ورقات تحليلية

إعصار سيبراني: انكشاف أمني أميركي غير مسبوق

حسن مظفر الرزو*

29 ديسمبر/ كانون الأول 2020

Al Jazeera Centre for Studies
Tel: +974 40158384
jcforstudies@aljazeera.net
http://studies.aljazeera.net

يتفادى القراصنة السيبرانيون ترك بصمات تحدد هويتهم (الجزيرة)

مقدمة

تعرضت كيانات الفضاء السيبراني للولايات المتحدة الأميركية إلى أكبر إعصار سيبراني بتاريخها، في 13 ديسمبر/كانون الأول 2020، عندما اكتشفت بصمات الهجمة الأولية في شبكات ونظم معلومات كل من وزارة الخزانة، ووزارة التجارة، ووزارة إدارة الاتصالات والمعلومات الوطنية(1). إلا أن البيانات الأمنية التي توافرت لدى الخبراء السيبرانيين أكدت أن الاختراق السيبراني قد بدأ منذ مدة ليست بالقصيرة ربما منذ بدايات شهر يناير/كانون الثاني 2020 عندما نجح القراصنة السيبرانيون في اختراق الشفرة البرمجية لبرمجيات تعود لثلاث شركات برمجية عملاقة، هي: مايكروسوفت Microsoft، وسولار ويندز SolarWinds، و(في إم وير) VMware(2).

أحدثت هذه الهجمة الشرسة صدمة كبيرة على مستوى القيادات الأمنية السيبرانية في عموم الولايات المتحدة، مع تنامي القلق لدى المؤسسات الفيدرالية والمحلية المستهدفة وكبريات شركات القطاع الخاص، وذلك لعدم وضوح تفاصيل وعمق الهجمة ومستوى حساسية البيانات التي استطاع القراصنة السيبرانيون حصادها من شبكات ونظم المعلومات والمستودعات الرقمية التي نجحوا بالوصول اليها؛ من أجل هذا هرع الكثير إلى إطلاق مصطلح "التهديد الخطير" وعلى جميع المستويات(3) والذي يُستخدم لوصف أشد أنواع التهديدات التي يمكن أن تتعرض لها نظم معلومات وشبكات المعلومات في الولايات المتحدة في التاريخ المعاصر(4).

الاختراق السيبراني: موارده وتحليل معماريته البرمجية

تسلل قراصنة المعلومات في هجمتهم السيبرانية الصادمة للولايات المتحدة من خلال منصة برمجيات شركة SolarWinds الأميركية(5)، فأضحت هذه الشركة ضحية ولقمة سائغة بيد القراصنة السيبرانيين الذين نجحوا بإقحام أداة برمجية خبيثة أُطلق عليها SUNBURST لتقيم في برمجيات المنصة البرمجية Orion® Platform(6)، والتي عندما تم تنشيطها (بواسطة

إيعازات برمجية محددة) وفَّرت للمهاجمين السيبرانيين فرصة اختراق المضيف الرقمي للمنصة الذي يقوم باستضافة برمجيات الشركة(7).

تميزت الهجمة السيبرانية بتعقيد ملحوظ في بيئة توريدها الرقمي بحيث أتاحت للمهاجمين فرصة اعتراض الفيض الرقمي لعدد كبير من مستخدمي البيئة البرمجية وتحقيق الأهداف المرجوة من الهجمة الشرسة التي يعتقد أنها قد تمت بواسطة قراصنة سيبرانيين من خارج حدود الولايات المتحدة، ودون أن تتوافر قرائن لدى خبراء الشركة بتحديد هويتهم أو البلدان التي ينتمون إليها.

وتبيَّن من عملية الفحص والتدقيق التي أجراها خبراء الأمن السيبراني بشركة SolarWinds أن هذه الأداة البرمجية الخبيثة قد تسلَّلت بتاريخ 13 ديسمبر/كانون الأول إلى أكثر من 18 ألف زبون من الزبائن الكبار لهذه المنصة البرمجية، وعن طريق الخدمة التي توفر التحديثات لحزمة البرمجيات الخاصة بمنصة أوريون Orion والتي تُستخدم بكثافة في المؤسسات الفيدرالية بالولايات المتحدة، وشركات Fortune 500 لمراقبة أداء شبكاتها المعلوماتية(8).

