الأنباء
الاربعاء 27 مايو 2015

### نائب رئيس «FireEye» لمنطقة الشرق الأوسط وتركيا وأفريقيا أكد أن الشركة تتعامل مع التهديد الإلكتروني خلال دقائق

# كافيتي لـ «الأنباء»: ميليشيات إلكترونية تمولها إيران والجيش السوري تستهدف المصالح الحيوية في دول الخليج خاصة المنشآت النفطية

أجرى اللقاء: أسامة ابوالسعود

**كشف نائب رئيس شركة FireEye لمنطقة الشرق الأوسط وتركيا وأفريقيا راي كافيتي خلال لقاء مع «الأنباء» عن اتهامات واضحة لميليشيات الكترونية تمولها ايران والجيش السوري لاستهداف المصالح الحيوية في دول الخليج خاصة المنشآت النفطية. لافتا الى ان ذلك هو ما أثبتته عملية القرصنة والهجوم الإلكتروني على شركة أرامكو السعودية ومصالح قطرية في العام 2012. مؤكدا ان عملية القرصنة التي تمت باسم «شمعون» كان مصدرها ايران التي تجند متخصصين لاستهداف المصالح الخليجية. واوضح ان الامر لا يتوقف عند ايران فقط فإسرائيل واميركا واوروبا الوسطى كلها تستهدف دول الخليج لـ 3 أسباب هي: اولا الموارد النفطية والغاز والبترول، وثانيا الأشخاص أصحاب الثروات الضخمة جدا، وثالثا السياسة الخارجية للسيطرة على بعض الجماعات الموجودة داخل الدول. وتحدث كافيتي عن التعاون مع شركة «نوف اكسبو» مؤكدا انها تساعدنا في عقد مؤتمرات توعية، لان الهجمات الالكترونية الخبيثة والجديدة هي شكل جديد على الحكومات والأفراد وبالتالي يجب توعيتهم وتعريفهم بهذه الڤيروسات الخبيثة اولا بأول قبل ان يعرفوا ما الحلول. لافتا الى ان الخلايا الخبيثة كانت تخترق الشبكات وتظل داخلها من 8 الى 9 اشهر من قبل دون ان يشعر بها احد لتحقيق اهدافها التي قد تكون سياسية او امنية او تجسسية، ولكن دائما يكون الهدف تخريبيا. مشددا على انه وبعد تعامل FireEye اصبح الوضع مختلفا جدا، حيث قلصت FireEye بقاء هذه الخلايا من 9 اشهر الى دقائق فقط ويتم التعامل معها فورا وكشف مصدر الهاكرز. والى تفاصيل اللقاء:**

## عملية القرصنة والهجوم الإلكتروني على شركة أرامكو السعودية مصدرها إيران

راي كافيتي متحدثا للزميل اسامة ابوالسعود

عبداللطيف السريع مع راي كافيتي ونانسي اسعد (ريليش كومار)

بداية هناك تعاون بين شركة FireEye والجهاز المركزي لتكنولوجيا المعلومات في الكويت من اجل تحصين شبكة المعلومات الكويتية من الاختراق من قبل الهاكرز، كيف تنظرون لهذا التعاون؟

● **كل دولة من دول الشرق الأوسط مستهدفة من قبل قراصنة الكترونيين، وهدفهم قد يكون سياسيا او امنيا او تجسسيا، ولكن دائما الهدف تخريبي. وهو زرع خلية داخل الشبكة المستهدفة بإرسال المعلومات الى القائد العام، وانا هنا اتحدث بشكل حقيقي عما يحدث عن طريق المجال الالكتروني، وهذه الخلية تنتشر داخل الشبكة لتصل الى الغاية التي ارسلت من اجلها ويمكن وصفها بـ «الهدف المستهدف» وتقوم بإرسال المعلومات التي تم اختراقها لمركز التحكم الخاص بتلك الخلية. وهذه الخلية تظل داخل الشبكة من 8 الى 9 اشهر دون ان يشعر بها احد، وهنا تقوم الأجهزة الحساسة المعنية في الدول مثل الاستخبارات ووزارات الداخلية والأمن القومي والشؤون العسكرية واجهزة مواجهة الجريمة الإلكترونية بمواجهة هذه الأمور.**

كيف يمكن اكتشاف تلك الخلايا التجسسية بعد 9 اشهر من العمل واختراق الأجهزة والمعلومات المهمة؟

