عمار الحديثي | نشر في ٢٦ أبريل ٢٠٢١,

كيف انخرط القراصنة في حرب مذاهب الشرق الأوسط؟

في منطقة تعج بكل أنواع الصراعات المذهبية والعرقية والقومية والإقليمية، تدور حرب أخرى بعيدًا عن جبهات القتال، يقودها قراصنة من كل بلاد الأرض، وطنيون، مرتزقة، محترفون، مأجورون وهواة.

تقرير لموقع Shadows Digital كشف أكثر من 2.57 مليون هجوم تصيُّد في جميع أنحاء الشرق الأوسط، من مصر إلى الإمارات العربية المتحدة والمملكة العربية السعودية وقطر والكويت والبحرين وعمان. تتنوع هذه الهجمات بين هجمات حكومات على بعضها، وحكومات على أفراد ومؤسسات أو العكس، وبالطبع لا يمكن ذكر الحرب السيبرانية في الشرق الأوسط، دون ذكر أعمدتها الثلاثة: إيران، "إسرائيل" والسعودية.

في 11 أبريل/ نيسان 2021، شنت "إسرائيل" هجومًا سيبرانيًا على منشأة نطنز النووية في إيران، وقع الهجوم بعد ساعات من إعادة المسؤولين في مفاعل نطنز تشغيل أجهزة الطرد المركزي المتقدمة التي يمكن أن تسرع إنتاج اليورانيوم المخصب، فيما وصف بأنه لحظة محورية في البرنامج النووي للبلاد. حاولت السلطات الإيرانية التعامل مع انقطاع التيار الكهربائي واسع النطاق في نطنز، والذي اعترفت وكالة الطاقة الذرية الإيرانية أنه ألحق أضرارًا بشبكة الكهرباء في الموقع. يمثل هذا الهجوم حلقة من عدة هجمات شنتها "إسرائيل" -منفردة أو مع المخابرات الأميركية- على البرنامج النووي الإيراني. ولعل أبرز هذه الهجمات كانت عملية ستوكسنت (Stuxnet) عام 2010.

ما هي عملية ستوكسنت؟

هي دودة كمبيوتر كانت تستهدف في الأصل المنشآت النووية الإيرانية وتحولت منذ ذلك الحين وانتشرت إلى منشآت صناعية وإنتاجية أخرى. استهدفت عملية ستوكسنت الأصلية وحدات التحكم المنطقية

القابلة للبرمجة (PLCs) المستخدمة لأتمتة عمليات الجهاز. تولدت موجة من الاهتمام الإعلامي بعد اكتشافها في عام 2010، لأنها كانت أول فيروس معروف قادر على تعطيل الأجهزة، ولأنه يبدو أنه تم إنشاؤه من قبل وكالة الأمن القومي الأميركية ووكالة المخابرات المركزية والمخابرات الإسرائيلية.

دمّرت ستوكسنت العديد من أجهزة الطرد المركزي في منشأة نطنز لتخصيب اليورانيوم الإيرانية من خلال التسبب في حرق نفسها. مع مرور الوقت، قامت مجموعات أخرى بتعديل الفيروس لاستهداف المنشآت بما في ذلك محطات معالجة المياه ومحطات الطاقة وخطوط الغاز. كانت ستوكسنت عبارة عن دودة متعددة الأجزاء تنتقل على أقراص USB وتنتشر عبر أجهزة كمبيوتر بنظام تشغيل مايكروسوفت ويندوز. قام الفيروس بالبحث في كل جهاز كمبيوتر مصاب لإيجاد علامات على برنامج Step 7 Siemens، والذي تستخدمه أجهزة الكمبيوتر الصناعية التي تعمل كمكون لأتمتة المعدات الكهربائية والميكانيكية ومراقبتها.

بعد العثور على الكمبيوتر، قام البرنامج بتحديث رمزه عبر الإنترنت والبدء في إرسال تعليمات مسبّبة للتلف إلى المعدات الكهروميكانيكية التي يتحكم فيها الكمبيوتر. في الوقت نفسه، أرسل الفيروس ملاحظات خاطئة إلى وحدة التحكم الرئيسية، وأي شخص يراقب المعدات لن يكون لديه أي مؤشر على وجود مشكلة حتى تبدأ المعدات بالتدمير الذاتي.