وفي يوم 14 ديسمبر/كانون الأول، أعلنت الشركة ذاتها أن حوالي 33 ألف زبون للشركة من مجموع ما يزيد على 300 ألف زبون قد قاموا بتحميل التحديث الخاص بتطبيقات منصة Orion الذي التصقت الأداة الخبيثة ببرمجياته(9). وقد أعلنت الشركة عن الاختراق بتاريخ 15 ديسمبر/كانون الأول بعد أن كشفت شركة الأمن السيبراني الشهيرة FireEye أنها قد تعرضت إلى اختراق نشأ عنه سرقة أكثر من 300 أداة برمجية تقوم الشركة بتجهيزها لزبائنها لضمان الأمن السيبراني للعمليات المعلوماتية والاتصالية لديهم(10).

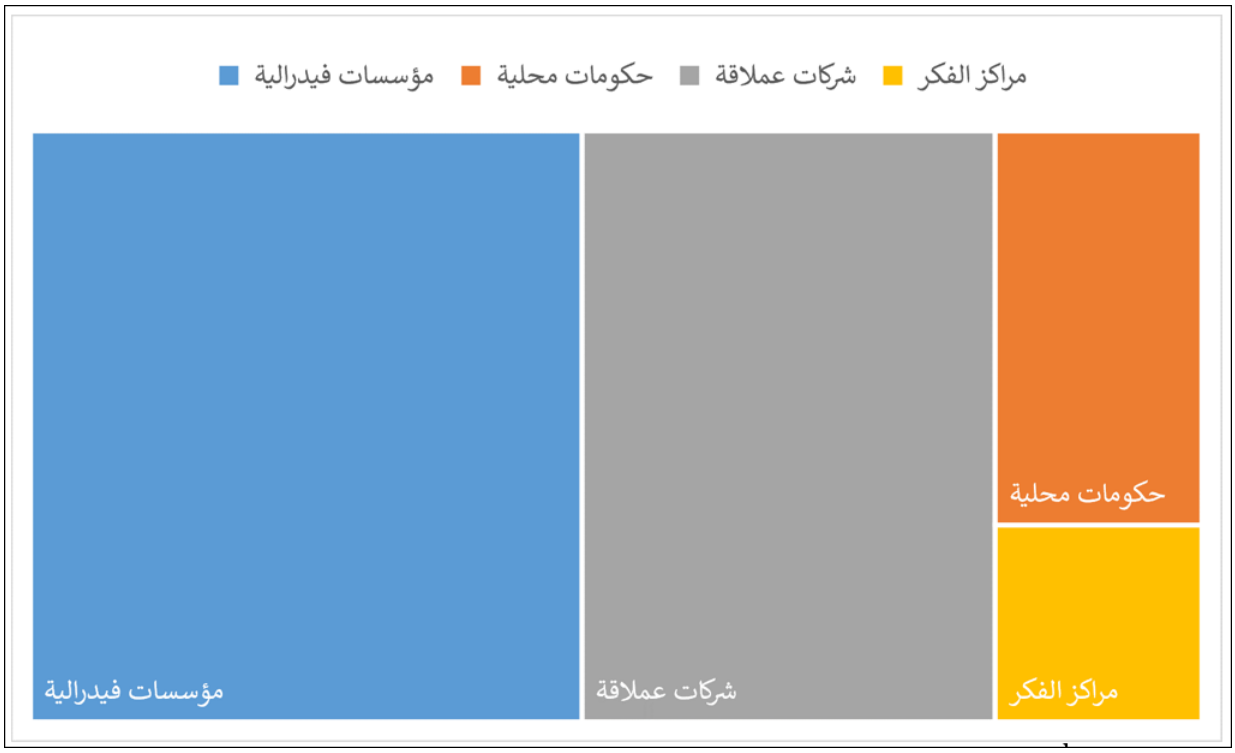
أما إذا تتبعنا الحدث وراء الكواليس المعلنة، سنجد أن شركة FireEye قد أصدرت منذ يوم 13 ديسمبر/كانون الأول تقريرًا تفصيليًّا حول معمارية الأداة الخبيثة التي استُخدمت في اختراق منصة برمجيات شركة SolarWinds تضمنت دلائل أكيدة بأن منصة برمجياتها قد أصيبت بالأداة الخبيثة منذ شهر مارس/آذار 2020، بيد أن شركة FireEye لم تذكر في تقريرها الأوَّلي أن إصابة منصتها البرمجية قد نشأت عن شركة SolarWinds، لكنها عادت وأكدت الإصابة عن طريق قناة الأخبار الأمنية Krebs On Security(11).