● **هذا كان يحدث قبل FireEye، اما بعد تعامل FireEye فأصبح الوضع مختلفا جدا، حيث قلصت FireEye بقاء هذه الخلايا من 9 اشهر الى دقائق فقط، ما بين دقيقتين الى 7 دقائق، وتقوم بتنظيف النظام كاملا، وهو ما كان يحدث من قبل خلال 9 اشهر واصبح الآن في دقائق مع FireEye.**

خلال تلك الدقائق القليلة هل يستطيع الهاكرز ان يستولي على ما يريد من معلومات؟

● **المجرم الالكتروني او القرصنة تحتاج على الأقل من 7 الى 10 دقائق ليدخل على النظام اولا ليبدأ بعدها عملية الاختراق والوصول الى الملفات التي يريدها، ونحن وضعنا الحلول لكل تلك الامور واصطياد هذا المجرم الإلكتروني.**

وهل تستطيعون الوصول الى مكانه؟

● **نعم، نستطيع تحديد موقع الهاكرز او من يقوم بعملية القرصنة فورا.**

هل تتعاملون مع الجهاز المركزي لتكنولوجيا المعلومات فقط كمظلة اكبر ام مع البنوك والوزارات والهيئات المختلفة والتي لديها بوابات الكترونية كوزارات العدل والداخلية وغيرهما لحمايتها من الهجمات الالكترونية؟

● **نتعامل مع الجميع والجهاز المركزي لتكنولوجيا المعلومات بالفعل هو المظلة الأكبر باعتباره الجهاز الحكومي المختص بتكنولوجيا المعلومات، وكل دولة لديها «سرت» لوضع الحلول والخدمات والحماية والأمن والخطط لرد اي هجمات الكترونية تتعرض لها الدولة، وذلك يتبع بروتوكول معتمد من الأمم المتحدة.**

وماذا عن التعاون الذي تم مع الكويت من خلال الجهاز المركزي لتكنولوجيا المعلومات وشركة نوف اكسبو؟

● **شركة نوف إكسبو تساعدنا في عقد مؤتمرات توعية، لان الهجمات الالكترونية الخبيثة والجديدة هي شكل جديد على الحكومات والأفراد وبالتالي يجب توعيتهم وتعريفهم بهذه الڤيروسات الخبيثة اولا بأول قبل ان يعرفوا ما هي الحلول، ونحن نركز على التوعية المستمرة عن موضوع الاختراق الالكتروني وآلية التعامل معه.**

ذكرت خلال ندوة «المخاطر والتحديات الأمنية في مشروعات الحكومة الالكترونية» ان ايران والجيش السوري هما اكثر الأنظمة التي تشن هجمات الكترونية دائمة تستهدف دول الخليج، هل هناك تفاصيل حول هذا الموضوع؟

● **نعم ايران تقوم باستهداف دول الخليج الكترونيا، ولا يخفى على احد ان هناك خلافات عديدة بين ايران ودول الخليج حتى في مسمى الخليج ذاته، واليوم السياسة الخارجية لايران تتعارض مع سياسة دول الخليج في كثير من الملفات، والجيش الايراني يحاول الدخول على المواقع الالكترونية لحكومات دول الخليج، كما ان لها رعايا وجواسيس في بعض دول المنطقة، وكذلك لها آمال وطموحات في المنطقة، وهذا الأمر يحدث كل يوم تقريبا. ونفس الأمر يحصل من جانب الجيش السوري، فهناك نزاع وحرب قائمة تستخدم فيها جميع الأسلحة بما فيها الأسلحة الالكترونية.**

ذكرت اثناء الندوة تعرض شركة ارامكو السعودية وهي اكبر شركة نفط في العالم لهجمات الكترونية خطيرة تحت مسمى «شمعون» وايضا هذا الهاكرز استهدف دولة قطر، من يقف وراء هذه القرصنة والاستهداف الالكتروني كما كشفت معلوماتكم؟

● **حينما دخلنا على الاتاك «شمعون» اكتشفنا انه من جروب من ايران وكان يستهدف السعودية وقطر، وهناك مجموعات على الانترنت اسمها «انانليس» وهي مجموعة تتكون من هاكرز، ومن وقاحتهم انهم نشروا في 2012 اعلانا على الانترنت انهم سيستهدفون خلال يوم كذا في الساعة كذا الشركات المستهدفة وهي شركات نفطية عربية وبنوك ومنها شركات كويتية وقطرية.**