يمكن اعتبار عملية ستوكسنت أنها أول غارة سيبرانية كبيرة تضرب المنطقة بهذا الحجم، ليبدأ بعدها توظيف القراصنة في الصراع الذي اندلع عقب ثورات الربيع العربي: تارة ضد الناشطين، تارة بين دولة وأخرى، وتارة عمليات يقوم بها اللصوص.

منذ هجوم ستوكسنت الصاعق، طورت إيران الكثير من مجموعات القراصنة الذين نفذوا عمليات عديدة ضد الدول المجاورة بما فيها "إسرائيل".

تقول روكسان فارمانفرمايان، وهي مديرة العلاقات الدولية والدراسات العالمية في معهد التعليم المستمر في جامعة كامبريدج: "كان لدى المملكة العربية السعودية وإيران مقاربتان مختلفتان تمامًا للحرب الإلكترونية.

اختارت المملكة العربية السعودية الاستعانة بمصادر خارجية لمعظم عمليات التطوير السيبراني، وشراء أدوات مخصصة من متعاقدين من القطاع الخاص في الولايات المتحدة و"إسرائيل" والمملكة المتحدة لإجراء عمليات إلكترونية محددة.

كما استخدمت المملكة العربية السعودية فيالق من الروبوتات (الحسابات الوهمية أو ما يُطلق عليه الذباب) لتعزيز صورة المملكة على وسائل التواصل الاجتماعي في أوقات الأزمات، خاصة بعد مقتل جمال خاشقجي. في الوقت نفسه، حاولت المملكة تعزيز دفاعاتها الإلكترونية، لا سيما من خلال إنشاء بنية تحتية مؤسسية واسعة للتعامل مع الأمن السيبراني.

في عام 2017، بدأ ذلك بإطلاق الهيئة الوطنية للأمن السيبراني، وهي هيئة سعودية مكافئة للقيادة السيبرانية الأميركية تحت السلطة المباشرة لمكتب الملك، وكذلك الاتحاد السعودي للأمن السيبراني والبرمجة والطائرات من دون طيار، وهي منظمة تحت رعاية اللجنة الأولمبية السعودية تقود مهمة بناء مجموعة من المحاربين السيبرانيين السعوديين المهرة".

في غضون ذلك، تقول فارمانفرمايان، طورت إيران برنامجها الهجومي المتكامل والمتعدد القواعد. بسبب العقوبات ووضعها الدولي تحت الحصار، كان برنامجها محلي في الغالب، على الرغم من بعض المساعدة من روسيا والصين.

في عام 2013، التزمت الصين بمساعدة إيران على تطوير شبكة إنترنت وطنية، تُعرف باسم شوما، وهي

مستقلة عن شبكة الويب العالمية، وهي شراكة يتوقع أن تتوسع باتفاق أمني مدته 25 عامًا تتفاوض الدولتان فيه حاليًا. ساهمت التطورات الإيرانية الميدانية في تعزيز مكانتها كواحدة من أكثر القوى الإلكترونية تقدمًا في المنطقة.

الحرس السيبراني الإيراني

منذ هجوم ستوكسنت الصاعق، طورت إيران الكثير من مجموعات القراصنة الذين نفذوا عدة عمليات ضد الدول المجاورة بما فيها "إسرائيل". تصنف هذه المجاميع ضمن ما يعرف بـ"مجاميع التهديد المتقدم" (Threats Persistent Advanced) أو ما يعرف اختصارًا بـ"APT"، وهي فرق سيبرانية منتشرة حول العالم تعتبر من أشد التهديدات الالكترونية.

وهذه أبرز المجاميع الإيرانية:

APT33

لها أسماء متعددة، تُعرف أيضًا باسم فريق Kitten Refined Elfin، Holmium Magnalium، ويعتقد أن APT33 قد تشكّل في عام 2013.

