الشرطة الأوروبية تؤكد أنه من المبكر التكهن بمصدر الفيروس

باحثون: كوريا الشمالية قد تكون متورطة في هجوم «الفدية الخبيثة»

قال باحثون في الأمن المعلوماتي أنهم وجدوا صلة محتملة بين كوريا الشمالية والهجوم الالكتروني الذي اخترق منذ الجمعة أجهزة الكمبيوتر لدى شركات ومؤسسات حكومية في كل انحاء العالم، في حين حذر آخرون من هجوم جديد.

ولكن مكتب الشرطة الأوروبية "يوروبول" قال أمس انه "من المبكر" التكهن بمصدر الفيروس.

ونشر نيل ميهتا خبير تكنولوجيا المعلومات لدى غوغل، شيفرات معلوماتية تُظهر بعض أوجه الشبه بين فيروس "واناكراي" الذي اخترق مئات آلاف الحواسيب في 150 بلدا وبين عمليات قرصنة نسبت إلى كوريا الشمالية.

وسارع خبراء آخرون الى استخلاص ان هذه الادلة، رغم انها ليست قاطعة، تثبت ان كوريا الشمالية تقف وراء هذا الهجوم الالكتروني.

وقالت شركة الحماية الأمنية الروسية "كاسبيرسكي لاب" انه "من الضروري حاليا تقصي النُسخ السابقة لواناكراي". وأضافت "الامر الاكيد هو ان اكتشاف نيل ميهتا هو المؤشر الأهم في الوقت الحالي بشأن بمنشأ واناكراي».

وأضافت ان نقاط التشابه في الشيفرات تشير الى مجموعة من قراصنة المعلوماتية تحمل اسم "لازاروس" ويعتقد أنها وراء الهجوم الذي تعرضت له شركة "سوني بيكتشرز" في 2014.

ونسب خبراء هذا الهجوم حينذاك الى قراصنة كوريين شماليين تحركوا ردا على انتاج "سوني بيكتشرز" فيلما يسخر من الزعيم الكوري الشمالي كيم جونغ-اون.

وقال باحثو "كاسبيرسكي" ان "هذه المجموعة نشيطة جدا منذ 2011" وأن "لازاروس مصنع فيروسات ينتج عينات جديدة بفضل العديد من المزودين المستقلين". ووصفوا نطاق عمل "لازاروس" بأنه "صادم».

ولكن في لاهاي، قال المتحدث باسم "يوروبول" يان اوب جن اورث لفرانس برس "نحن منفتحون للتحقيق في كل الاتجاهات ولكننا لا نتكهن ولا يمكننا تأكيد هذا. الوقت مبكر جدا للإدلاء بأي تصريح". وأضاف أن الفيروس "يمكن أن يأتي من أي مكان، من أي بلد. التحقيق جار».

وقالت الشرطة الأوروبية أن نحو 165 ألف عنوان بروتوكول انترنت أو معرّف رقمي لأي جهاز كمبيوتر (أي بي) كانت مخترقة صباح الثلاثاء في مختلف أنحاء العالم، بتراجع نسبته 38% عن الأحد حين أبلغت عن اختراق 226 ألف عنوان "أي بي».

وتحدثت شركات للامن المعلوماتي كذلك في إسرائيل وكوريا الجنوبية عن صلة كوريا الشمالية بالهجوم.

وكتب مدير شركة "انتيزير لابس" الإسرائيلية للأمن المعلوماتي ايتاي تيفيت مساء الاثنين على تويتر ان شركته "تؤكد ان كوريا الشمالية وراء واناكراي ليس فقط بسبب لازاروس. سننشر المزيد من المعلومات لاحقا».

وفي سيول قال مدير شركة "هوري" سايمون تشوي لفرانس برس الثلاثاء ان الشيفرة المستخدمة في الهجوم تشبه من نواح عدة شيفرات اتهمت بيونغ يانغ باستخدامها، مشيرا الى الهجوم على "سوني بيكتشرز" وبنك بنغلادش المركزي.

