتنافس على المشروعات الإلكترونية التي ترعاها الحكومة الإيرانية. وغالباً ما تُقسم هذه المشروعات بما يجعل مقاولَيْن مختلفَيْن (أو أكثر) مطالبين عادةً بتحقيق الهدف الذي حددته الحكومة. وقد أطلق مجتمع أبحاث الأمن الإلكتروني على هذه المجموعات مجموعةً متنوعة من الأسماء المميزة، تبدأ عادةً بكلمة «كيتين» للدلالة على الأصل الإيراني. وعلى الرغم من الإشارة إلى الجهات الفاعلة الإلكترونية الإيرانية في هذه الوثيقة، فقد استخدمنا واحدةً من اصطلاحات التسمية البديلة

---

(٨) مجموعة إنسيكت Insikt Group: مجموعة تتألف من باحثين مختصين في مجال التهديد الإلكتروني (ولاسيما مجال العملات الرقمية)، يقومون بتعقب الاختراق الإلكتروني، ويدعمون محللي الاستخبارات والمهندسين وعلماء البيانات، من أجل إيجاد رؤى لتقليل المخاطر المحتملة.
انظر: كشف التسلسل الهرمي للمخترقين الإيرانيين،
Levi Gundert, Sanil Chohan, and Greg Lesnewich. Recorded Future, 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf

التي توفر مجموعة أكثر تميزاً من الأسماء لسهولة التعرف عليها. وقد أنتجت شركات الأمن الإلكتروني مثل «فايرآي»[٩] و«كرودستريك»[١٠] تقاريرَ مستفيضة عن الأنشطة والقدرات الفنية للمجموعات الفردية، وتُواصِل تتبُّع أعمالها. إن أنشطة هذه المجموعات وتقييمها أمر دائم التغير؛ إذ إن الكثير من المعلومات الاستخباراتية عن هذه المجموعات - بعيداً عن الاستخبارات السرية التي حصلت عليها دول أجنبية - مستمدة من نشاطها الإلكتروني لا من البشر الذين يُنتجون هذا النشاط. وعلى الرغم من ذلك، فقد حُدِّدت أسماء مجموعة من الأفراد، خاصة في لوائح الاتهام الأمريكية؛ مثل أولئك الذين يعملون في «معهد مبنى»[١١]، الذي كلفه الحرسُ الثوري الإيراني باختراق شبكات مئات الجامعات الأمريكية والشركات وغيرها من الضحايا؛ لسرقة البحوث والبيانات الأكاديمية والملكية الفكرية. وبفضل مكتب التحقيقات الفيدرالي[١٢]، أصبح لدينا صورُهم وأوصافهم الجسدية الأساسية، لكننا نعرف القليل عن دوافعهم الحقيقية أو انتمائهم أو حياتهم المهنية.

٣,٤. تقدم مدونة النشاط الإلكتروني الإيراني «تهديدات إيران» عدة استنتاجات[١٣]، مفادها أن «النظام الإيكولوجي للجهات الفاعلة الإيرانية نظام فوضوي ودائم التغير؛ ما يجعل الغموضَ الموجود بين الحملات والمجموعات المختلفة أمراً مزعجاً». ويمكننا أن نفترض أن الأفراد الإيرانيين سوف يتنقلون بين الشركات؛ ويترتب على هذا، مع مرور الوقت، إمكانية استخدام مقاولين آخرين لبرامجهم، وأجزاء شيفراتهم البرمجية، والبنية الأساسية للهجمات التي صمموها.

٤,٤. قد تعمل المؤسسات الأكاديمية الإيرانية أيضاً بوصفها جزءاً من مجموعة الأدوات المتاحة للنظام، إما عن طريق تمكين النظام من تحديد المواهب، أو العمل مباشرة باعتبارها جزءاً

(٩) فايرآي، تقارير الإيرانيين.
https://www.fireeye.com/search.html?q=iranian

(١٠) تعرف على التهديدات المستمرة المتقدمة: قائمة بأسماء القوى الفاعلة في التهديدات الإلكترونية. ٢٤ فبراير ٢٠١٩،
Adam Meyers. https://www.crowdstrike.com/blog/meet-the-adversaries/

(١١) تسعة إيرانيين متهمون بشن حملة سرقة إلكترونية ضخمة لصالح الحرس الثوري الإيراني. ٢٣ مارس ٢٠١٨.
https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

(١٢) مخترقو «مبنى» الإيرانيون.
https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers

(١٣) من «كيتين» الطائر إلى «كيتين» الصاروخ، حالة من الغموض والكود المشترك. ٥ ديسمبر ٢٠١٧،
https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/

من متعهدي تقديم الخدمة. ومن الأمثلة على ذلك: «جامعة الشهيد بهشتي» التي يوجد بها معهد متخصص في الأبحاث الإلكترونية، و«جامعة الإمام الحسين» التي أسسها الحرس الثوري الإيراني، وتخضع لعقوبات من حكومة الولايات المتحدة لدعمها عمليات الحرس الثوري الإيراني. في عام ٢٠١٤، ألقى آية الله علي خامنئي خطاباً تحريضيّاً على طلاب الجامعات الإيرانية يحثهم فيه على إعداد أنفسهم للحرب الإلكترونية[١٤].

٥. القدرة:

١,٥. أُدرجت مراجعةٌ للنشاط الإلكتروني المنسوب إلى إيران خلال الاثني عشر شهراً الماضية في الملحق أ، والذي سنستخدمه لاستخلاص استنتاجات حول القدرة. ويمكننا، من خلال هذا الاستعراض، أن نرى عدداً من الجماعات الإيرانية الرئيسة وقد شاركت في عام ٢٠١٩ في هجمات إلكترونية؛ أطلق عليها مجتمع الأمن الإلكتروني أسماء: إلفين (أ ١٨، وأ ١٧، وأ ١٣، وأ ٤)؛ ومَدِّي ووتر (أ ٨)، وأويل ريج (أ ١٢، و أ ٥)، وشافر (أ ١٦). وغيرها من المجموعات الأخرى العاملة التي لم تُحدَّد بعد.

٢,٥. بيانات اعتماد المستخدم:

١,٢,٥. غالبية الهجمات الإلكترونية الإيرانية تبدأ بالحصول على بيانات اعتماد المستخدم تمهيداً لاختراق شبكات الكمبيوتر. وعادة ما يصل المخترق إلى بيانات الاعتماد هذه من خلال هجمات التصيُّد الاحتيالي غير المتطورة على نطاق واسع. ومع ذلك، فقد طورت جماعات إيرانية، مثل «إلفين» نظاماً أكثر تطوراً لمهاجمة نظام أسماء النطاقات[١٥] (DNS) (أ ١٤)، وشنت مجموعات أخرى هجمات تصيُّد احتيالي موجه أكثر تقدماً. يتطلب النوع الأخير مهارات لغوية أكثر تقدماً، وأبحاثاً مفتوحة المصدر؛ ولدى هذه المجموعات القدرة على كليهما، وعلى الرغم من ذلك فإن استخدام عمليات التصيُّد الاحتيالي واسعة النطاق، التي تتطلب القليل من المهارات، هي الطريقةُ الأكثر شيوعاً.

(١٤) المرشد الأعلى لإيران يطالب الطلاب بالاستعداد للحرب الإلكترونية. روسيا اليوم، ١٣ فبراير ٢٠١٤، https://www.rt.com/news/iran-israel-cyber-war-899/

(١٥) نظام أسماء النطاقات (DNS)، هو النظام الذي يترجم عنوان الويب إلى عنوان بروتوكول الإنترنت الفعلي (IP). تعمل الهجمات الموجهة لنظام أسماء النطاقات من خلال التلاعب بنظام أسماء النطاقات الخاص بالمنظمة المستهدفة أو الاستيلاء عليه، من أجل توجيه المستخدمين إما إلى موقع مختلف، أو إلى مسار غير مباشر إلى الوجهة المذكورة. وفيه تُجذب الأهداف إلى وجهة أو مسار خاضع لسيطرة المهاجم (أي موقع ويب مخترق يحتوي على شفرة ضارة).

٣,٥. سرقة الملفات:

١,٣,٥. فور حصول المجموعة الإلكترونية الإيرانية على إمكانية الوصول إلى شبكة أو جهاز، يكون لديها القدرة المؤكدة على الكشف عن الملفات سرّاً. وبالنظر إلى حجم هجمات سرقة كلمات المرور، فمن الواضح أن إيران تسرق البيانات على نطاق واسع من مجموعة من الأهداف.

٢,٣,٥. يشمل تقييمنا للمعلومات النموذجية التي سرقتها المنظمة ما يلي:

- **الحكومات والقوات المسلحة:**

- التجسس على الموقف السياسي والعسكري تجاه إيران والتقنيات والمعلومات التي توفر تفوقاً اقتصاديّاً.

- **موزّدي البتروكيماويات:**

- معلومات عن المرافق والخطط والمعدات والموظفين.

- **مصنّعي المعدات وشركات الخدمات البتروكيماوية:**

- التكنولوجيا، خصوصاً شفرة المصدر وتصميم المعدات.

- **مزوّدي الاتصالات:**

- الوصول إلى قواعد البيانات التي توفر معلومات المشترك، وسجلات المكالمات، والبريد الإلكتروني، وبيانات الاتصالات الأخرى؛ مثل معلومات تحديد الموقع الجغرافي.

- **السفر:**

- الوصول إلى قواعد البيانات التي توفر بيانات السفر، وبيانات العميل؛ لتتبُّع الأهداف.

- **الأفراد المعارضين:**

- الحصول على معلومات حول تحركاتهم واتصالاتهم.

- **المؤسسات الأكاديمية والعلمية، والشركات المصنعة:**

- الملكية الفكرية والتكنولوجيا.

٣,٣,٥. يمكن أن يشملَ الاستهداف عدة نطاقات مختلفة: سرقة الملكية الفكرية والمعلومات (من الحكومات والمصنعين والأوساط الأكاديمية والمعارضين)، ودعم الوصول إلى المعلومات على نطاق أوسع (الاتصالات السلكية واللاسلكية، والسفر)، أو السعي إلى

التدمير (البتروكيماويات والحكومات). ولا شك في أن هذا النشاط سيُنتج بيانات مهمة تحتاج إلى ترجمة من مجموعة من اللغات، مع توفُّر المعرفة الخبيرة لاستغلالها. ويمكن للمرء أن يتصور أن كمية المعلومات قد تكون كبيرة؛ بسبب التعاقد مع القوى العاملة الإلكترونية، التي يُقاس نجاحها في أداء المهمة -في بعض الحالات- بحجم البيانات المسروقة. وهنا تظهر مشكلة خاصة عندما يفتقر المقاول إلى الخبرة التي تُمكِّنه من تقييم المواد التي سرقها؛ ولا شك في أن هذا سيحدث مع اتساع دائرة الاستهداف. يمكن لإيران استخدام القوى العاملة التي تتعاقد معها لتقييم البيانات المسروقة، على الرغم من أن التقارير تشير إلى أن وزارة الاستخبارات الإيرانية لديها ٣٠٠٠ ضابط[١٦]، لكن لا يمكنهم العمل على هذه المهمة.

٤,٥. تدمير البيانات:

١,٤,٥. وَضَع فيروس «شمعون» (أ ١٩) المعيار العالمي لأسوأ حالات الهجمات المدمرة. وإن كان هناك هدف وحيد أمكنه أن ينجو من آثار فقدان مثل هذه البيانات، والخسائر في تكنولوجيا المعلومات، فهو شركة أرامكو السعودية، أغنى شركة في العالم. عاد فيروس «شمعون» ثلاث مرات معلومة، وسيعود على الأرجح مرة أخرى لكن بدرجة أعلى من التطور. وقد أدى النجاح الذي حققه «شمعون١» إلى غزارة إنتاجية؛ فقد ركز مجتمع الأمن الإلكتروني على تطوير برمجيات الحد من المخاطر، وركز العملاء على شرائها، ولم تتعرض أرامكو السعودية لهجوم ناجح مرة أخرى. لم ينجح «شمعون٢» ولا «شمعون٣» ذلك النجاحَ الذي حققه «شمعون١»، على الرغم من أن عملية اختيار الهدف المحسن؛ مثل اختيار شخص أقل استعداداً، يمكن أن تؤدي إلى مستويات تدمير مماثلة في الإصدارات اللاحقة. ويحرص الإيرانيون أيضاً على اختيار أهداف نسختهم الخاصة من «شمعون»، والوصول سرّاً إلى شبكات الأهداف التي ضربها الإصداران ٢ و٣ مسبقاً. ويسعى «شمعون٣» أيضاً إلى تعطيل سلاسل التزويد، والتي قد تكون وسيلةً أخرى لإلحاق الضرر بالأهداف الرئيسة -مثل أرامكو السعودية- التي أصبح من الصعب للغاية مهاجمتها مباشرةً.