ولم تسلم شركة Microsoft العملاقة من هذه الهجمة بعد أن تبين من التقرير الذي أعدته الوكالة الأميركية للأمن السيبراني وأمن البنى التحتية (CISA)، بتاريخ 17 ديسمبر/كانون الأول(12) ، والذي ذُكر فيه أن الوكالة المذكورة قد عثرت على أدلة تثبت أن القراصنة السيبرانيين قد نجحوا في زرع رموز وشهادات المصادقة Authentication Tokens في حسابات الامتيازات العالية للشركة المذكورة في خطوة لتصعيد تأثيرات الهجمة السيبرانية عن طريق فتح الباب للوصول إلى الموارد المعلوماتية التي تستضيف مختلف أشكال الخدمات الداعمة للجهات الحكومية وشركات القطاع الخاص.

ولم يعد خافيًا على الشبكات الإخبارية ما حصل، فأُعلن عن نجاح هجمة القراصنة السيبرانيين ووصولهم إلى موارد المراسلات الإلكترونية في وزارتي الخزينة والتجارة، وبعد يوم واحد أُعلن عن تسللهم إلى شبكات المعلومات في وزارة الأمن الداخلي الأميركية (DHS)، التي أجبرت الوكالة الأميركية للأمن السيبراني وأمن البنى التحتية (CISA) على الطلب من المؤسسات الفيدرالية الأميركية بالتوقف عن استخدام منصة تطبيقات شركة SolarWinds على الفور(13).

وقد بدأت قائمة الجهات التي تعرضت إلى هذه الهجمة السيبرانية الشرسة تتوسع شيئًا فشيئًا فالتحقت بالجهات أعلاه كل من(14): وزارة الدفاع الأميركية (البنتاغون)، ووزارة العدل، ووزارة إدارة الاتصالات والمعلومات، وإدارة الأمن النووي الوطني (NNSA) التي تنهض بمهام تخزين الأسلحة النووية، وهيئة التنظيم الفيدرالي التابعة لوزارة الطاقة (FERC)، والمختبرات الوطنية في واشنطن ونيومكسيكو، ومكتب النقل الآمن ومكتب Richland Field Office.

وقد أعلنت الوكالة الأميركية للأمن السيبراني وأمن البنى التحتية (CISA) تفاصيل أخرى عن الجهات التي طالتها هذه الهجمة السيبرانية(15)، فحذَّرت من وجود جهات أخرى تنتمي إلى المؤسسات الحكومية الأميركية، والمحلية والإقليمية، بالإضافة إلى شركات القطاع الخاص، لم تحدد هويتها لغاية هذا التاريخ بسبب عمق الهجمة. وأضافت أن هناك احتمالًا كبيرًا لتوسع نطاق الهجمة وتأثيره البالغ على نظم المعلومات على المستويين، المحلي والفيدرالي، انظر الشكل (1).
الشكل (1) يبيّن توزيع آثار الهجمة السيبرانية على المؤسسات الفيدرالية والمحلية والقطاع الخاص بالولايات المتحدة الأميركية(16).