تُسب إلى الفريق عدد من الهجمات على أهداف في الولايات المتحدة وكوريا الجنوبية والمملكة العربية السعودية، لا سيما المنظمات العاملة في صناعات الفضاء والدفاع والبتروكيماويات. حدثت إحدى الحملات الأخيرة البارزة عام 2019، والتي شهدت استهداف العديد من الشركات السعودية.

تستخدم المجموعة مجموعةً من أدوات البرامج الضارة، وتفضّل تلك التي يمكنها مسح محركات الأقراص الثابتة أو تثبيت الأبواب الخلفية Backdoor Encryption. وقد شاركت أيضًا في عمليات تصيّد احتيالي كبيرة، وسجلت عدة حالات لعمليات قرصنة تنتحل فيها شخصية الشركات البارزة.

تم تحديد APT39 لأول مرة في أواخر عام 2018، ولكن يعتقد أنها كانت نشطة منذ عام 2014.

APT34

تعرف APT34 أيضًا باسم Rig Oil وKitten Helix، وهي واحدة من أبرز مجموعات APT التي يعتقد أنها مدعومة من الحكومة الإيرانية.

بعد أن نشطت منذ عام 2014، شنت مجموعة من الهجمات ضد البنية التحتية الوطنية الحيوية في العديد من البلدان، بما في ذلك الإمارات العربية المتحدة والأردن والبحرين. وشملت أهدافها المطارات والوكالات الأمنية ومقدمي الطاقة والمؤسسات الحكومية.

تستخدم المجموعة ترسانة من أدوات القرصنة للتسلل إلى الشبكات، بما في ذلك العديد من البرامج الضارة وأدوات التصيّد، بالإضافة إلى تدوين المفاتيح وأدوات تفريغ بيانات الاعتماد وطرق التجميع الآلي للوصول.

ومع ذلك، تعرضت APT34 لضربة كبيرة في عام 2019 عندما تم الكشف عن عدد كبير من البيانات التي يعتقد أنها تفصّل قيادة APT34 عبر تطبيق تيليغرام. تضمّن التسريب تفاصيل عن 10 أفراد، ثلاثة منهم يعملون في وزارة المخابرات الإيرانية، بينما يعمل الباقون في شركة راهاكورب الإيرانية للأمن السيبراني.

APT39

تم تحديد APT39 لأول مرة في أواخر عام 2018، ولكن يُعتقد أنها كانت نشطة منذ عام 2014، وتعتبر مجموعة تجسس إلكتروني نظرًا إلى تركيزها على سرقة المعلومات الشخصية.

تستهدف بشكل أساسي قطاع الاتصالات وشركات السفر وتكنولوجيا المعلومات التي تدعمها وقطاع التكنولوجيا الفائقة، وقد ركزت حملات APT39 على الشركات في الولايات المتحدة وتركيا وإسبانيا ومصر والعراق والإمارات العربية المتحدة والمملكة العربية السعودية.

يعتقد أن المجموعة تستخدم أدوات قرصنة جاهزة لإجراء عمليات تتبع ومراقبة ضد أفراد رئيسيين، بطريقة أدت بالخبراء إلى الاعتقاد بأنها تقوم على الأرجح بنشاط تجسس لصالح الحكومة الإيرانية.

المجموعة مرتبطة أيضًا باختراق شبكة HBO التي شهدت تسريب نصوص لحلقات مسلسل Game of Thrones على المقننة غير الإنترنت.

"الهرة الساحرة"

تعرّف تشارمينغ كيتن (Kitten Charming) أيضًا باسم APT35 وPhosphorus وSecurity Ajax وNewsBeef، وهي واحدة من أكثر مجموعات APT شهرة في إيران، على الرغم من اعتبارها تستخدم تقنيات غير متطورة نسبيًا.

يعتقد أن المجموعة كانت نشطة منذ عام 2014، وتستخدم مزيجًا من عمليات الاستغلال غير المباشرة والبرامج الضارة والتصيّد وتقنيات الهندسة الاجتماعية، لسرقة البيانات من الأفراد في الوكالات الحكومية والشركات العاملة في التكنولوجيا والجيش والدبلوماسية. تتمركز معظم الأهداف في الولايات المتحدة و"إسرائيل" والمملكة المتحدة.