---

(١٦) القوة العسكرية الإيرانية: ضمان بقاء النظام وتأمين الهيمنة الإقليمية، وكالة استخبارات الدفاع الأمريكية، ٢٠١٩.
https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Iran_Military_Power_V13b_LR.pdf

٥,٥. أنظمة التحكم الصناعي:

١,٥,٥. تسبب فيروس «شمعون» في إلحاق ضرر واسع النطاق بالبنية الأساسية لتكنولوجيا المعلومات لشركات البتروكيماويات، لكنه لم يمسَّ أنظمة التحكم الصناعي؛ وهي الأنظمة الكهروميكانيكية والأدوات المرتبطة بها المستخدمة للتحكم في العمليات الصناعية. ربما طُوِّرَت منهجية الهجوم لإحداث أقصى قدر من الضرر بما يغني عن مهاجمة أنظمة التحكم الصناعي، ولا ريب في أن إيران تعمل على تطوير هجمات إلكترونية موجهة لأنظمة التحكم الصناعي، لكنها ستواجه تحديات التطوير. سيمكنها فقط الوصول إلى مجموعة فرعية من المعدات التي تحتاج إلى اختبارها؛ بسبب العقوبات التي تمنعها من المبيعات الدولية. على سبيل المثال، حتى لو تمكنت إيران من اكتشاف المعدات الدقيقة المثبتة داخل منشأة ما في المملكة العربية السعودية، فسيكون لديها معرفة محدودة حول المعدات المثبتة، ولا يمكنها الوصول إليها لإجراء التجارب عليها.

٢,٥,٥. سيتعين على إيران سرقة هذه البيانات من مورِّدي أنظمة التحكم الصناعي. ويبدو أن مجموعة «إلفين» (أ ٤) قد كُلِّفت بالحصول على مثل هذه المعلومات، على الرغم من الحاجة إلى وجود موارد معقدة ووقت متاح لعكس هندسة أي بيانات مسروقة. ومع ذلك، فإن إيران هي أول من اكتوى بنار هذا النوع من الهجمات، وتفهم بشكل مباشر الضرر الذي يمكن أن يُحدثه هجوم ناجح على أنظمة التحكم الصناعي، وستواصل جهودها، وربما تسعى للحصول على هذه التكنولوجيا من شريك مثل روسيا (٣,١٠).

٦. هجوم رفض الخدمة:

١,٦. في مجال الحوسبة، يعني هجوم رفض الخدمة[١٧] هجوماً عبر الإنترنت يسعى فيه المهاجم إلى جعل جهاز أو مَورد شبكة غيرَ متاح لمستخدميه المقصودين؛ عن طريق تعطيل خدمات مضيف متصل بالإنترنت مؤقتاً، أو إلى أجل غير مسمّىً. وعادةً ما تُرفض الخدمة عن طريق إغراق الجهاز أو المَورد المستهدف بطلبات زائدة على الحاجة، في محاولة لزيادة التحميل على الأنظمة، ومنع تنفيذ بعض أو جميع الطلبات المشروعة.

(17) https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/

٢,٦. لم يَكشف هذا الاستعراض عن أي هجمات إيرانية مرتبطة بهجوم رفض الخدمة خلالَ الفترة قيد الدراسة. وقد كان هذا في العادة تكتيكاً إيرانيّاً شائعاً؛ فقد شَنَّت إيران هجوماً متواصلاً من هذا النوع على البنوك الأمريكية والكيانات الأخرى خلالَ الفترة ٢٠١١ - ٢٠١٣ [١٨]. وقد أصبحت خدمات الحماية من هجمات رفض الخدمة الآن شائعةً، وقد يكون غياب مثل هذه الهجمات علامةً على أن أهداف إيران صارت محميةً بشكل جيد ضد هذه الأنواع من الهجمات.

٧. أجهزة الهواتف المحمولة:

١,٧. هناك نقص ملحوظ في الهجمات المسجلة على أجهزة الهواتف المحمولة في البحث، بالنظر إلى الآلاف من الهجمات على أجهزة الكمبيوتر. وتنحصر قدرة إيران في مهاجمة أجهزة الهواتف المحمولة في خداع الهدف لتحميل تطبيق مراسلة مزيف (أ ٩)، والذي بدوره يمكنه استخراج البيانات من الجهاز سرّاً. وتُعد هذه طريقةً محدودة؛ لأن التطبيقات المزيفة لا يمكن «توفيرها» من خلال أسواق التطبيقات المعتادة، مثل متجر «جوجل بلاي». ويقتصر الهجوم أيضاً على الأجهزة التي تعمل بنظام «أندرويد»؛ إذ لا توجد طريقة لتثبيت تطبيقات جهة خارجية على أجهزة أبل. وعلى الرغم من ذلك، حقق الإيرانيون بعض النجاح في هذا النهج، وسيواصلون استخدام هذه التقنية وتعزيزها.

٢,٧. يمكننا أن نفترض أن مجموعات الإنترنت الإيرانية ستعمل على مهاجمة الأجهزة المحمولة مباشرةً (من خلال أنظمة التشغيل الخاصة بهم)، لكنهم لا يملكون هذه الإمكانية في الوقت الحالي. لديهم أيضاً القدرة على مهاجمة جهاز من خلال هجوم تصيُّد احتيالي، وعلى الرغم من ذلك، فإن الاختراقات الناجحة لموفري الاتصالات قد تتطلب يوماً ما منصةً أخرى.

٨. وسائل التواصل الاجتماعي:

١,٨. تستخدم إيران وسائل التواصل الاجتماعي لتوزيع الدعاية وهندسة هجمات التصيُّد الاحتيالي الموجه ضد الأفراد عن طريق انتحال شخصيات آخرين (أ ١٦، أ ١١). وقد اضطلعت بهذه

---

(١٨) سبعة إيرانيين متهمون بشن هجمات رفض الخدمة ضد البنوك الأمريكية.
bankinfosecurity.com, Eric Chabrow
https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989

الأنشطة لسنوات عديدة وبدرجة من النجاح: نشر دعاية تحت اسم مستعار، أو انتحال شخصية آخرين لإجراء تواصل مع الأهداف المعنية. ومع ذلك، في عام ٢٠١٩، أصبحت هذه الأنشطة أكثرَ صعوبةً؛ نظراً لانتشار فضائح «الأخبار المزيفة»؛ فمن الأرجح أن تتحقق وسائل الإعلام من مصادرها، ولكون منصات وسائل التواصل الاجتماعي أصبحت تملك الآن، بشكل متزايد، إجراءات أقوى للتسجيل وفحص المحتوى. ويُعتبر موقع «فيس بوك»[١٩] خاصة قويّاً في إزالة شبكات الحسابات المزيفة التي تنشر الدعاية الإيرانية. نحن نعتقد أن إيران ستُواصل استخدام وسائل التواصل الاجتماعي لنشر الدعاية، لكنها ستواجه صعوبةً متزايدة في إنشاء حسابات مزيفة والحفاظ على نشاط تلك الحسابات، خاصةً على نطاق واسع.

٩. استخبارات الإشارات:

١,٩. أحد الأسباب المحتملة لنهج إيران واسع النطاق تجاه الهجمات الإلكترونية، هو افتقارها إلى القدرة على امتلاك استخبارات إشارات عالمية[٢٠]، تسمح لإيران بجمع بيانات الاتصالات عن جيرانها الإقليميين وخصومها العالميين. ولا تملك تكنولوجيا استخبارات الإشارات العالمية إلا أغنى دول العالم؛ مثل الولايات المتحدة وحلفائها من دول «العيون الخمسة» FVEY، وكذلك روسيا والصين. بالإضافة إلى ذلك، هناك عدد صغير من الدول الغنية ذات القدرة الإقليمية المحدودة، والتي تستخدم الأصول العسكرية لجمع البيانات.

٢,٩. أدت سنواتٌ من شبه العزلة الإيرانية إلى محدودية الوصول إلى التكنولوجيا والتدريب؛ ما حدَّ من القدرة على تطوير التكنولوجيا المتقدمة. وتفتقر إيران أيضاً إلى أقاليم خارجية يمكنها استخدام مثل هذه التكنولوجيا فيها للحصول على امتداد بعيد المدى (مثل كوبا للاتحاد السوفيتي السابق). وربما أدى ذلك إلى إعطاء الأولوية لجهودها الهجومية الإلكترونية، وخاصة الجهود الرامية إلى استهداف مزودي الاتصالات. إن اختراق هذه

(١٩) إزالة المزيد من الحسابات المزيفة التي تسلك سلوكا منسقاً من إيران وروسيا، ٢١ أكتوبر ٢٠١٩.
https://newsroom.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/

(٢٠) يقصد باستخبارات الإشارات: معلومات استخباراتية مستمدة من الإشارات الإلكترونية والأنظمة التي تستخدمها الأهداف الخارجية؛ مثل أنظمة الاتصالات والرادارات وأنظمة الأسلحة. وتوفر استخبارات الإشارات نافذة حيوية على قدرات الخصوم الأجانب، وأفعالهم، ونواياهم.
https://www.nsa.gov/what-we-do/signals-intelligence/

الجهات سيوفر لإيران قدرةً معززةً بشكل كبير على تحديد الأفراد واستهدافهم. وسيؤدي ذلك إلى تحسين قدرتها على شن هجمات تصيُّد احتيالي موجه، بل الهجوم المباشر على الفرد من خلال شبكة مزود الخدمة.

٣,٩. ومع ذلك، تُطَوِّر إيران منشأةً لجمع بيانات الأقمار الصناعية، وفقاً لما أوردته مجلة «جينز إنتليجنس ريفيو» في يونيو ٢٠١٨ [٢١]. ويشير تحليل المجلة لمكان الموقع وتكوينه إلى أنه يستهدف أقمار الاتصالات في المدارات المتزامنة، بما في ذلك تلك الموجودة في إسرائيل، والمملكة العربية السعودية، والولايات المتحدة. تمتلك إيران أيضاً إمكانية الوصول إلى الاتصالات واعتراضها من عدد من الكابلات البحرية التي تمر عبر أراضيها. الكابلات البحرية، هي كابلاتُ اتصالات ممتدة في قاع البحر بين المحطات الأرضية لنقل إشارات الاتصالات عبر المحيطات والبحار. وتَستخدم هذه الكابلات تقنيةَ الألياف الضوئية لنقل البيانات الرقمية، التي تشمل الاتصالات الهاتفية والإنترنت وحركة البيانات الخاصة. هناك محطات أرضية للكابلات[٢٢] في المدن الإيرانية: بندر عباس، وجاسك، وشابهار. وأحد هذه الكابلات يسمى «فالكون»، وهو متصل بعشر دول أخرى؛ من بينها المملكة العربية السعودية.

٤,٩. من شأن استخبارات الإشارات أن تُعَزِّز بشكل كبير قدرة إيران على جمع بيانات الاتصالات، وكذلك قدرتها على الوصول إلى حركة البيانات من الكابلات البحرية، إضافةً إلى جهود تجميع البيانات الإقليمية. هذا يمكن أن يجعل إيران أقل اعتماداً على المقاولين التقليديين الذين ينفذون برنامجها الإلكتروني ضد جيرانها. ومع ذلك، فمن الصحيح أيضاً أن الوصول إلى مثل هذه البيانات يمكن أن يعزز القدرة الحالية، مضيفاً خيارات لجمع البيانات ولإنشاء بنية أساسية جديدة لمهاجمة أهدافها. وتُعتبر تكنولوجيا استخبارات الإشارات مكلفة للغاية، وتتطلب تقنيات متقدمة؛ لذا، سيكون من الصعب على إيران امتلاك أي قدرة من شأنها مواكبة أساليب جمع البيانات الحالية.

---

(٢١) منشأة إشارات فضائية إيرانية جديدة تستهدف القمر الصناعي.

IHS Markit, Jane's Editorial Staff, June 2018,
https://ihsmarkit.com/research-analysis/new-iranian-space-signals-facility-targets-satellites.html

(٢٢) خريطة الكابلات البحرية.