أوجه شبه بين فيروس «واناكراي» الذي اخترق مئات آلاف الحواسيب وبين عمليات قرصنة نسبت إلى كوريا الشمالية

هجوم جديد ممكن

بعد الاختراق الالكتروني غير المسبوق الذي تم احتواؤه على ما يبدو، حذر تشوي مثل خبراء آخرين، من هجمات جديدة "نظرا لأنه، وخلافا للتجارب البالستية أو النووية، يمكن (للكوريين الشماليين) أن ينكروا ويتنصلوا من الهجمات الإلكترونية».

وأضاف "لاحظت السنة الماضية أن كوريا الشمالية تعد لهجمات مع برمجيات فدية أو أنها بدأت بذلك مستهدفة شركات كورية جنوبية" مشيرا إلى سرقة معطيات 10 ملايين مستخدم لدى موقع "انترباركّ" للتجارة الإلكترونية مع طلب فدية من ثلاثة ملايين دولار.

واكد ميشال فان دين بيرغ المدير العام لشركة "اورنج سايبر ديفانس" للامن المعلوماتي التابعة للمجموعة الفرنسية "اورانج" ان البرنامج الذي استخدمه قراصنة المعلوماتية "يمكن رصده" ببرامج مكافحة الفيروسات المعلوماتية.

لكنه حذر من امكانية حدوث هجوم جديد.

وقال لوكالة فرانس برس "سنشهد الآن موجة ثانية بنسخ مختلفة من الفيروس: كثيرون سيستخدمون الفيروس الاصلي لتوليد نسخ مختلفة منه" جديدة وبالتالي لا يمكن رصدها ببرامج مكافحة الفيروسات.

وسعى الخبراء الى الطمأنة الاثنين مؤكدين ان الوضع مستقر وهو ما سمح بتجنيب الحكومات والشركات الأوروبية المزيد من الخسائر جراء الهجوم الذي بدأ الجمعة مرفقا بطلب دفع فدية.

ويؤدي الفيروس الى توقف الحواسيب عن العمل وظهور رسالة "تم تشفير ملفاتكم" مع طلب دفع 300 دولار بعملة "بتكوين" خلال ثلاثة أيام والا تضاعف المبلغ، واذا لم يتم تسديده خلال سبعة أيام تمحى كل الملفات.

وكانت الاستجابة لطلب الفدية محدودة إذ سجلت 243 عملية دفع لحسابات مرتبطة بالفيروس بلغت في المجمل 63 ألف دولار (57 ألف يورو) وفق "يوروبول».

والفيروس المسمى "واناكراي" من البرمجيات المعلوماتية الخبيثة. وهو الأول الذي يجمع بين "دودة" – لأنه قادر على التوغل في شبكة بأكملها انطلاقا من كمبيوتر واحد مصاب – وبرنامج خبيث لطلب فدية.

الادارة الاميركية لم تتأثر

أكد الرئيس الروسي فلاديمير بوتين الاثنين ان لا علاقة لروسيا بالهجوم الإلكتروني العالمي، مشيرا الى ان "إدارة مايكروسوفت حددت مصدر التهديدات مباشرة" وقالت ان "مصدر الفيروس هو الأجهزة السرية الأميركية". وكانت الولايات المتحدة اتهمت في السابق روسيا بشن هجمات معلوماتية.

وأصيبت عشرات المستشفيات في بريطانيا واضطر عدد كبير منها الى الغاء مواعيد المرضى الاثنين لأن الأطباء عجزوا عن فتح الملفات الطبية.

وأصاب الفيروس النظام المصرفي الروسي ومجموعة "فيديكس" الاميركية وشركة الاتصالات الاسبانية "تيلفونيكا" وشركة "رينو" الفرنسية لصناعة السيارات وجامعات يونانية وايطالية.

لكن البيت الابيض اكد الاثنين أن أيا من فروع الإدارة الأميركية لم يتأثر بالهجوم. وقال طوم بوسيرت مستشار الرئيس دونالد ترامب، في مؤتمر صحافي "حتى هذا اليوم، لم يتأثر أي نظام فدرالي" بالهجوم، داعيا جميع المواطنين الاميركيين الى الحذر.

وأضاف ان "عددا صغيرا" من الشركات وقع ضحية لهذا الهجوم في الولايات المتحدة.