على وجه الخصوص، اتهمت تشارمينغ كيتن باستهداف الأفراد المتورطين في اتفاق إيران النووي؛ استهداف حملة رئاسية أميركية لم يتم تسميتها ومحاولة سرقة البيانات من الصحافيين والمسؤولين الحكوميين والإيرانيين المختارين الذين يعيشون في الخارج.

المجموعة مرتبطة أيضًا باختراق شبكة HBO الذي شهد تسريب نصوص لحلقات مسلسل Game of Thrones على الإنترنت.

مجموعة الـ"ساطور"

تم تحديد مجموعة كليفر (Cleaver) لأول مرة في عام 2014، وهي مجموعة APT مسؤولة عن عملية كليفر، وهي حملة منسقة حددها Cylance وبدأت في عام 2012 وقد لا تزال مستمرة.

تستهدف المنظمات في 16 دولة منها الولايات المتحدة و"إسرائيل" والصين والهند وفرنسا والمملكة المتحدة والمملكة العربية السعودية، ومن بين ضحايا عملية كليفر المنظمات العسكرية وشركات الطيران وعمالقة صناعة الطاقة.

تضمنت هجمات كليفر، التي يبدو أنها ركزت على سرقة البيانات، إنشاء ملفات تعريف لينكدإن وهمية لتسهيل انتشار البرامج الضارة.

تم ربط التنظيم بالحرس الثوري، على الرغم من أن الحكومة الإيرانية نفت رسميًا مشاركتها في حملة عملية كليفر.

CopyKittens

مجموعة أخرى من APT مقرها إيران تركز على نشاط التجسس، تم تحديد كوبي كيتنز (CopyKittens) لأول مرة في عام 2015 ويعتقد أنها تعمل منذ عام 2013.

باستخدام مجموعة مختارة من أدوات البرمجيات الخبيثة الجاهزة والمخصصة للوصول إلى الأنظمة وتشفير البيانات وسرقتها، هاجمت المجموعة بشكل أساسي أهدافًا استراتيجية في دول مثل الولايات

المتحدة والأردن وتركيا و"إسرائيل" والمملكة العربية السعودية وألمانيا. وقد ركزت عادةً على المؤسسات الحكومية والأكاديمية، فضلًا عن شركات الدفاع وتكنولوجيا المعلومات. تشتهر كوبي كيتنز بشكل خاص بحملتها العملية Tulip Wilted، وهي حملة تجسس إلكتروني واسعة النطاق تستهدف المنظمات الحكومية.

ليفمينر

يعتقد أن مجموعة ليفمينر (Leafminer) نشطة منذ عام 2017، وتشارك أيضًا في أنشطة التجسس الإلكتروني، إلا أنها تركز بشكل خاص على المنظمات في الشرق الأوسط.

تستهدف ليفمينر عددًا كبيرًا من الصناعات، بما في ذلك البتروكيماويات والاتصالات والمالية والشحن وشركات الطيران، فضلًا عن المؤسسات الحكومية، وقد ركزت أنشطتها في دول بما في ذلك المملكة العربية السعودية ولبنان و"إسرائيل" والكويت.

يعتقد أن المجموعة تستخدم مزيجًا من البرامج الضارة المخصصة والمتاحة على نطاق واسع للوصول المستمر إلى الأجهزة وسرقة البيانات.

"المياه الموحلة"

بعد أن نشطت مجموعة التجسس الإلكتروني مودي ووتر (Water Muddy) منذ عام 2017، ركزت بداية على الشرق الأوسط، ولا سيما المملكة العربية السعودية ولبنان وسلطنة عمان، ولكنها وسّعت أيضًا من جهودها لاستهداف المنظمات الأوروبية وأميركا الشمالية.

مع التركيز على سرقة البيانات، استهدفت المجموعة المنظمات ليس فقط عبر الحكومة والاتصالات والنفط، ولكن أيضًا العملات المشفرة.

يشير صعود ونجاح عصابات برامج الفدية ذات نموذج الابتزاز المزدوج المربحة للغاية مثل Maze وEgregor وSodinokibi وNetwalker إلى أن هجمات برامج الفدية المستهدفة ستستمر لتصبح مصدر قلق أمني أكبر لشركات الشرق الأوسط.