Tele Geography, https://www.submarinecablemap.com/#/

١٠. المساعدة الخارجية:

١٠,١. ليس لإيران تحالفات وثيقة وعلنية مثل الصداقات العالمية التي يتمتع بها جيرانها؛ كما هو الحال مثلاً بين المملكة العربية السعودية والولايات المتحدة. تتمتع إيران بعلاقة طويلة الأمد ومعقدة مع روسيا، التي تشاركها العداء لخصوم سياسيين؛ كالولايات المتحدة والمملكة المتحدة والاتحاد الأوروبي، على الرغم من عدم وجود ثقة متبادلة بين البلدين. في عام ٢٠١٢، ذكرت مكتبة الكونغرس الأمريكية[٢٣]، حولَ العلاقة الاستخباراتية بين روسيا وإيران من خلال التعاون بين وزارة الشؤون الخارجية الإيرانية وجهاز الاستخبارات الخارجية الروسي، أنه على الرغم من العقائد المتباينة بين الوكالتين والعلاقة المعقدة بين إيران وروسيا في الماضي، فقد تمكنتا من التعاون في التسعينيات، ليس فقط بناءً على اعتزامهما الحد من النفوذ السياسي الأمريكي في آسيا الوسطى، ولكن أيضاً اعتماداً على جهودهما المشتركة في القضاء على الاضطرابات العرقية المحتملة. لم يقتصر دور روسيا على تدريب المئات من العملاء الإيرانيين فحسب، بل دربت أيضاً العديد من العملاء الروس داخلَ إيران لتزويد أجهزة الاستخبارات الإيرانية بمعدات الإشارات في مُجَمَّع قيادتهم العامة.

١٠,٢. هناك مجموعة من الأدلة مفتوحة المصدر تدعم وجود علاقة إلكترونية بين إيران وروسيا. ففي وقت مبكر من عام ٢٠١٤، استمعت لجنة الشؤون الخارجية بمجلس النواب الأمريكي إلى شهادة[٢٤] مفادها أن التغير في موازين الأمن القومي بين الولايات المتحدة وإيران يرجع إلى «تطور القدرات الإلكترونية الإيرانية وإلى توطيد إيران علاقتها بروسيا». وتتابع الإفادة بأنه «في فترة زمنية قصيرة للغاية، انتقلت إيران من قدرة (المستوى ٢/ المستوى ٣) إلى أن أصبحت تقريباً من الطراز العالمي في مجال القدرات الإلكترونية، وتأتي مباشرة بعد الولايات المتحدة وروسيا والصين وإسرائيل». في الآونة الأخيرة اعتباراً من مارس ٢٠١٧،

---

(٢٣) وزارة الاستخبارات والأمن الإيرانية: ملف تعريف، مكتبة الكونغرس، تقرير أعدته شعبة الأبحاث الفيدرالية بمكتبة الكونغرس بموجب اتفاق بين الوكالات مع برنامج دعم الحرب غير النظامية التابع لمكتب الدعم الفني لمكافحة الإرهاب، ديسمبر ٢٠١٢.
https://fas.org/irp/world/iran/mois-loc.pdf

(٢٤) دعم إيران للإرهاب في جميع أنحاء العالم. بيان المبجل بيت هوكسترا، زميل شيلمان الأقدم، مشروع التحقيق في الإرهاب (الرئيس السابق للجنة الاستخبارات الدائمة لمجلس النواب الأمريكي).
https://docs.house.gov/meetings/FA/FA13/20140304/101832/HHRG-113-FA13-Transcript-20140304.pdf

أعلنت قناة «برس تي في» الإيرانية التابعة للدولة[٢٥] أن إيران وروسيا ستُطوران التعاون الأمني الإلكتروني، ومن المعقول أن يشمل ذلك التعاون الهجمات الإلكترونية أيضاً، وربما ظهرت أولى ثمار هذا التعاون في وقت لاحق من عام ٢٠١٧.

٣,١٠. «تريتون»... «ستاكس نت» الثاني:

٤,١٠. في ديسمبر ٢٠١٧ اكتُشف برنامج ضار أُطلق عليه لاحقاً مُسمى «تريتون» في أنظمة السلامة الخاصة بمرفق للبتروكيماويات مجهول الهوية في المملكة العربية السعودية[٢٦]. وقد سعى ذلك البرنامج الخبيث إلى إعادة برمجة وحدات التحكم الصناعي المستخدمة لتحديد مشكلات السلامة. ولحسن الحظ، دخلت بعض وحدات التحكم المستهدفة في وضع «العطل الآمن»؛ ما تسبب في إيقاف تشغيل العمليات ذات الصلة، ومكَّن مهندسي المصنع من تحديد الهجوم. وتعتقد شركة الأمن الإلكتروني «فايرآي» بأن تصرفات المهاجم تسببت دون قصد في إيقاف التشغيل في أثناء محاولته التحقق من النظام لمعرفة كيفية عمله.

٥,١٠. وُصِفَ «تريتون» لاحقاً بأنه «أكثر البرامج الضارة فتكاً في العالم»[٢٧] وخضع لتحليل واسع النطاق من قِبَلِ خبراء الأمن الإلكتروني ومن شركة «شنايدر»[٢٨]، الشركة المصنعة لمعدات السلامة. تمكن «تريتون» من الوصول إلى شبكة المصنع من خلال هجوم غير معلوم، جاء على الأرجح عن طريق رسالة بريد إلكتروني للتصيُّد الاحتيالي، أو جهاز نقل بيانات (USB). وبشكل خطير، انتقل البرنامج الضار من شبكة المستخدم إلى معدات أنظمة التحكم الصناعي، وفي هذه الحالة انتقل البرنامج إلى نوع شائع من أنظمة تحكم المستخدم، للتحكم في إدارة المعدات الصناعية. ومن المقدر أن هدف «تريتون» النهائي

---

(٢٥) إيران وروسيا تعلنان عن خطط للتعاون في مجال الأمن الإلكتروني، برس تي في، عبر موقع يوتيوب، ١٥ مارس ٢٠١٧.
https://www.youtube.com/watch?v=NaCukjiECWM

(٢٦) قراصنة يوقفون عمليات مصنع في هجوم إلكتروني فاصل، جيم فينكل، ١٤ ديسمبر ٢٠١٧.
https://uk.reuters.com/article/us-cyber-infrastructure-attack/hackers-halt-plant-operations-in-watershed-cyber-attack-idUKKBN1E8271

(27) MIT Technology Review, Martin Giles, 5 March 2019
https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/

(28) TRITON - Schneider Electric Analysis and Disclosure, 23 January 2018
https://www.youtube.com/watch?v=f09E75bWvkk

كان تغيير حدود السلامة داخل وحدة التحكم، ومن ثم؛ دفع المعدات إلى حالة غير آمنة، لا يتعامل معها؛ الأمر الذي يقود إلى فشل كارثي محتمل. وربما استُخدم «تريتون» في وضع الاستطلاع للتعرف على النظام، وربما للمساعدة في تطويره.

٦,١٠. بالنظر إلى موقع الهدف ونوعه اشتُبِه في أن تكون إيران وراء «تريتون»، على الرغم من أن هذا من شأنه أن يُمثل تغيراً في القدرة الإلكترونية الهجومية الإيرانية، التي لم يسبق لها أن هددت أي معدات لأنظمة التحكم الصناعي. لكن «فايرآي»[٢٩] قَدَّرت بعد مزيد من التحليل الشامل أن الحكومة الروسية هي من طورت «تريتون».

٧,١٠. اختيار الهدف غير عادي بالنسبة إلى روسيا، التي يُستبعد أن تستهدف المملكة العربية السعودية بمثل هذا الهجوم المدمر. قد يكون الهدف اختير أداةً لاختبار «تريتون» عن بعد، لكنْ، لماذا لم يُختر موقعٌ آخر في منطقة أقل اضطراباً خصوصاً مع وجود القواسم المشتركة بين المعدات. كان لا بد من إجراء بحث مكثف لتحديد المنشأة المستهدفة؛ فهل ستُجري روسيا بالفعل مثل هذه البحوث المفصلة في منطقة خارج أهدافها الاستخباراتية التقليدية؟ قد تشير هذه التساؤلات حولَ الدافع وراء الهجوم إلى تعاون مع إيران بشأن استهداف المنشأة على الأقل. إذ لا تملك إيران قدرة مهاجمة أنظمة التحكم الصناعي، لكن لديها رغبة قوية ومحاولات سابقة لشن مثل هذا الهجوم. ولدى إيران القدرة على الوصول إلى المعلومات الاستخباراتية لتحديد هدف اختباري مناسب، وستشير إليها أصابع الاتهام إذا اكتُشف الهجوم. ويمكن لروسيا أن تستهدف هذه المنشأة لأسباب كثيرة؛ من بينها أن الهجوم الاختباري لن يُنسب إليها (إذا ما اكتُشف)، ومساعدة إيران حليفتها الإلكترونية. قد لا نصل أبداً إلى إجابة عن هذا السؤال، لكنْ، يمكننا الجزم بأن المساعدة الروسية للبرنامج الإلكتروني الإيراني ستزيد من قدرته. في أكتوبر ٢٠١٩ (أ ٥) اكتُشِف عنصر إلكتروني روسي فاعل يستخدم البنية الأساسية الإلكترونية الإيرانية لشن هجمات إلكترونية. كان الافتراض هو أن روسيا سرقت ما وصل إليه الإيرانيون، لكنْ، هل يُحتمل كونهم يعملون معاً؟

---

(٢٩) نسبة «تريتون»: مختبر روسي تملكه الحكومة على الأرجح صمم أدوات اختراق مخصصة لمهاجمي «تريتون».
FireEye Intelligence, 23 October 2018, https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

١١. ملخص حول القدرة:

١,١١. تستخدم إيران القدرة الإلكترونية عنصراً أساسيّاً في قدرتها الهجومية غير المتماثلة (٣). فالهجمات الإلكترونية تُستخدم للتجسس، والوصول إلى البيانات، وسرقة الملكية الفكرية، والدعاية (٥).

٢,١١. تعرضت إيران لهجمات إلكترونية ضارة في الماضي، تعلمت منها قيمة امتلاك القدرة الإلكترونية واستخدامها المحتمل ضد خصومها (١,٣). وستواصل تطوير ونشر نسختها من هجمات «شمعون» (٦,٥) الموجهة لمحو بيانات الأقراص الصلبة، على الرغم من أن تطورات الأمن الإلكتروني والاستثمارات في هذا المجال سوف تُقوّي دفاعات الأهداف ضد تلك الهجمات. وقد بدأت إيران بالفعل في تحويل دفة هجماتها إلى سلاسل التوريد بدلاً من الأهداف الرئيسة. ويُعد امتلاك القدرة على مهاجمة أنظمة التحكم الصناعي (٥,٧) أولويةً واضحةً، وعلى الرغم من أن ذلك صعبٌ ومكلف تقنيّاً، فإن إيران ستسعى لتطوير تلك التقنية من خلال سرقة معلومات هذه الأنظمة مباشرةً من الشركات المصنعة لها، وقد تتلقى أيضاً مساعدة من روسيا (٣,١٠).

٣,١١. تستخدم إيران القدرة الإلكترونية لتلبية احتياجاتها الاستخباراتية بدلاً من الوصول إلى جهاز عالمي لاستخبارات الإشارات (٩)، رغم أنها تعمل على تطوير هذه التقنية. وستستمر الهجمات ضد شركات الاتصالات والسفر (٥,٥)، مع سعي إيران للوصول إلى قواعد البيانات التي توفر معلومات استخباراتية حول اتصالات وحركات الأفراد المستهدفين. ستصبح هذه الهجمات عالميةً بشكل متزايد مع اكتشاف مصادر جديدة للبيانات. نحن نعتقد أن إيران ستسعى للحصول على قدرة أكثر تقدماً ضد الأجهزة المحمولة؛ إذ إن قدرتها الحالية عليها قيود شديدة (٧).

٤,١١. لدى إيران قدرة محدودة على الوصول إلى خصومها، ولا يمكنها إرسال أشخاص لجمع المعلومات الاستخباراتية حول غالبية أهدافها. نتيجةً لذلك، تستخدم المجموعات الإلكترونية الأبحاث مفتوحة المصدر بفاعلية لتحديد الأهداف، إضافةً إلى هندسة هجمات تصيُّد احتيالي موجه متقنة. وسيستمر استخدام وسائل التواصل الاجتماعي (٨) لتحديد أهداف للتصيُّد الاحتيالي الموجه ونشر الدعاية، وعلى الرغم من ذلك فإن شركات وسائل التواصل

الاجتماعي ستزيد من صعوبة هذا الأمر على إيران، ما سيجعل محاولاتها في النهاية أقلَّ فاعلية.