وهل حصل هذا، وكيف تعاملتم مع هذا الامر؟

● **نعم، حدث، وهؤلاء لديهم ثقة عمياء في ان وسائل الدفاع لهذه الشركات «هشة» للغاية، ووقتها جاءتنا اتصالات كثيرة من كل الشركات، والشركات التي اشترت منا FireEye ووسائل الدفاع كانت محمية من هؤلاء الهاكرز بينما الشركات الاخرى لم تكن محمية من ذلك.**

هل تتعرض الكويت لهذه الهجمات بين فترة واخرى وهل لذلك تأثير على الحكومة الالكترونية؟

● **كلما تحول العمل من يدوي الى الكتروني وديجيتال او رقمي فهو معرض للقرصنة، ومن اليوم من ليس لديه اتصال بالإنترنت او الايميل؟ وهاتان هما البوابتان المستهدفتان في الاختراق. والحكومة الالكترونية والرقمية ما هي الا تحويل العمل من يدوي الى الكتروني وبالتالي فهي محل استهداف دائم.**

هل استهداف منطقة الخليج يتوقف عند حدود ايران وسورية فقط، وماذا عن اسرائيل وغيرها من الدول؟

● **اسرائيل واميركا واوروبا الوسطى كلها تستهدف دول الخليج وهناك 3 اسباب وراء ذلك وهي: اولا الموارد النفطية والغاز والبترول، وثانيا الأشخاص اصحاب الثروات الضخمة جدا، والسبب الثالث: السياسة الخارجية للسيطرة على بعض الجماعات الموجودة داخل الدول.**

ولكن هل الهجمات التي ذكرتها عن ايران فردية من اشخاص ام منظمة من قبل اجهزة في ايران؟

● **منظمة وممولة من الدولة، وهناك ميليشيات وافراد يتم دفع رواتب لهم وعملهم هو اختراق الشركات الخليجية، حيث يطلب من هذا الشخص مثلا اختراق شركة نفط الكويت وهذه مهمته الاولى، وبعد الدخول على شبكة شركة نفط الكويت تكون المهمة الثانية الحصول على تفاصيل الشركة وكل ما يتعلق بها من خرائط وآبار ومصاف وعمال وموظفين وغير ذلك، ويمكن ان يتم بيع تلك المعلومات التي تم الحصول عليها عن طريق القرصنة او خلية الاختراق الداخلي المزروعة داخل شبكة الشركة الالكترونية لجماعات ارهابية. وهذا بيزنس ضخم يمكن ان يؤثر في اسعار النفط في العالم في اي وقت لو استطاع مثلا اغلاق مصاف او اطفاء الكهرباء وأنظمة التحكم وغيرها من الامور الخطيرة.**

هل يمكن ان يستخدم تنظيم القاعدة او داعش او غيرهما تلك المعلومات، وهل الاختراق هو احد أسلحتها في الهجوم على دول الخليج حاليا؟

● **نعم، وهو اقوى على الانترنت من وجودهم على الارض، فهم يتقدمون الكترونيا اكثر من تقدمهم على الارض.**

اخيرا، ينظر البعض الى شركة FireEye على انها شركة تابعة لوكالة المخابرات المركزية C.I.A ما حقيقة ذلك؟

● **لا، هذا الكلام غير صحيح نهائيا، فشركة FireEye هي شركة تجارية مستقلة يتم تداول اسهمها على البورصة الاميركية «ناسداك»، وهي شركة عامة وأسهمها موجودة وفق الأسس الاميركية مثل مايكروسوفت وibm. واتش بي وغيرها من الشركات العالمية.**

**شركة «نوف إكسبو» تساعدنا في عقد مؤتمرات توعية**

**يجب توعية الحكومات والأفراد بالڤيروسات الخبيثة أولاً بأول**

**الخلايا التجسسية كانت تخترق الشبكات وتظل داخلها من 8 إلى 9 أشهر دون أن يشعر بها أحد**

**إسرائيل وأميركا وأوروبا الوسطى كلها تستهدف دول الخليج**

**هدف الخلايا الخبيثة يكون سياسياً أو أمنياً أو تجسسياً ودائماً يكون تخريبياً**

**مع «FireEye» أصبح الوضع مختلفاً حيث يتم التعامل مع الڤيروسات أو الخلايا الخبيثة خلال دقيقتين**

**القرصنة تحتاج من 7 إلى 10 دقائق للدخول على النظام ليبدأ بعدها الاختراق والوصول إلى الملفات**

**التنظيمات الإرهابية تتقدم إلكترونياً أكثر من تقدمها على الأرض**

كافيتي متحدثا عن الاختراقات التي تتعرض لها الانظمة وكيفية التصدي لها