خسائر ضخمة وتهديد كبير

وفقًا لدراسة أجرتها وكالة IBM security، يتجاوز معدل الخسائر للهجوم السيبراني الناجح في خرق البيانات الـ 6 ملايين دولار، وهو ضعف متوسط الخسائر من الحوادث العادية. يكمن سبب ارتفاع معدل الخسائر إلى انتشار الرقمنة في أغلب القطاعات الحيوية في المنطقة، وهو ما يعرض تلك القطاعات للاختراق. لا تنحصر الخسائر في الأضرار الناتجة عن الاختراقات وحسب، يضاف إليها تكاليف التأمين الإلكتروني التي تتم عادة من قبل ما يسمى بـ"القراصنة البيض".

وفي منطقة غنية بالثروات، تغيب عنها السياسات الوطنية في كثير من البلدان، تحولت الحرب السيبرانية إلى معارك تكسير عظام بين الدول المتناحرة، وأثّر ذلك بشكل كبير أيضًا على الناشطين والصحافيين الذين وجدوا أنفسهم في مواجهة إمكانات كبيرة للتجسس عليهم. بالإضافة إلى انتهاكات البيانات وتكتيكات التصيد، يواجه مسؤولو الأمن السيبراني المزيد من الهجمات مثل خروقات حسابات وسائل التواصل الاجتماعي وهجمات ما يسمى بـ"الفدية" التي تسعى إلى ابتزاز مبالغ كبيرة أو بيانات حساسة من ضحاياها.

في العام 2020، شهدت بداية يناير/ كانون الثاني تغطية دولية لحادثتي قرصنة علنيتين. أوّلا، تم اختراق حساب وكالة الأنباء الكويتية (كونا) الحكومية على تويتر بتغريدة تخبر الجماهير أن القوات الأميركية تعتزم الانسحاب من قاعدة عريفجان في غضون ثلاثة أيام. وفي شهر يناير/ كانون الثاني 2020 نفسه، كشفت

شركة عمان المتحدة للتأمين ش.م، أكبر شركة تأمين في عُمان، عن هجوم "فدية" على مركز بياناتها أدى إلى تعليق العمليات لمدة يوم واحد. كشفت الشركة أن مجرمي الإنترنت حصلوا على بيانات العملاء من ديسمبر/ كانون الأول 2019 إلى يناير/ كانون الثاني 2020 لكنهم لم يعلنوا عن خسائر مالية أو تداعيات الاختراق.

في الفترة من يونيو/ حزيران إلى سبتمبر/ أيلول 2020 ، تم الكشف عن خمس شركات شرق أوسطية (الإنشاءات والتصنيع والهندسة والتكنولوجيا على التوالي) كضحايا على الموقع الإخباري المظلم Maze إلى أيلول /سبتمبر من ،ذلك إلى بالإضافة .Maze الفدية برامج لعصابة بيانات ابتزاز موقع وهو ،News نوفمبر/ تشرين الثاني من عام 2020، تم تسمية أربع شركات أخرى (الخدمات المهنية، البيع بالتجزئة، التصنيع وصناعات الرعاية الصحية) على الصفحة الرئيسية لـ News Egregor، وهو مماثل لبرامج الفدية لـ Maze زاد من وتيرة الهجمات وتعقيدها في وسط وقف عمليات .

يشير صعود ونجاح عصابات برامج الفدية ذات نموذج الابتزاز المزدوج المربحة للغاية مثل Maze وEgregor وSodinokibi وNetwalker إلى أن هجمات برامج الفدية المستهدفة ستستمر لتصبح مصدر قلق أمني أكبر لشركات الشرق الأوسط. عمليات ابتزاز لم تسلم منها شركة آبل نفسها، بعدما هددتها إحدى عصابات القرصنة بنشر بيانات تتعلق بخططها المستقبلية في حال لم تدفع لها الشركة 50 مليون دولار نظير السكوت عن تلك الخطط. فهل كان ما ينقص الشرق الأوسط تهديد جديد يدخل إلى كل منزل وكل هاتف أو كومبيوتر محمول؟!

رابط المقال: https://www.noonpost.com/40498/