٥,١١. بدلاً من تطوير قدرة إلكترونية حكومية داخلية، قررت إيران الاستفادة من شبكة من المقاولين، باستخدام الشركات الإيرانية الخاصة والمؤسسات الأكاديمية الداخلية (٤). هذه المجموعات ليست متجانسة، وتُجْمَعُ جهودها في بعض الأحيان لشَنِّ الهجمات، وقدراتهم مختلطة، مع وجود مستويات متفاوتة من المهارة بين المجموعات، بل داخل سلسلة الهجمات الفردية نفسها. وهذا يجعل تحديد مرتكبي الهجوم على وجه الدقة وتعقُّبهم تحدياً صعباً. ومع ذلك، فإن مجتمع الأمن الإلكتروني الدولي ينتج قدراً هائلاً من التقارير المفصلة حول هذه المجموعات. وسوف تزداد الصورة وضوحاً لدى هذا المجتمع مع تطوير الإيرانيين للقدرات الإلكترونية، على الرغم من أن الإدارة الداخلية لهذه المجموعات ستُصَعِّب دائماً من مسألة التحديد الدقيق والوقتي لمرتكبي الهجمات.

٦,١١. تستخدم إيران مزيجاً من الهجمات منخفضة المهارات (مثل التصيُّد الاحتيالي)؛ بالإضافة إلى تقنيات أكثر تطوراً؛ للوصول سرّاً إلى شبكة الهدف (٤,٥). وينتج عن هذا العديد من الهجمات التي تبدو عشوائية وغير احترافية. وهناك احتمال كبير لكشف مثل هذه الهجمات واسعة النطاق، خاصة عن طريق أهداف لديها القدرات التقنية. قد يكون هذا النهج ناتجاً عن القدرة المنخفضة لبعض المقاولين الإلكترونيين، أو مدفوعاً بالحاجة المالية إلى تحقيق نتائج أكثر كمّاً عبر استراتيجية استخباراتية نوعية طويلة المدى. نتساءل أيضاً عمّا إذا كان لدى إيران القدرة على تقييم كميات كبيرة من المعلومات التي يُتَحَصَّل عليها من الهجمات الإلكترونية، خاصةً إذا كانت تقنية. قد يؤدي ذلك إلى سياسة تجميعية أكثر استهدافاً، كما رأينا مع هجمات المجموعة «إلفين» الموجهة إلى أنظمة التحكُّم الصناعي (أ ٤)، أو تحديد الأولويات لمزيد من الاختراقات الأوسع نطاقاً والأكبر تدميراً.

٧,١١. في الفضاء الإلكتروني تُعدُّ إيران لاعباً عدوانيّاً مصمِّماً على هدفه، وتهاجم على نطاق عالمي بقدرات متفاوتة. وعلى الرغم من أن الأمر في هذه الأنشطة يحتاج إلى جهد ليكون سريّاً، إلا أنه يُكتشف بشكل منتظم. ولا يبدو أن إيران تلقي إلى ذلك بالاً؛ فهي تستخدم الهجمات الإلكترونية للتجسس والهجوم باعتبارها جزءاً من نهجها الأمني.

الملحق أ:

استعراضٌ للهجمات الإلكترونية المرتبطة بإيران:

١. تُعَدُّ الهجمات الإلكترونية مادة إخبارية ثرية؛ وسيقف البحث الذي يسعى إلى تجميع الحوادث المرتبطة بهذا الموضوع على وفرة من النتائج؛ تتمثل في التقارير الصادرة عن وسائل الإعلام، وشركات الأمن الإلكتروني، والباحثين في مجال الأمن الخاص، والحكومات العالمية. وفيما يتعلق بإعداد هذه الورقة، فقد استعرضنا التقارير المتعلقة بالحوادث الإلكترونية المهمة التي نُسبت إلى إيران على مدار الاثني عشر شهراً الأخيرة، بما في ذلك أي حوادث ذات صلة وقعت قبل هذه الفترة. وذلك لاستكشاف القدرات الحديثة التي ستكون أكثر صلة بأي هجمات قد تحدث في المستقبل. وعلى كل الأحوال لا يُعد هذا ملخصاً شاملاً؛ لأن الإحاطة بهذا الموضوع شبهُ مستحيلة؛ وكذلك، فإن اكتشاف هذه الهجمات، أو الحكم بنسبة أيٍّ منها إلى إيران، ليس أمراً مؤكداً بنسبة مئة في المئة. وبالمثل، فإن هناك عدداً غير معروف من الهجمات التي تعجز عن اختراق أهدافها، الأمر الذي لا يضمن إجراء مزيد من التحقيقات، أو قد يُنسب ارتكابها خطأً إلى مجرمين أو دول أخرى، وتضيع في النهاية وسط الضجيج العالمي للنشاط الإلكتروني الضار. وأخيراً، كما أوضحنا، فإن هناك عدداً لا يُحصى من المجموعات التي تعمل داخلَ إيران؛ ما يجعل اكتشاف مُنفِّذ الهجمات أمراً صعباً وغير متسق؛ وقد خلصت دراستنا إلى أن تحديد منفذ الهجمات بدقة أمر يتغير مع مرور الوقت.

٢. اعتمدنا في إعداد قائمة الحوادث على مجموعة من التقارير الإعلامية، وعلى تقارير مركز الدراسات الاستراتيجية والدولية بواشنطن[٣٠]، الذي نشر جدولًا زمنيّاً مسجلة فيه الحوادث الإلكترونية المهمة التي وقعت منذ عام ٢٠٠٦. وإضافةً إلى ذلك، فقد ضمَّنّا التقاريرَ والتحليلات التي كُتبت حول تسريبات المستندات التي ادُّعِيَ أنها صادرة عن الجهات الفاعلة الإلكترونية الإيرانية؛ وهي تقدم تفاصيل لم تكن معروفة من قبل حولَ الاستهداف والهجمات.

---

(٣٠) مركز الدراسات الاستراتيجية والدولية، الحوادث الإلكترونية المهمة.
https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

٣. رُتبت التقارير حسب تاريخ النشر، ولا يُعَبِّرُ هذا بالضرورة عن أولوية الكشف عن الهجوم أو نسبته إلى منفذيه، فبعض الهجمات (التي يُشار إليها بعد أن تصبح معروفة) كانت تعمل على مدار شهور، أو ربما سنوات، قبل أن تصبح معروفة على نطاق واسع.

٤. نوفمبر ٢٠١٩:

مجموعة إلكترونية إيرانية تسعى للحصول على قدرة تتعلق بأنظمة التحكم الصناعي:

١,٤. نشرت وسائل الإعلام تقارير عن مؤتمر أعلنت فيه شركة ميكروسوفت[٣١] تقديرها بأن مجموعة الاختراق الإيرانية المعروفة باسم «إلفين» تسعى لتطوير قدرةٍ لمهاجمة أنظمة التحكم الصناعي. وقد ذكرت ميكروسوفت أن المجموعة كانت تستهدف عشرات الآلاف من المؤسسات باستخدام تقنيات بدائية للقرصنة؛ عن طريق محاولة الوصول إلى الحسابات باستخدام كلمات المرور المعروفة والشائعة. وقد ضاق نطاق هجمات «إلفين» الآن ليصل إلى نحو ٢٠٠٠ مؤسسة شهريّاً، مع زيادة عدد الحسابات المستهدفة في كلٍّ منها إلى عشرة أضعاف تقريباً. وقد صنَّفت ميكروسوفت هذه الأهداف حسب عدد الحسابات التي حاولت المجموعة اختراقها؛ فكان «نحو نصف المراكز الـ٢٥ الأولى شركات مصنّعة، أو موردين، أو مشرفين على معدات أنظمة التحكم الصناعي». وتعتقد ميكروسوفت بأن «إلفين» تسعى إلى تطوير قدرةٍ تُمَكِّنها من تنفيذ هجمات إلكترونية على أنظمة التحكم الصناعي تكون ذات آثار مادية مدمرة.

٢,٤. التقييم: لن يكون هناك سببٌ وجيهٌ أمام إيران للوصول إلى شبكات الشركات المرتبطة بأنظمة التحكم الصناعي ما لم تكن تسعى للحصول على معلومات عن هذه الأنظمة. وقد حسَّنت «إلفين» من بحثها ليقتصر على عدد أقل من الشركات، أو أُعيد تكليفها بتركيز جهودها (لتكون أكثر نجاحاً).

---

(٣١) طاقم اختراق إيراني شهير يستهدف أنظمة للتحكم الصناعي.
Wired.com, Andy Greenberg, 22 November 2019, https://www.wired.com/story/iran-apt33-industrial-control-systems/

٥. أكتوبر ٢٠١٩:

اكتشاف فاعل إلكتروني روسي يستخدم البنية الأساسية الإلكترونية الإيرانية لشن هجمات إلكترونية:

١,٥. كشف تحقيق مشترك أجرته الحكومتان البريطانية والأمريكية عن أن عملية إلكترونية إيرانية اختُرقت أنشطتها من جانب روسيا[٣٢]. وقد استهدف الفاعل الإلكتروني الروسي البنية الأساسية الإلكترونية السرية للقيادة والسيطرة التي أنشأتها مجموعة الاختراق الإيرانية المعروفة للباحثين باسم «أويل ريج» (١٣). وقد صممت «أويل ريج» هذه البنية الإلكترونية الأساسية لشَنِّ هجماتها الخاصة، لكنَّ المجموعة الروسية استولت عليها سرّاً لنشر برمجياتها الخاصة بصورة سرية، مستغلةً الهجوم الحالي ليوصلها إلى الهدف. وكانت الهجمات الروسية قادرةً على استخراج قوائم الأدلة وملفات من الأهداف، مع رصد تفاصيل النشاط الإيراني. وشمل ذلك قوائم الضحايا الناشطين، مع بيانات اعتماد المستخدمين الخاصة بالوصول إلى بياناتهم الأساسية. وقد استُهدف أكثر من ٣٥ دولة، وكان غالبية الضحايا في الشرق الأوسط.

٢,٥. التقييم: لم يقتصر الأمر على اكتشاف المزيد من النشاط الإلكتروني الإيراني فحسب، بل تَركت هذه الأنشطةُ الأنظمةَ عُرضة للآخرين؛ ما يزيد من احتمال وقوع التلف وفقدان البيانات.

٦. أكتوبر ٢٠١٩:

اكتشاف جهات إلكترونية إيرانية فاعلة تحاول اختراق حسابات بريد إلكتروني:

١,٦. أصدرت ميكروسوفت[٣٣] في الفترة من أغسطس إلى سبتمبر ٢٠١٩ تقارير تفيد بأن مجموعة إلكترونية إيرانية معروفة شنَّت أكثر من ٢٧٠٠ محاولة لتحديد حسابات البريد الإلكتروني المرتبطة بمجموعة محددة من عملاء ميكروسوفت. وقد شرعت المجموعة في مهاجمة ٢٤١ حساباً من هذه الحسابات، وشمل المستهدفون أشخاصاً مرتبطين بحملة رئاسية أمريكية،

---

(٣٢) أدفيزري: مجموعة «تورلا» تستغل مجموعة (APT) الإيرانية لتوسيع نطاق تغطية الضحايا، المركز القومي للأمن الإلكتروني في المملكة المتحدة، ٢١ أكتوبر ٢٠١٩.
https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims

(٣٣) الهجمات الإلكترونية الأخيرة تتطلب منا جميعًا أن نكون يقظين. توم بيرت. ٤ أكتوبر ٢٠١٩.
https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/

ومسؤولين حكوميين أمريكيين حاليين وسابقين، وصحفيين يغطون أخبار السياسة العالمية، وإيرانيين بارزين يعيشون خارج إيران.

٢,٦. ذكرت ميكروسوفت أن تلك المجموعة جمعت معلومات من بحث مفتوح المصدر، ثم شنَّت هجمات أولية لفرض إعادة تعيين لكلمة المرور أو لاستخدام ميزة استرداد الحساب، ثم محاولة الاستيلاء على تلك الحسابات. على سبيل المثال، تم ذلك بأن تسعى المجموعة إلى الوصول إلى حساب البريد الإلكتروني الثانوي المرتبط بحساب المستخدم على ميكروسوفت، ثم تحاول الوصول إلى حساب المستخدم الأساسي من خلال التحقُّق الذي يُرسل إلى الحساب الثانوي. في بعض الحالات، جمعوا أرقام هواتف تابعة لأهدافهم، واستخدموها للمساعدة في المصادقة على إعادة تعيين كلمة المرور.