المصدر: إعداد الباحث

تعد هذه الهجمة من أشد الهجمات تأثيرًا على الكيانات الرقمية ومستودعات المعلومات الحساسة بتاريخ الولايات المتحدة، ولقد اتسمت هذه الهجمات بتقنية عالية وتعقيد بنيوي ملحوظ بحيث ساد الاعتقاد بأن الكثير من الكيانات المعلوماتية التي طالتها الهجمة لن تتمكن من إزالة جميع آثارها التخريبية المحتملة على المستوى القريب، وأن هناك حاجة ماسَّة إلى مراجعة أمنية-معلوماتية شاملة لضمان خلوها من البصمة التأثيرية للأداة الخبيثة والتسلل السيبراني في منظومات شبكات المعلومات والاتصالات الأميركية.

كذلك، فإن العمق التأثيري لهذه الهجمة ونوع وحجم البيانات التي استطاع القراصنة السيبرانيون الظفر بها(17)، والآثار المستقبلية التي قد تترتب على زرع أدوات خبيثة وبرمجيات تجسس أثناء عملية الاختراق لم تتضح لهذا التاريخ لأسباب عدة، لعل أهمها أن الهجمة السيبرانية لا يمكن استباق حصولها وإنما تأتي الإجراءات بعد حصولها، وبمدة زمنية قد تزيد على بضعة أيام، أو شهور أو قد تستغرق أكثر من ذلك لحين عثور الجهات المسؤولة عن أمن النظام المعلوماتي على آثار مريبة.

من هو المهاجم الشرس؟

إن الإجابة عن هذا التساؤل ليست عملية سهلة عندما نتعامل مع هجمة بُوشرت في فضاء سيبراني لا تحكمه مؤثرات المكان والزمان التقليديين، ويسري فيض هجماته في فضاء متخيل، لا تحكمه حدود البلدان الجغرافية والسياسية.

بصورة عامة، فإن فضاء المنازعة والتجاذب السيبراني للولايات المتحدة الأميركية مع خصومها تقيم فيه جيوش وفصائل وميليشيات سيبرانية تعود لأربعة دول تناصبها العداء، هي: روسيا، والصين، وإيران، وكوريا الشمالية(18). ورغم أن التصريحات الرسمية بالولايات المتحدة قد وجهت إصبع الاتهام إلى روسيا على لسان الرئيس المنتخب، جو بايدن، ووزير الخارجية الحالي، بومبيو، وعضو الكونغرس، ميت رومني(19)، وخبراء أمنيين ووسائل الإعلام الأميركية، من جهة، بينما انفرد الرئيس الأميركي الحالي، دونالد ترامب، فقلَّل من أهميتها ثم وجه إصبع اتهامه إلى الصين، إلا أننا نرى من الضروري التريث في قبول هذه الاتهامات التي لم تثبتها أدلة قاطعة (من ذوي الاختصاص) في تحديد هوية الجهة المهاجمة التي لم يُعثر على أثر غفل عنه الفاعلون في الشفرات البرمجية للأداة الخبيثة، ولم تتضح جغرافية مسار الفيض الرقمي من مصدره إلى الجهة المستهدفة، كما لم يتحدد، لغاية هذا التاريخ، مستوى عمق الهجمة وحجم الآثار التخريبية التي حصلت نتيجة عنها.

من أجل هذا، سنحاول تحليل عناصر ميدان الصراع السيبراني والجهات التي تقيم فيه، مع تركيز اهتمامنا على وقائع النزاعات السيبرانية خلال عام 2020، لكي تتضح الصورة أمامنا ونستطيع تحديد تراتبية الدور المحتمل للخصوم السيبرانيين الأربع للولايات المتحدة.