الكرملين يعتبر الأنباء عن كشف معلومات سرية «بدون معنى»

ترامب يؤكد حقه المطلق في مشاركة معلومات مع روسيا

أكد الرئيس الاميركي دونالد ترامب أمس حقه «المطلق» في مشاركة معلومات تتعلق بالارهاب والسلامة الجوية مع موسكو بعد الجدل الذي اثارته الانباء عن كشفه معلومات سرية لوزير الخارجية الروسي خلال لقائهما الاخير.

وحاول البيت الابيض مساء أمس الأول الاثنين احتواء البلبلة التي أثارتها صحيفة "واشنطن بوست" بكشفها ان ترامب تقاسم مع سيرغي لافروف خلال لقائهما الاسبوع الماضي في البيت الابيض معلومات استخباراتية سرية تتعلق بعملية يحضرها تنظيم الدولة الاسلامية.

من جهته اعتبر الكرملين هذه الانباء بانها "بدون معنى" ولا تستحق النفي او التاكيد.

وكتب ترامب على تويتر صباحا "بصفتي رئيسا، رغبت في ان اتقاسم مع روسيا، وهو حقي المطلق، وقائع تتعلق بالارهاب والسلامة الجوية. ولاسباب انسانية ارغب ايضا بان تسرع روسيا بشكل كبير حملتها ضد تنظيم الدولة الاسلامية والارهاب».

فقد كشفت صحيفة "واشنطن بوست" ان ترامب وخلال لقاء عقده في الاونة الاخيرة في المكتب البيضاوي مع سيرغي لافروف تطرق الى معلومات استخباراتية تتعلق بعملية يعدها تنظيم الدولة الاسلامية. وهذه المعلومات وصلت لواشنطن عبر شريك للولايات المتحدة لكنه لم يعط الاذن بتقاسمها مع موسكو.

ورغم ان ترامب لم يخالف القانون مبدئيا، لان الرئيس يملك هامش مناورة كبيرا للكشف عن معلومات بحوزته، الا ان مبادرته يمكن ان تهدد عملية تقاسم معلومات مع حلفاء مقربين. والكشف عن مثل هذه المعلومات الحساسة يمكن ان يعطي مؤشرات حول الطريقة التي تجمع فيها وبالتالي ان يعرض المصادر لصعوبات.

في موسكو، اعلن الناطق باسم الكرملين ديمتري بيسكوف تعليقا على تقرير صحيفة "واشنطن بوست"، "بالنسبة الينا، انها بدون معنى" مضيفا "ليست مسالة تستحق النفي او التاكيد». وكان الجنرال هربرت ريموند ماكماستر الذي يرأس مجلس الامن القومي وحضر الاجتماع اكد مساء الاثنين ان "الرواية التي تم نشرها كاذبة».

وأوضح ان ترامب ولافروف استعرضا "التهديدات التي تمثلها التنظيمات الارهابية على بلدينا، بما يشمل التهديدات المحدقة بالطيران المدني". وأضاف "لم يتم في اي لحظة بحث وسائل الاستخبارات او المصادر" لكن بدون ان ينفي بشكل واضح ان الرئيس الاميركي كشف عن معلومات سرية.

وفي ختام هذا التصريح المقتضب امام الجناح الغربي في البيت الابيض، غادر رئيس مجلس الامن القومي بدون الرد على أسئلة العديد من الصحافيين الحاضرين.


الرئيس الأميركي دونالد ترامب متحدثاً

لدي معلومات رائعة

دافع غريغ ميلر احد صحافيي "واشنطن بوست" مع غريغ جاف في حديث لشبكة "سي ان ان" عن صحة مقاله معتبرا ان البيت الابيض "يتلاعب بالكلمات" ويتجنب الخوض في عمق المسالة.

ويأتي الكشف عن هذه المعلومات فيما سلطت الاضواء مجددا على الدور الذي لعبته موسكو في الحملة الانتخابية الرئاسية الاميركية، اثر الإقالة المفاجئة لمدير مكتب التحقيقات الفدرالي (اف بي آي) جيمس كومي الذي كانت اجهزته تحقق في تواطوء محتمل بين فريق حملة ترامب وروسيا.

كما يأتي قبل ايام من مغادرة ترامب في اول رحلة له الى الخارج ستقوده الى السعودية واسرائيل والفاتيكان وبروكسل لحضور قمة حلف شمال الاطلسي وصقلية (مجموعة السبع).