٣,٦. التقييم: صرحت ميكروسوفت بأن الهجمات «لم تكن معقدة تقنيّاً»، لكنها لاحظت كيف أن المهاجمين سعَوْا إلى استخدام قدر كبير من المعلومات الشخصية لتحديد الحسابات التي تنتمي إلى أهدافهم المقصودة ومحاولة مهاجمتها. ونحن نعتقد أن المهاجمين قد استفادوا بشكل كبير من المصادر المفتوحة، وأنهم قد خصصوا قدراً كبيراً من الوقت في محاولاتهم الوصول إلى الحسابات. وجاء اختيار الأهداف مثيراً للاهتمام أيضاً؛ لأنه قد يُظهر اهتماماً بالعملية الانتخابية الأمريكية، وهو أمرٌ لم يُنسب إلى إيران من قبل.

٧. أغسطس ٢٠١٩:

قراصنة مرتبطون بإيران يخترقون شبكات العديد من الوكالات الحكومية البحرينية وموردي البنية التحتية الحيوية:

١,٧. أفادت وسائل الإعلام المختلفة[٣٤] باختراق شبكات الكمبيوتر التابعة لوكالة الأمن القومي في البحرين، ووزارة الداخلية، ومكتب النائب الأول لرئيس الوزراء. ولا توجد تفاصيل عن طبيعة الاختراق أو الأضرار الحادثة، رغم أن وسائل الإعلام الأمريكية ذكرت أن المخابرات الأمريكية تعتقد أن إيران هي الجاني المحتمل.

(٣٤) قراصنة إيرانيون يُشتبه في أنهم شنوا هجمات إلكترونية على البحرين. تحذير من وراء الخليج، تقرير: زاك دوفمان. ٨ أغسطس ٢٠١٩.
https://www.forbes.com/sites/zakdoffman/2019/08/08/iranian-hackers-suspected-of-cyberattacks-on-bahrain-sending-message-beyond-the-gulf-report/#567af93a324b

٢,٧. في يوليو ٢٠١٩، ذكرت وسائل الإعلام نفسها أن شبكات هيئة الكهرباء والماء في البحرين تعرضت لخطر «إغلاق العديد من الأنظمة»، وأن «المخترقين تمكنوا من السيطرة المحدودة على عدة أجزاء من النظام». ونقلت وسائل الإعلام نفسها عن «محللين وخبراء» لم يُصَرَّح بأسمائهم أن مستوى التطور في هذه الهجمات أعلى من الهجمات السابقة المنسوبة إلى إيران. يُضاف إلى ذلك ما ذكرته صحيفة «وول ستريت جورنال»[٣٥] من أن شركة ألمنيوم البحرين (ألبا)، وهي واحدة من أكبر المصاهر في العالم، كانت مستهدفةً أيضاً، على الرغم من أن الشركة أصدرت بياناً لاحقاً قالت فيه: إنها لم تقع ضحيةً لهجوم إلكتروني.

٣,٧. التقييم: تشير التقارير الإعلامية إلى وجود أوجه شبهٍ بهجمات «شمعون» (أ ١٩) التي وقعت في عام ٢٠١٢ [٣٦]. وقد تسببت تلك الهجمات في أضرار واسعة النطاق حيث تسببت في مسح البيانات من الأقراص الصلبة للأنظمة المستهدفة، لكنها لم تؤثر على أنظمة التحكم الصناعي. يُنسب «شمعون» إلى إيران، وقد ظهر مرتين في يناير ٢٠١٧، وديسمبر ٢٠١٨. وفي وقت كتابة هذه الورقة، كان هناك القليل جدّاً من المعلومات المتاحة للجمهور عن هذه الهجمات الجديدة.

٨. يونيو ٢٠١٩:

تسريبات توضح بالتفصيل الأفراد غير المعروفين المستهدفين بالهجمات الإلكترونية في البلدان المحيطة بإيران:

١,٨. قدَّم تسريب غير مقصود للبيانات على تطبيق المراسلة «تليجرام» معلوماتٍ تقنيةً عن مجموعة إيرانية تُعرف باسم «مَدِّي ووتر»، اكتُشفت لأول مرة عام ٢٠١٧ [٣٧]. كانت هذه المجموعة تستهدف -في الغالب- الأفراد في دول الشرق الأوسط. ومع ذلك، لُوحظ أنهم يهاجمون أهدافاً أخرى، من بينها أهدافٌ في الهند والولايات المتحدة الأمريكية.

---

(٣٥) اختراقات إلكترونية عالية المستوى تضرب البحرين وسط توترات مع إيران.
Bradley Hope, Warren P. Strobel and Dustin Volz. 7 August 2019
https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488

(٣٦) فيروس «شمعون» يستهدف البنية التحتية لقطاع الطاقة. ١٧ أغسطس ٢٠١٢.
https://www.bbc.co.uk/news/technology-19293797

(٣٧) تعكير المياه: هجمات استهدافية في الشرق الأوسط. توم لانكستر. ١٤ نوفمبر ٢٠١٧.
https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

٢,٨. نشرت شركة الأمن الإلكتروني «كليرسكاي» تحليلاً فنيّاً مفصلاً[٣٨] عن المعلومات المسربة، المتعلقة باستهداف أفراد باستخدام طريقة العمل نفسها المستخدمة عام ٢٠١٧؛ عن طريق إرسال مستندات بالبريد الإلكتروني تنتحل صفة مراسلات رسمية، لكنها تحتوي على شفرة سرية ضارة تهدف إلى الوصول إلى البيانات الأولية التي تُمَكِّن من الوصول إلى أجهزة الهدف. وفي هذه الحالة، يُزعم أن المستندات مُرسلةٌ من جهات فاعلة حكومية (مثل مزودي الاتصالات في الدولة، أو الأمم المتحدة). تضم مجموعة الأفراد المستهدفين: الحكومات العراقية، والطاجيكية، والباكستانية، وشركة اتصالات باكستانية، وأفراداً غير معروفين في الهند والإمارات وقبرص، وأخيراً الجماعات الكردية في العراق.

٣,٨. التقييم: ذكرت شركة «كليرسكاي» أن الهجوم استخدم ثغرة أمنية معروفة، وكان بدائيّاً في نهجه الذي يتطلب من الهدف النقر على رسائل خطأ، ومع ذلك، لم يكتشفه إلا ثلاثة محركات لمكافحة الفيروسات. وقد زُيِّفت الوثائق بجودة عالية وكانت غامضة نسبيّاً؛ ما يشير إلى أن المهاجمين قد أجرَوْا قدراً كبيراً من الأبحاث حول أهدافهم باستخدام مصدر مفتوح. وجاء نطاق اختيار الأهداف واسعاً، ومن المفترض أنه كان بغرض التجسس. ومع ذلك، يمكن أن يشير تضمين مزود اتصالات واحد على الأقل إلى أن أحد أهداف الهجمات كان تمكين الوصول إلى أهداف أخرى داخل شبكات مُقدِّمي الخدمة هؤلاء. ولا نعرف ما إذا كانت هذه الهجمات قد نجحت في تحقيق أهدافها، أم لا.

٩. يونيو ٢٠١٩:

تطبيقات وهمية للهاتف المحمول تُستخدم للتجسس على أفراد عسكريين في الشرق الأوسط:

١,٩. كشفت شركة الأمن الإلكتروني «تريندميكرو»[٣٩] عن مجموعة من تطبيقات الهواتف المحمولة الوهمية التي تعمل بنظام أندرويد، تنتحل صفة تطبيقات حقيقية. وتحاكي هذه

---

(٣٨) مجموعة (APT) «مدى ووتر» الإيرانية تعزز من قدراتها: نظرة عامة وتحليل للبنى الأساسية والتكتيكات والتقنيات والإجراءات الجديدة لـ «مدى ووتر». شركة الأمن الإلكتروني «كليرسكاي»، يونيو ٢٠١٩.
https://www.clearskysec.com/wp-content/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf

(٣٩) حملة التجسس الإلكترونية على الهواتف المحمولة «بونسينج جولف» تؤثر على الشرق الأوسط، تريندميكرو، أوكيولر شو، جري جو، ١٨ يونيو ٢٠١٩.
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

التطبيقات المظهر العام لتطبيقات المراسلة، مثل «تليجرام» أو «كيك» أو «بلس»، ولكنها تحتوي على برمجيات خبيثة تهدف إلى سرقة البيانات من الجهاز المضيف، وكذلك تسجيل الصوت والفيديو بشكل سري. راقبت «ترينديميكرو» خادم الأوامر والتحكم الذي يستخدمه المهاجمون، وتوصلت إلى أن ٦٦٠ جهازاً محمولاً تستخدم التطبيقات المزيفة، وأن معظم الأجهزة المتأثرة موجودة في الشرق الأوسط، وأن كثيراً من البيانات المخزنة مرتبطة بشؤون عسكرية؛ ما يشير إلى استهداف أفراد عسكريين. ويشير التقرير إلى الأبحاث السابقة التي أجرتها شركة «تشيكبوينت ريسيرش»[٤٠]، التي اكتشفت أنشطةً مشابهةً في الفترة من ٢٠١٦ حتى ٢٠١٨، ضد مجموعة كبيرة من الأهداف الإيرانية التي يُعتقد أنها محلية.

٢,٩. التقييم: تمتلك إيران القدرة على مهاجمة الأجهزة المحمولة وزرع البرمجيات الثابتة فيها؛ من خلال استخدام تطبيقات وهمية. هذه التطبيقات المزيفة لا تستضيفها منصات التطبيقات الرسمية؛ مثل «جوجل بلاي». وقد لاحظت «ترينديميكرو» أن هذه التطبيقات يُروَّج لها على وسائل التواصل الاجتماعي، ما يشير إلى أن أهداف هذه الهجمات لا بد أنها تُوَجَّه لتحميل التطبيق، إما عن طريق إرسال رسائل البريد الإلكتروني التي تُرسل إلى الهدف باستخدام التصيُّد الاحتيالي الموجه، أو مباشرةً عن طريق جهات الاتصال الضارة (التي تعمل لصالح إيران). ويشير البحث أيضاً إلى تحوُّل في استخدام هذه التقنية من الأهداف المحلية إلى الأهداف الدولية. قد يكون هذا نتيجة زيادة ثقة إيران في التقنية (بناءً على النجاحات الماضية)، وكذلك القدرة على نشر التطبيقات خارج إيران والتحكم فيها.

١٠. مايو ٢٠١٩:

تسريبات حول أهداف وأعمال مجموعة إلكترونية إيرانية:

١,١٠. سُرِّبت بيانات غير منسوبة على تطبيق المراسلة «تليجرام» تقدم نسخاً من وثائق الحكومة الإيرانية الرسمية تدور بصورة مفصلة حول «معهد رانا»[٤١]. صُنِّفت الوثائق على أنها «سرية»،

---

(٤٠) أهداف محلية: عملية مراقبة إيرانية، تشيكبوينت ريسيرش، ٧ سبتمبر ٢٠١٨.
https://research.checkpoint.com/2018/domestic-kitten-an-iranian-surveillance-operation/

(٤١) تسريب جديد حول عمليات تجسس إلكتروني إيرانية تستهدف برنامج تليجرام والإنترنت المظلم. كاتالين سيمبانو، شبكة «زيرو داي». ٩ مايو ٢٠١٩.
https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web/

ويبدو أن وزارة الاستخبارات الإيرانية هي من أنتجت هذه الوثائق. وقد أظهر تحليل مفصل أجرته شركة الأمن الإلكتروني «كليرسكاي»[٤٢] لتلك الوثائق استهدافَ «رانا» لتتبُّع المواطنين الإيرانيين خارج إيران مع مجموعة كبيرة من المعلومات حول الحملات الإلكترونية السابقة. ويتضمن ذلك تفاصيل الهجمات التي ركزت على اختراق شركات الطيران للاستيلاء على بيانات المسافرين، واختراق مواقع حجز السفر للاستيلاء على بيانات الحجوزات وأرقام بطاقات الدفع. وفي بعض الحالات، أُشير إلى أفراد محددين، مع عدم ذكر أسمائهم، بأنهم يسافرون على متن رحلات دولية. وتشمل الأهداف الإضافية: شركات التأمين، وتكنولوجيا المعلومات، وشركات الاتصالات السلكية واللاسلكية، وكذلك الوكالات والإدارات الحكومية على نطاق عالمي. وليس من الواضح ما إذا كانت هذه الهجمات قد خُطِّط لها فقط أم إنها نُفِّذَتْ بالفعل، وما إذا كانت انتهت بالنجاح أم بالفشل.

٢,١٠. تُظهر إحدى الوثائق أن الحرس الثوري الإيراني كلَّف المجموعة بتطوير برامج ضارة قادرة على إتلاف أنظمة التحكم الصناعي، لكنَّ «المشروع لم ينجح ولم يحقق أهدافه على الرغم من ميزانيته الكبيرة». ويوفر مستند إضافي لقطة شاشة لمحاولة إخفاء عملية شراء عُملة مشفرة (ربما بسبب العقوبات) باستخدام بيئة افتراضية (وباستخدام اتصال مناسب) لتظهر العملية على أنها قادمة من الهند.

٣,١٠. التقييم: تغطي هذه المعلومات المسربة نطاقاً واسعاً، خاصةً مع الزعم بأنها مصادر أصلية. فالوصول إلى معلومات السفر أمر غير معتاد؛ لأنه يشير إلى أن المهاجمين مكلفون بتتبع تحركات الأفراد خارج إيران، ويُفترض أن ذلك يحدث بهدف الربط بمعلومات استخباراتية أخرى غير محددة. وقد ذُكر أن أهداف المجموعة تتمثل في التركيز على الإيرانيين، وعلى الأرجح، أولئك المشتبه في ضلوعهم في أنشطة مضادة للنظام. ومع ذلك، لا يقتصر الاستهداف على هذا الجانب فقط، خاصةً أن من الأهداف كيانات إسرائيلية. وقد يكون هذا استهدافاً للإيرانيين اليهود الذين يقيمون في إسرائيل، أو للتجسس على الحكومة الإسرائيلية.

---

(٤٢) نظرة عامة وتحليل للوثائق المسربة: الأهداف، والخطط، وأبعاد الهجوم. شركة الأمن الإلكتروني «كليرسكاي». مايو ٢٠١٩.
https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf

١١. مايو ٢٠١٩:

الكشف عن شبكة حسابات وهمية وأخبار مزيفة على تويتر، تُستخدم لنشر معلومات كاذبة عن الولايات المتحدة وإسرائيل والمملكة العربية السعودية:

١,١١. كشفت شركة الأمن الإلكتروني «فايرآي»[٤٣] عن عدد كبير من حسابات تويتر باللغة الإنجليزية تنتحل صفة شخصيات أمريكية؛ لتبنِّي وجهات نظر مؤيدة لإيران ونشر محتوىً سلبيٍّ عن إسرائيل والمملكة العربية السعودية. بعض هذه الحسابات انتحل شخصية مواطنين أمريكيين حقيقيين، من بينهم مجموعة من المرشحين السياسيين الجمهوريين. وقد استولت هذه الحسابات المزيفة على صور ومحتوى من الحسابات الحقيقية للمرشحين؛ ما يجعل من الصعب التمييز بين الحسابات الحقيقية والمزيفة.

٢,١١. يُضاف إلى ذلك، نشرُ مجموعة من المحتويات المؤيدة لإيران والمعادية للمملكة العربية السعودية في وسائل الإعلام الأمريكية والإسرائيلية، مع ظهور حسابات أخرى للضغط على الصحفيين لتغطية موضوعات محددة. وقد حققت هذه الحملات بعض النجاح، ما دفع وسائل إعلام مختلفة لإجراء مقابلات مع مواطنين من الولايات المتحدة والمملكة المتحدة للحديث عن القضايا السياسية. وقد انتشر هذا النهج الاحتيالي عبر إرسال الرسائل، وأعمدة الضيوف الصحفية، ومنشورات المدونات -في الغالب- إلى منافذ إخبارية محلية أمريكية صغيرة. ويرجع تاريخ العديد من هذه المقالات إلى الفترة من ٢٠١٨ إلى ٢٠١٩، ولكنَّ بعضها يرجع إلى عام ٢٠١٥. ٣,١١. التقييم: تدل هذه الأمور على وجود حملة دعائية محددة، لا بد أنها استغرقت وقتاً طويلاً وسُخِّرت لها مهارات جيدة في اللغة الإنجليزية لتنسيقها. ولا يمثل هذا هجوماً إلكترونيّاً بشكله المعتاد، لكنه يجسد قدرة إلكترونية مهمة. ولا بد أن المُنفِّذين قد بذلوا الكثير من الموارد في البحث في منشورات الهدف ودراسة بياناته الشخصية. وتشير أبحاث «فايرآي» إلى أنه، في إحدى الحالات، تبنَّى الحساب وجهات نظر ضد إيران، ولكنه تحوَّل إلى صفها بعد ذلك، ربما لجذب قاعدة مبدئية من المعجبين من

---

(٤٣) شبكة من حسابات وسائل التواصل الاجتماعي تنتحل صفات مرشحين سياسيين أمريكيين، وتحث وسائل الإعلام الأمريكية والإسرائيلية على دعم المصالح الإيرانية. فايرآي، أليس ريفيلي، لي فوستر. ٢٨ مايو ٢٠١٩.
https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html

الجمهور الأمريكي. وهذا يدل على مستوى محدد من الجهد والتطور لنشر الدعاية، مع وجود تأثير إضافي، هو زعزعة الثقة في مصادر وسائل الإعلام.

١٢. أبريل ٢٠١٩:

قراصنة إيرانيون يشنون هجمات على البنوك وشبكات الحكومة المحلية والهيئات العامة الأخرى في المملكة المتحدة:

١,١٢. تابعت وسائل الإعلام البريطانية المختلفة[٤٤] الهجوم الذي وقع في ديسمبر ٢٠١٨ واستمر حتى أبريل ٢٠١٩ على مكتب بريد المملكة المتحدة، وجهات محلية حكومية أخرى لم يُصرَّح بأسمائها، تشمل شبكاتٍ ومسؤولينَ وبنوكاً. وقد سُرق من مكتب البريد وحده تفاصيل شخصية خاصة بآلاف الموظفين. ولا تُوجد تعليقات رسمية كثيرة على هذه الهجمات، على الرغم من أن العديد من خبراء الأمن الإلكتروني قد نسبوها إلى إيران.

٢,١٢. التقييم: من التقارير القليلة المتاحة، قد يبدو هذا هجوماً يهدف إلى سرقة عدد كبير من بيانات اعتماد المستخدمين، ما يسمح بمزيد من الهجمات الأعمق على المنظمات المستهدفة. علاوةً على ذلك، فإن محاولات شنِّ هجمات على مسؤولين بالمملكة المتحدة ربما تسمح للمهاجم بانتحال شخصياتهم فيما بعد، ما قد يوفر وصولاً أو تأثيراً رسميّاً أعمق على الجمهور البريطاني. وعلى الرغم من أنه من الواضح أن المهاجمين قد حقَّقوا بعض النجاح، فإن هجوماً بهذا الاتساع وعلى هذا النطاق يسهُل اكتشافه؛ فهو يخلق المزيد من «لفت الأنظار» إليه؛ لأنه يستهدف العديد من المنظمات التي من المرجح أن تدقَّ ناقوس الخطر، وتنسق فيما بينها لمواجهة الهجمات، وهذا من شأنه في النهاية أن يحدَّ من فاعليتها.

١٣. أبريل ٢٠١٩:

تسريبات متداولة حول أهداف وأعمال مجموعة إلكترونية إيرانية:

١,١٣. سُرِّبت بيانات غير منسوبة على تطبيق المراسلة «تليجرام» تُقدم تفاصيل عن أدوات وأعضاء

(٤٤) إيران تخترق مؤسسات المملكة المتحدة في هجوم تجسس حكومي.
SC Media: The Cyber-Security source. 3 April 2019
https://www.scmagazineuk.com/iran-infiltrates-uk-institutions-state-spying-attack/article/1581009

وضحايا مجموعة إيرانية معروفة تُدعى «أويل ريج»[٤٥]. وقد اكتشف المجموعةَ لأول مرة باحثو شركة الأمن الإلكتروني الأمريكية «بالوألتو نيتوركس» في مايو ٢٠١٦[٤٦]، وقد صرحوا بأن «مجموعة (أويل ريج) ليست متطورة، لكنها مثابرة في السعي لتحقيق أهداف مهامها. وعلى عكس بعض الخصوم الآخرين الذين يحملون دوافع للتجسس، هم أكثر استعداداً للانحراف عن منهجيات الهجوم الحالية، واستخدام تقنيات جديدة لإنجاز أهدافهم». وفي المجمل، تضمَّن التسريب تفاصيل ١٣٠٠٠ من بيانات اعتماد المستخدمين المسروقة، وغيرها من البيانات المخترقة لكيانات في ٢٧ دولة و٩٧ منظمة و١٨ صناعة.

٢,١٣. التقييم: تركز تقارير وسائل الإعلام عن التسريبات على اختراق كيانات تجارية وحكومية موجودة بالشرق الأوسط، على الرغم من أن تحليل شركة «بالوألتو» أوضح أن هجمات «أويل ريج» عالمية النطاق. وقد تعمل المجموعة على نطاق عالمي، أو تسعى للوصول إلى أطراف ثالثة؛ كالموردين والشركات التابعة لأهدافها الرئيسة في الشرق الأوسط.

١٤. مارس ٢٠١٩:

مجموعة إلكترونية إيرانية تستهدف البنية الأساسية الرقمية الحكومية والصناعية في المملكة العربية السعودية والولايات المتحدة:

١,١٤. قدم خبراء شركة «سيبر سيكيوريتي» تقريراً عن أنشطة مجموعة مرتبطة بإيران تعرف باسم «إلفين»، نشطت منذ أواخر عام ٢٠١٥. وأشارت تقارير شركتي «سيبر سيكيوريتي» وشركة مكافحة الفيروسات «سيمانتك»[٤٧] إلى أن مجموعة «إلفين» تخصصت في البحث عن مواقع الويب التي تحتوي على ثغرات معروفة. وفورَ اكتشاف هذه المواقع، تهاجم «إلفين» المواقعَ نفسها أو تستخدمها بنيةً أساسيةً لشَنِّ المزيد من الهجمات. وقد هاجمت

---

(٤٥) مجموعة قراصنة يكشفون عمليات وأعضاء مجموعة (APT) الإيرانية، أيونوت إيلاسكو، ١٨ أبريل ٢٠١٩.
SC Media: The Cyber-Security source. 3 April 2019
https://www.scmagazineuk.com/iran-infiltrates-uk-institutions-state-spying-attack/article/1581009

(٤٦) وراء الكواليس مع «أويل ريج». براين لي وروبرت فالكون، ٣٠ أبريل ٢٠١٩.
https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/

(٤٧) «إلفين»: مجموعة تجسس قوية تستهدف منظمات متعددة في المملكة العربية السعودية والولايات المتحدة الأمريكية. فريق التحقيق في الهجمات بقسم الاستجابة الأمنية. ٢٧ مارس ٢٠١٩.
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

المجموعة ما لا يقل عن ٥٠ منظمة، ٤٢٪ منها تقع داخل المملكة العربية السعودية، و٣٤٪ داخل الولايات المتحدة. وأهدافها واسعة النطاق، وتشمل: حكوماتٍ، ومؤسساتٍ بحثيةً، ومعظم القطاعات التجارية والصناعية. وقد لاحظت شركة «سيمانتك» أن بعض هذه المؤسسات الأمريكية ربما تكون مستهدفة من «إلفين» لاستخدامها في شن هجمات على سلسلةٍ من سلاسل التوريد. ففي إحدى الحالات، تعرضت شركة أمريكية كبيرة للهجوم في الشهر نفسه الذي تعرضت فيه شركةٌ شرقُ أوسطية مملوكة لها للهجوم أيضاً. وانطلقت هذه الهجمات باستخدام رسائل تصيُّد احتيالي موجَّه على البريد الإلكتروني. وتشير أبحاث «سيمانتك» إلى أن مجموعة الأدوات التي تستخدمها «إلفين» في الهجوم، هي في الغالب للتجسس؛ إذ إن تقنياتها وأدواتها تهدف -بشكل أساسي- إلى الوصول السري إلى الشبكات والأجهزة لسرقة الملفات. ومع ذلك، رُبط أيضاً بين أنشطة مجموعة «إلفين» وفيروس «شمعون» المدمر (أ ١٩).