ونقلت واشنطن بوست عن مسؤول اميركي طلب عدم كشف اسمه ان المعلومات التي كشفها ترامب لوزير الخارجية الروسي وكذلك للسفير الروسي في الولايات المتحدة سيرغي كيسلياك الذي كان حاضرا ايضا، تتسم بإحدى أعلى درجات السرية التي تستخدمها وكالات الاستخبارات الاميركية.

وقال هذا المسؤول ان الرئيس الاميركي "كشف للسفير الروسي عن معلومات اكثر من تلك التي نتقاسمها مع حلفائنا».

وبحسب واشنطن بوست فان ترامب "بدأ بوصف تفاصيل تهديد إرهابي يمثله تنظيم الدولة الاسلامية ومرتبط باستخدام اجهزة كمبيوتر محمولة داخل طائرات».

وأوضحت الصحيفة انها قررت عدم نشر مزيد من التفاصيل المتعلقة بهذا المخطط الارهابي بناءً على طلب صريح من مسؤولين اميركيين.

وخلال لقائه مع لافروف تباهى ترامب بانه مطلع على معلومات محددة جدا حول هذا التهديد. وقال بحسب المسؤول الذي تحدث الى الصحيفة "+لدي معلومات ممتازة. لدي اشخاص يقدمون لي يوميا معلومات ممتازة».

بسبب دعم موسكو لحركة التمرد الانفصالية في الشرق

أوكرانيا تحجب مواقع وخدمات إلكترونية روسية رائجة

فرضت اوكرانيا أمس عقوبات جديدة على روسيا المتهمة من قبل كييف بدعم حركة التمرد الانفصالية في شرق اوكرانيا، عبر حجب عدد من خدمات الانترنت الرائجة وتقدمها شركات روسية. واستهدفت الاجراءات التي وردت في مرسوم نشر على موقع الرئاسة الاوكرانية خصوصا شبكات التواصل الاجتماعي "في-كونتاكتي" التي توصف في بعض الاحيان ب"فيسبوك الروسي" وينتمي إليها أكثر من 15 مليون مستخدم أوكراني وشبكة "اودنوكلاسنيكي" وبوابة "ميل.رو" وكلها شركات يهيمن عليها الملياردير الروسي عليشير عثمانوف. كما تستهدف هذه العقوبات مجموعة "ياندیكس" المدرجة في بورصة نيويورك ويحظى محرك بحثها بشعبية كبيرة وطور عددا من الخدمات الصحافية والمتعلقة بالخرائط. ولم تكتف كييف بحجب هذه المواقع بل قررت تجميد موجوداتها في أوكرانيا والحد من عملياتها التجارية والمالية.

وتستهدف اجراءات الرئيس بترو بوروشنكو ايضا مختبرات مكافحة الفيروسات المعلوماتية "كاسبيرسكي». وتوسع هذه العقوبات تلك التي فرضت على موسكو منذ ضمها شبه جزيرة القرم في آذار / مارس 2014 وأعقبها اندلاع النزاع في الشرق مع الانفصاليين الموالين لروسيا الذين تتهم كييف موسكو بدعمهم.

وأسفرت المعارك عن سقوط اكثر من عشرة آلاف قتيل خلال ثلاث سنوات.

قمة بين الرئيس الكوري الجنوبي الجديد وترامب في يونيو

يزور رئيس كوريا الجنوبية الجديد مون جاي-ان الشهر المقبل الولايات المتحدة للقاء الرئيس الاميركي دونالد ترامب في اجواء من التوتر الناجم عن الطموحات النووية لكوريا الشمالية.

واعلن يون يونغ-شان، الناطق باسم مون، أمس الثلاثاء ان القمة بين الرئيس الكوري الجنوبي وترامب ستعقد في نهاية يونيو في واشنطن. واضاف ان الموعد الدقيق للقمة وجدول اعمال المحادثات سيعلنان في وقت لاحق.

ومون محام سابق في قضايا حقوق الانسان، يساري ويؤيد إجراء شكل من الحوار مع الشمال لخفض التوتر. اما ادارة ترامب فقد قالت ان الخيار العسكري مطروح.