٢,١٤. التقييم: تُعد مجموعة «إلفين» مهاجماً مثابراً ذا نظرة ثاقبة في استخدام أطراف ثالثة في بلدان أخرى لتنفيذ هجمات على سلاسل التوريد للتأثير على الأهداف الرئيسة. ويشير بحث «سيمانتك» إلى مجموعة من الأدوات والتقنيات التي تمتلكها المجموعة، وإلى أنها تُجري مراجعات مستمرة لتحديث منهجها لمواكبة التطورات التي يشهدها مجال الأمن الإلكتروني. ويبدو أن المجموعة مكلفة بالتجسس، على الرغم من أن «استطلاعاتها الإلكترونية» يمكن أن تضع الأساس لشَنِّ المزيد من الهجمات المدمرة إذا لزم الأمر.

١٥. مارس ٢٠١٩:

جهاز المخابرات الإيراني يخترق الهاتف المحمول لزعيم المعارضة الإسرائيلية:

١,١٥. ذكرت وسائل إعلام إقليمية مختلفة[٤٨] أن إيران اخترقت الهاتف المحمول لزعيم المعارضة في إسرائيل، بيني غانتز، وسرقت منه بيانات شخصية وحساسة. وتدعم وسائل الإعلام ادعاءاتها بالاستشهاد ببيان صادر عن جهاز الأمن الداخلي الإسرائيلي (لم نستطع الوقوف عليه).

---

(٤٨) وكالة الاستخبارات الإسرائيلية تعترف بأن إيران اخترقت هاتف غانتز. ١٦ مارس ٢٠١٩.
https://www.middleeastmonitor.com/20190316-israel-intelligence-agency-admits-iran-hacked-gantzs-phone/

٢,١٥. التقييم: كان هذا قبل الانتخابات الإسرائيلية مباشرةً، ومن المؤكد أن تفاصيل الهجوم قد بُولغ فيها لتحقيق مكاسب سياسية. ومع ذلك، ظهر غانتز نفسه مؤكداً وقوع الحادث من خلال الادعاء بأنه لم تُسرق من هاتفه أي بيانات حساسة. وجه الغرابة أن تقريراً إعلاميّاً آخر أشار إلى أن روسيا[٤٩] تقف وراء الهجوم، رغم أن التقرير لم يُقَدِّم أي أدلة تدعم هذا الادعاء. وما يميز هذا التقرير أنه واحد من التقارير القليلة التي تتحدث عن قيام إيران بتهديد جهاز هاتف محمول، لكنْ، بالنظر إلى عدم وجود تفاصيل، والادعاء غير المعتاد بوقوف روسيا وراء الهجوم، فمن الصعب تقييم مدى أهمية هذا التقرير.

١٦. فبراير ٢٠١٩:

الولايات المتحدة الأمريكية تتهم خبيرةً سابقةً في سلاح الجو الأمريكي بالمساعدة في الهجمات الإلكترونية الإيرانية:

١,١٦. اتهمت حكومة الولايات المتحدة عدة مواطنين إيرانيين، إضافة إلى المتخصصة السابقة في مكافحة التجسس بسلاح الجو الأمريكي، مونيكا ويت[٥٠]، بشنِّ هجمات إلكترونية وارتكاب جرائم تُهدد الأمن القومي. انشقت ويت والتحقت بإيران بعد أن أمضت ١٣ عاماً في سلاح الجو الأمريكي، ولعملها مقاولاً عسكريّاً؛ كان لديها ما يؤهلها لنقل المعلومات الاستخباراتية إلى النظام الإيراني. ومع ذلك، يبدو أن ويت قد اضطلعت بدور أكثر نشاطاً، وعملت مع مجموعة غير معروفة من القراصنة الإيرانيين للسعي إلى اختراق حسابات زملائها السابقين[٥١]. أنشأت المجموعة التي تعمل مع ويت حساباً مزيفاً على «فيسبوك» ينتحل صفة ضابط مخابرات أمريكي حقيقي، ثم أجرت تواصلاً من هذا الحساب مع ضباط مخابرات آخرين، ثم أرسلت إليهم رسائل تحثهم على النقر على روابط تقودهم إلى برامج ضارة. ولا يشير قرار الاتهام إلى ما إذا كان المهاجمون قد نجحوا في اختراق أي أنظمة مستهدفة، غير أن الرسائل التي أرسلوها كانت رسائل بدائية وغير احترافية.

---

(٤٩) روسيا تخترق هاتف غانتز قبل الانتخابات الإسرائيلية. ٢٩ أغسطس ٢٠١٩.
https://www.middleeastmonitor.com/20190829-gantzs-phone-hacked-by-russia-ahead-of-israel-election/

(50) https://en.wikipedia.org/wiki/Monica_Witt.

(٥١) عميلة مكافحة التجسس الأمريكية تساعد إيران في إلقاء قنابل إلكترونية على أمريكا، كما يقول محامو العم سام، ذا ريجيستر، توماس كلابيرن، ١٤ فبراير ٢٠١٩.
https://www.theregister.co.uk/2019/02/14/counterintelligence_agent_espionage/

٢,١٦. التقييم: يُعَدُّ انشقاق شخص مثل ويت انقلاباً كبيراً ومكسباً عظيماً بالنسبة إلى الحكومة الإيرانية. ويمكن للمرء أن يفترض أنها قدَّمت لهم معلومات استخباراتية مهمة تغطي مدة حياتها المهنية. ومن الواضح أن إيران تجاوزت مجرد استخلاص المعلومات منها، وسعت لاستخدامها في دور أكثر نشاطاً للمساعدة في تحديد الهوية للاستهداف المباشر. ومع ذلك، يبدو أن هذه الفرصة قد أُهدرت نظراً للنهج المتبع في التعامل مع الأهداف النهائية، والذي يصطبغ بعدم الاحترافية. ربما يدل هذا على أن ويت قد أُسند إليها فقط مهمة تحديد أسماء الأهداف وصورهم المؤكدة على وسائل التواصل الاجتماعي، ولم يكن لها دور في تنفيذ الهجمات. ولا شك في أن معرفتها بالهدف، مع معرفتها بالثقافة الأمريكية واللغة الإنجليزية كانت ستزيد من احتمالية النجاح.

١٧. يناير ٢٠١٩:

باحثون أمنيون يكتشفون مجموعة إلكترونية إيرانية جديدة:

١,١٧. اكتشفت «فايرآي» مجموعة اختراق إيرانية جديدة[٥٢] تُعرف الآن باسم «شافر»، بدأت ملاحظتها منذ نوفمبر ٢٠١٤. تعطي مجموعة «شافر» الأولوية لاستهداف قطاعي الاتصالات والسفر، وشركات تكنولوجيا المعلومات التي تدعم القطاعين، وصناعة التكنولوجيا الفائقة. وفي تقدير «فايرآي» فإن دور «شافر» يتمثل في تتبُّع أو مراقبة الأهداف التي تهم الدولة الإيرانية؛ من خلال جمع المعلومات الشخصية، بما في ذلك مسارات السفر، وجمع بيانات العملاء من شركات الاتصالات. تستخدم «شافر» المسار المألوف لرسائل البريد الإلكتروني الاحتيالية لسرقة بيانات اعتماد المستخدم من الأفراد، أو استغلال الثغرات الموجودة في خوادم الويب الخاصة بالمنظمات المستهدفة.

(٥٢) APT39: مجموعة تجسس إلكترونية إيرانية تركز على المعلومات الشخصية. سارة هاولي، بن رید، كريستيانا برافمان كيتنر، نالاني فريزر، أندرو تومبسون، يوري روزانسكي، ساناز ياشار، ٢٩ يناير ٢٠١٩.
https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

٢,١٧. وقد نشرت شركة «كاسبرسكاي» بحثاً[٥٣] يغطي فترة خريف عام ٢٠١٨، التي تركزت فيها غالبية هجمات «شافر» داخل إيران فعليّاً. وكان عدد غير معلوم من هذه الهجمات موجهاً ضد كيانات دبلوماسية أجنبية داخل إيران.

٣,١٧. التقييم: يبدو أن لدى «شافر» أولويات واضحة متداخلة مع الجهات الفاعلة الإيرانية الأخرى، على الرغم من انفرادها بالاستهداف الداخلي.

١٨. يناير ٢٠١٩:

تورُّط إيران في حملة عالمية امتدت سنواتٍ لسرقة نظام أسماء النطاقات (DNS):

١,١٨. ذكرت «فايرآي»[٥٤] أن مجموعة نُسبت إلى إيران، أطلقت عليها ميكروسوفت[٥٥] لاحقاً في مارس ٢٠١٩ اسم «إلفين»، استهدفت الآلاف من الموظفين في أكثر من ٢٠٠ دولة في العامَيْن الماضيَيْن. وشملت الأهدافُ الرئيسة صناعةَ النفط والغاز، والآلات الثقيلة، ومزودي الاتصالات، ومزودي البنية الأساسية للإنترنت، والحكومات في المملكة العربية السعودية، وألمانيا، والهند، والمملكة المتحدة، وبعض المناطق في الولايات المتحدة.

٢,١٨. استخدمت الحملة هجوماً جديداً على نظام أسماء النطاقات، وهو النظام الذي يترجم عنوان الويب إلى عنوان بروتوكول الإنترنت الفعلي (IP) للوصول إلى الحواسيب والخدمات عبر البنية التحتية للإنترنت . ونُفِّذَ الهجوم عن طريق التلاعب بنظام أسماء النطاقات الخاص بالمنظمة المستهدفة أو الاستيلاء عليه، من أجل توجيه المستخدمين؛ إما إلى موقع مختلف، أو إلى مسار غير مباشر إلى الوجهة المذكورة. وفيه تُجذَبُ الأهداف إلى وجهة أو مسار خاضع لسيطرة المهاجم، ثم يُخترق النظام الأوسع وتُستخرج البيانات. وقد تمكن المهاجمون من محو البيانات الموجودة على بعض الأجهزة التي اخترقوها.

٣,١٨. التقييم: من المحتمل أن تكون هذه حملةً ناجحةً للغاية من الهجمات الموجهة لسرقة

---

(٥٣) «شافر» تستخدم برمجيات «ريميكسي» الخبيثة للتجسس على الكيانات الدبلوماسية الأجنبية المتمركزة في إيران، دينيس ليجيزو، ٣٠ يناير ٢٠١٩.
https://securelist.com/chafer-used-remexi-malware/89538/

(٥٤) حملة عالمية لسرقة نظام أسماء النطاقات: معالجة سجلات نظام أسماء النطاقات على نطاق واسع. فايرآي. موكس هيراني، سارة جونز ، بن ريد. ١٠ يناير ٢٠١٩.
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

(٥٥) قراصنة إيرانيون يسرقون أسرار الشركات. استهداف ٢٠٠ شركة من شركات النفط، والغاز، وشركات التصنيع. داتا إنسيدر. كريس بروك ، ٧ مارس ٢٠١٩.
https://digitalguardian.com/blog/iranian-hackers-stole-corporate-secrets-200-oil-gas-manufacturing-firms-targeted

بيانات اعتماد المستخدم، والوصول إلى أنواع متعددة من الأهداف. وقد جَرَّبت الهجماتُ المستخدمةُ واختبرت التصيُّدَ الاحتيالي للفرد المستهدف، ولكنْ، نظراً لاستخدام الهجوم الأكثر حداثة على نظام أسماء النطاقات، لم يتطلب الأمر دراسة اجتماعية معقدة لكل هدف على حدة لإقناعه بزيارة الرابط المسموم. كان هذا -على الأرجح- هجوماً بهدف التجسس لسرقة الملكية الفكرية، بالنظر إلى تقرير محو البيانات بغرض التغطية على عملية الاختراق.

١٩. «شمعون»:

أغسطس ٢٠١٢، نوفمبر ٢٠١٦، وديسمبر ٢٠١٨:

١,١٩. «شمعون٣»، ديسمبر ٢٠١٨:

١,١,١٩. في عام ٢٠١٢، أُطلقت واحدة من أكثر الهجمات الإلكترونية تدميراً في التاريخ على شركتَي البتروكيماويات: أرامكو السعودية[٥٦] ورأس غاز القطرية[٥٧]. أُطلق على الهجوم، فيما بعد، اسم «شمعون» نسبةً إلى كلمة وجدها باحثون في مجال الأمن في الشفرة البرمجية الخاصة بالفيروس، وقد أدى «شمعون» إلى تدمير ٣٠,٠٠٠ قرص صلب في أرامكو، وتعطيل هائل للعمليات بسبب الإتلاف شبه الكامل لشبكة تكنولوجيا المعلومات الخاصة بالشركة. يعمل «شمعون»[٥٨] عن طريق الانتشار داخل الشبكة وكتابة بيانات تالفة إلى سجل الإقلاع الرئيس لكل قرص صلب يكتشفه (سجل الإقلاع الرئيس هو أول منطقة (قطاع) قابلة للقراءة على القرص، وهو المسؤول عن تحديد كيفية ومكان وجود نظام التشغيل بحيث يمكن تحميله (إقلاعه) إلى ذاكرة الكمبيوتر). وفي حالة تدمير سجل الإقلاع الرئيس لا يمكن استخدام القرص، وستكون هناك حاجة إلى أدوات فحص متخصصة لاستعادة البيانات المتبقية. وفي هذا الهجوم، احتوت البيانات التالفة على صورة علم أمريكي محترق. وفي النهاية، يرسل «شمعون» للمهاجم تقريراً بعنوان بروتوكول الإنترنت الفعلي (IP) الخاص بكل جهاز مُحيت بياناته، ربما لإحصاء الأجهزة المُدَمَّرة.

---

(٥٦) في هجوم إلكتروني على شركة سعودية، الولايات المتحدة ترى رد إيران. نيويورك تايمز، نيكول بيرلوثوت، ٢٣ أكتوبر ٢٠١٢.
https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

(٥٧) هجوم فيروس غامض يوقف عمليات عملاق الغاز القطري رأس غاز، ذا ريجيستر، جون ليدن، ٣٠ أغسطس ٢٠١٢.
https://www.theregister.co.uk/2012/08/30/rasgas_malware_outbreak/

(58) W32.Disttrack.B, Symantec Security Centre, 23 November 2016
https://www.symantec.com/security-center/writeup/2016-112300-5555-99

٢,١,١٩. وقع الهجوم على الشركتين خلالَ شهر رمضان المبارك، على الأرجح لأن المهاجمين كانوا يعتقدون أن كثيرين من العمال سيكونون في إجازة. أما شركة أرامكو السعودية، فالاعتقاد السائد، هو أن الهجوم وصل أولاً إلى الشبكة عن طريق موظف نقر على رابط في رسالة تصيُّد احتيالي موجه على البريد الإلكتروني، لكنَّ المحققين ما زالوا لا يعرفون وقت إرسال الرسالة أو محتواها على وجه التحديد.

٣,١,١٩. على الرغم من تدمير شبكات الشركتين، لم تُهاجَمْ أنظمة التحكم الصناعي واستمر الإنتاج؛ فرغم حدوث خلل كبير كان لا بد من استمرار العمليات الإدارية المتعلقة بمتابعة وتوزيع الإنتاج دون الاعتماد على تكنولوجيا المعلومات. وقد أجرى موقع الأمن الإلكتروني «دارك ريدنج»[٥٩] مقابلة مع كريس كوبيكا، المستشارة التي عملت في قسم الاستجابة الأمنية بشركة أرامكو السعودية، والتي ذكرت أن أرامكو السعودية استثمرت بكثافة في تأمين أنظمة التحكم الصناعي من الهجمات الإلكترونية، لكنَّ المهاجمين شلُّوا حركة الشركة من خلال استهداف أجهزة الكمبيوتر المكتبية وخوادم البريد، وغيرها من الأنظمة التي تعمل تحت نظام ويندوز. خلال الهجمات، أصدرت مجموعة تُطلق على نفسها «سيف العدالة القاطع»، بياناً تشير فيه إلى سبب الهجوم؛ وهو دعم أرامكو السعودية للأسرة المالكة: آل سعود. ويتفق مجتمع أمن المعلومات على أن هذه المجموعة، هي فاعلٌ إلكترونيٌّ غيرُ معروف يعمل لصالح إيران.

٢,١٩. «شمعون٢»:

١,٢,١٩. في نوفمبر ٢٠١٦ ذكرت شركة الأمن الإلكتروني «سيمانتك»[٦٠] أن فيروس «شمعون» قد عاود الظهور مرة أخرى، ويستهدف هذه المرة أهدافاً متعددة غير معلومة داخل المملكة العربية السعودية. وتعتقد «سيمانتك» أن هذا الإصدار من «شمعون» «لم يتغير إلى حد كبير» عن الإصدار السابق، غير أنه استخدم هذه المرة صورة لجثة طفل سوري لاجئ

(٥٩) ما بعد الكارثة في حادثة اختراق شركة أرامكو السعودية، موقع «دارك ريدنج»، فهميدة ي. راشد، ٨ أغسطس ٢٠١٥.
https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676

(٦٠) شمعون: يُبعث بعد موات ليدمر من جديد، قسم الاستجابة الأمنية بشركة «سيمانتك»، ٣٠ نوفمبر ٢٠١٦.
https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever

غرق في البحر المتوسط في عام ٢٠١٥. وعلى غرار هجوم «شمعون» الأول، ضُبط توقيت الهجوم لينطلق بعد أن عاد معظم الموظفين إلى منازلهم لقضاء عطلة نهاية الأسبوع في السعودية. وهناك أيضاً اتفاق بين شركات أمن إلكترونية أخرى[٦١] على أن مرتكبي الهجوم تمكنوا من الوصول إلى الشبكات المستهدفة قبل إطلاق «شمعون»، وذلك باستخدام بيانات اعتماد المستخدم التي استطاعوا الاستيلاء عليها؛ لتوسيع نطاق الوصول.

٣,١٩. «شمعون٣»:

١,٣,١٩. في ديسمبر ٢٠١٨ اكتُشف فيروس «شمعون» مرةً أخرى[٦٢]، وقد اكتُشف في البداية في شبكات شركة الخدمات البتروكيماوية الإيطالية «سايبم»، التي ذكرت أن فيروس «شمعون» «قد مسح ملفات من ٣٠٠-٤٠٠ خادم، وما يصل إلى ١٠٠ جهاز كمبيوتر من إجمالي ٤٠٠٠ جهاز تقريباً». وقالت الشركة: إن الهجوم أثَّر بشكل أساسي على الخوادم في الشرق الأوسط، بما في ذلك المملكة العربية السعودية، والإمارات العربية المتحدة، والكويت، إلى جانب بعض الأجهزة في الهند وأسكتلندا. ومن بين عملاء شركة «سايبم»: شركة أرامكو السعودية. وبشكل منفصل، ذكرت شركة «سيمانتك»[٦٣] أن منظمات بتروكيماوية غير مسماة في المملكة العربية السعودية والإمارات العربية المتحدة قد تعرضت للهجوم، غير أن التقارير لم تتطرق إلى مدى الضرر.

٢,٣,١٩. في الإصدار الأخير منه، استخدم «شمعون» مرة أخرى أسلوب إتلاف الأقراص الصلبة، واستخدم بيانات اعتماد المستخدم المسروقة لينتشر عبر الشبكات. وفي هذه المرة، لا يوجد أي تقرير يفيد بأنه يترك صورة خلفه. هذا الإصدار من «شمعون» أكثر فاعلية أيضاً في محو البيانات؛ فهو يُتلف سجل الإقلاع الرئيس كالإصدارَيْن السابقين منه؛ ما يجعل محرك الأقراص غير قابل للاستخدام، ولكنَّ هذا الإصدار تضمَّن وظيفة إضافية

---

(٦١) شمعون٢: عودة فيروس «ديستراك» الماحي، شبكة «بالوألتو»، روبرت فالكون، ٣٠ نوفمبر ٢٠١٦.
https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/

(٦٢) هجمات «شمعون٣» تستهدف عدة قطاعات، سيكيوريتي ويك، إدوارد كوفاكس، ١٧ ديسمبر ٢٠١٨.
https://www.securityweek.com/shamoon-3-attacks-targeted-several-sectors

(٦٣) «شمعون»: تهديد مدمر يعاود الظهور، مزوداً بلدغة جديدة في ذيله، فريق التحقيق في الهجمات بقسم الاستجابة الأمنية، ١٤ ديسمبر ٢٠١٨.
https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail

لمسح الملفات من محتويات القرص بالكامل. وعلى الرغم من أن القرص الصلب الذي هاجمه «شمعون١» قد يكون غير قابل للاستخدام، فإن الملفات الموجودة عليه قد تكون قابلة للاسترداد باستخدام أدوات الفحص. أما الملفات التي يُزيلها هذا الإصدار الجديد من «شمعون»، فإن استردادها يصبح مستحيلاً.

٣,٣,١٩. التقييم: هاجم الإصدارُ الأول من «شمعون» هدفَيْن في الشرق الأوسط، وهاجم الإصدارُ الثاني أهدافاً متعددة في المملكة العربية السعودية، وهاجم الإصدارُ الثالث أهدافاً رئيسة في الشرق الأوسط، وهاجم كذلك مورِّدي تلك الأهداف في أوروبا، فيما قد يكون هجوماً على سلسلة التوريد. وبصفة عامة، تطلبت الإصدارات الثلاثة الوصول إلى شبكات أهدافها، وقد حصلت عليها -على الأرجح- عن طريق هجوم تصيُّد احتيالي غير احترافي. ومع ذلك، فقد لاحظ الباحثون الأمنيون أن استطلاعاتٍ إلكترونيةً مهمةً قد أُجريت على الشبكة، ربما لسرقة المزيد من بيانات اعتماد المستخدمين للسماح بوصول أكبر. وقد أصبحت عمليات استهداف «شمعون» أكثر تطوراً، وكذلك قدرته على التسبب في إحداث الأضرار.

٤,٣,١٩. على عكس العديد من الهجمات، لم يتم الربط بين «شمعون» وبين فاعل إلكتروني إيراني معروف بعينه. ومع ذلك، لاحظت شركة «سيمانتك» أن أحد أهداف «شمعون» في المملكة العربية السعودية، في أحدث هجماته، قد هاجمته أيضاً مجموعة «إلفين» مؤخراً؛ ما يشير إلى وجود صلة بين هذين الهجومَيْن على هذه المنظمة لقُربهما، وربما تكون مهمة مجموعة «إلفين» استطلاع الشبكة وتزويد «شمعون» بإمكانية الوصول إليها. ولا يعني هذا بالضرورة أن «إلفين» تقف وراء هجمات «شمعون»؛ لأن «إلفين» ربما تكون عاملة مع مجموعة أخرى غير معروفة، وربما تكون بالفعل جزءاً من منظومة تضم المجموعات المهاجمة.

مركز الملك فيصل للبحوث والدراسات الإسلامية

تأسّس المركز سنة ١٤٠٣هـ/١٩٨٣م لمواصلة الرسالة النبيلة للملك فيصل بن عبدالعزيز -رحمه الله- في نشر العلم والمعرفة بين المملكة وبقية دول العالم. ويعدُّ المركز منصةَ بحثٍ تجمع بين الباحثين والمؤسسات لحفظ العمل العلمي ونشره وإنتاجه، وإثراء الحياة الثقافية والفكرية في المملكة العربية السعودية، وبناء جسرٍ للتواصل شرقاً وغرباً. ويرأس مجلس إدارة المركز صاحب السمو الملكي الأمير تركي الفيصل بن عبدالعزيز، وأمينه العام هو الدكتور سعود بن صالح السرحان.

ويقدّم المركز تحليلات متعمّقة حول قضايا الدراسات الأمنية والسياسية المعاصرة، والاقتصاد السياسي، ودراسات إفريقيا، والدراسات الآسيوية. ويتعاون المركز مع مؤسسات البحث العلمي المرموقة في مختلف دول العالم، ويضمّ نخبةً من الباحثين المتميّزين، وله علاقة واسعة مع عددٍ من الباحثين المتخصّصين في مختلف المجالات البحثية. ويحتضن المركز مكتبة الملك فيصل، ومجموعة مخطوطات نادرة، ومتحفاً إسلامياً، وقاعة الملك فيصل التذكارية، وبرنامج الباحثين الزائرين. ويهدف المركز إلى توسيع نطاق المؤلَّفات والبحوث الحالية لتقديمها إلى صدارة المناقشات والاهتمامات العلمية، متّبعاً مساهمة المجتمعات الإسلامية في العلوم الإنسانية والاجتماعية والفنون والآداب قديماً وحديثاً.

مركز الملك فيصل للبحوث والدراسات الإسلامية
King Faisal Center for Research and Islamic Studies

ص.ب ٥١٠٤٩ الريـــــاض ١١٥٤٣ المملكة العربية السعودية
هاتف: ٤٦٥٢٢٥٥ (١١ ٩٦٦+) تحويلة: ٦٨٩٢ - فاكس: ٤٦٥٩٩٩٣ (١١ ٩٦٦+)
بريد إلكتروني: research@kfcris.com