وقال الناطق باسم الرئيس الكوري الجنوبي "سنعد لهذه القمة كفرصة لتعزيز العلاقات الشخصية والصداقة بين الرجلين».

بعد منح برلين اللجوء السياسي إلى بعض العسكريين الأتراك

يلديريم يدعو ألمانيا الى الاختيار ما بين تركيا والانقلابيين

دعا رئيس وزراء تركيا بن علي يلديريم أمس ألمانيا الى أن تختار بين صداقتها مع أنقرة أو الانقلابيين المزعومين بعد منح برلين اللجوء السياسي إلى بعض العسكريين الأتراك المتهمين بأنهم على صلة بالانقلاب الفاشل صيف 2016.

وقال يلديريم في خطاب بثه التلفزيون "على المانيا أن تقرر بشأن أمر واحد: إذا أرادت تحسين علاقاتها مع تركيا (...) فعليها إذن أن تلتفت نحو الجمهورية التركية" وليس مؤيدي الداعية فتح الله غولن المقيم في الولايات المتحدة وتتهمه أنقرة بتدبير محاولة الانقلاب.

صدرت هذه التصريحات غداة منع انقرة نوابا المانا من زيارة قاعدة انجرليك في جنوب تركيا التي ينتشر فيها جنود المان.

ووصفت المستشارة الالمانية أنغيلا ميركل الاثنين هذا القرار بأنه "مؤسف" وتحدثت عن "بدائل ممكنة من انجرليك" كالاردن على سبيل المثال.

ومن دون ان يتطرق مباشرة الى أنجرليك، اتهم يلديريم برلين الثلاثاء بأنها تسببت في "تدهور جديد للعلاقات" من خلال منح "عسكريين فروا الى الخارج" حق اللجوء بعد الانقلاب الفاشل في تموز/يوليو.

وقدم مئات من الديبلوماسيين والعسكريين وعائلاتهم طلبات لجوء في المانيا منذ الانقلاب الذي عزته انقرة الى حركة غولن.

ومنذ كانون الثاني/يناير، طلبت انقرة من برلين رفض تلك الطلبات وطالبت ايضا بتسليم الانقلابيين المفترضين الذين يسود الاعتقاد أنهم لجأوا الى المانيا.

وتواجه برلين وانقرة منذ سنة مزيدا من الخلافات والأزمات الدبلوماسية، اذ دائما ما تتهم تركيا المانيا بالتدخل او دعم المجموعات المعارضة للرئيس رجب طيب أردوغان، مثل حزب العمال الكردستاني.

إلا ان هذا الخلاف الجديد يأتي مباشرة بعد الازمة العميقة التي حصلت في الربيع، عندما اتهم اردوغان برلين وعواصم اوروبية اخرى بممارسات "نازية" بعد منع عدد كبير من اجتماعات الدعم للاصلاح الدستوري الذي عزز صلاحيات الرئيس التركي.

حكومة ساحل العاج تعلن التوصل إلى اتفاق مع العسكريين المتمردين

عاد الهدوء أمس الى ابيدجان وبواكيه اكبر مدينتين في ساحل العاج مع إعلان الحكومة عن ابرام اتفاق مع الجنود المتمردين منذ الجمعة.

وأعلنت حكومة ساحل العاج مساء الاثنين انها توصلت الى اتفاق لم تكشف تفاصيله مع العسكريين المتمردين الذين اتسعت حركتهم الاحتجاجية وادت الى اضطرابات كبيرة في ابيدجان وبواكيه.

وتوقف اطلاق النار في الهواء في ابيدجان وبواكيه الذي حدث بشكل كثيف الاثنين في محيط الثكنات والمعسكرات.

وفي ابيدجان استؤنف النشاط الطبيعي في حي الاعمال "بلاتو" لكن قسما كبيرا من السكان بقوا في بيوتهم عملا بنصيحة شركاتهم قبل الاعلان عن الاتفاق.

وفي بواكيه تستأنف الحياة بشكل طبيعي في المدينة حيث فتح عدد اكبر من المحلات التجارية ابوابها. لكن المتمردين ما زالوا متمركزين عند مدخلي المدينة بدون ان يعترضوا طرق السيارات.