لقد قمنا بمعالجة مسألة تحديد الهوية من خلال ثلاثة محاور(20):

المحور الأول: حصة كل جهة من عدد الهجمات على الفضاء السيبراني الأميركي، انظر الشكل (2)؛ حيث يبدو واضحًا أن القراصنة الإيرانيين قد مارسوا هجمات سيبرانية أكثر من بقية الخصوم وبنسبة وصلت إلى 34.48% من مجموع الهجمات، بينما جاءت كل من روسيا والصين بالمرتبة الثانية وبنسبة 20.6%.

الشكل (2) يبيّن حصة كل جهة من خصوم الولايات المتحدة السيبرانيين من الهجمات السيبرانية الموثقة خلال عام 2020.

المصدر : إعداد الباحث

المحور الثاني: هوية الأهداف التي حاولت الهجمات السيبرانية بلوغها، والتي أودعناها في الشكل (3)، والتي حاولنا تصنيفها إلى: مؤسسات حكومية، ومؤسسات بحثية وأكاديمية، وسرقة بيانات من مستودعات رقمية، أو استهداف شبكات المعلومات، أو سرقة أموال.

الشكل (3) يبين هوية الأهداف التي ضربتها الهجمات خلال عام 2020

المصدر : إعداد الباحث

ويبدو واضحًا أن إيران تبوأت المقام الأول على صعيد المؤسسات الحكومية، وعلى المؤسسات البحثية والأكاديمية، بينما تبوأت كوريا الشمالية المقام الأول على صعيد سرقة الأموال لدعم اقتصادها المتهالك، بينما تقاسمت كل من روسيا والصين وإيران المقام ذاته على صعيد مهاجمة شبكات المعلومات الوطنية بالولايات المتحدة.

المحور الثالث: حجم تأثير الهجمات السيبرانية على كيانات الفضاء السيبراني بالولايات المتحدة الأميركية والتي أودعناها في الشكل (4).

الشكل (4) يبين حجم التأثيرات المترتبة على الهجمات السيبرانية في الفضاء السيبراني للولايات المتحدة خلال عام 2020

المصدر : إعداد الباحث

ويبدو واضحًا أن الهجمات السيبرانية الخطيرة قد مورست من قبل القراصنة السيبرانيين الروس بينما تبوأت إيران المرتبة الأولى على صعيد الهجمات متوسطة التأثير وبنسبة كبيرة مقارنة مع بقية الخصوم.

رغم ما تناقلته وسائل الإعلام عن خبراء في الأمن السيبراني(21)، وصفوة الطبقة السياسية الأميركية، حول توجيه أصابع الاتهام إلى مجاميع من القراصنة الروس الذين يدعمهم النظام الروسي بهذه الهجمة الشرسة إلا أن المقال الذي صدر صباح يوم الجمعة، 25 ديسمبر/كانون الأول، عن صحيفة BBC News قد شكَّك بهوية المهاجمين التي لم تتضح لغاية هذا التاريخ. وقد أكَّد ذلك تصريح مستشار الأمن القومي الأميركي، روبرت أوبراين Robert O'Brien، لشبكة Fox News الإخبارية بأن ما توافر لديهم هو أن هناك هجمة سيبرانية شرسة، استبطنت عملًا استخباريًّا، بواسطة آليات سيبرانية بالغة التعقيد، بوشرت بواسطة قراصنة سيبرانيين، تدعمهم دول مناهضة للولايات المتحدة الأميركية(22).

ولما كانت الهجمة قد صُنِّفت ضمن فئة هجمات (APT(23) وبالخصوص فئة الهجمات (APT29(24)؛ فإن هذه الفئة من الهجمات ترتبط بفريق القراصنة الروس الذي يُعرف في ميدان الأمن السيبراني باسم Cozy Bear الذي سبق وأن مارست مجموعته سلسلة هجمات سيبرانية على أهداف معلوماتية في الولايات المتحدة وكندا، والمملكة المتحدة، منذ عام 2008، والتي يُعتقد أنها تعمل كجناح للتجسس السيبراني لصالح جهاز المخابرات الروسي(25). كذلك، فإن هذا النمط من الهجمات تمارسه الفصائل الرقمية الإيرانية التي تدعمها إيران التي نجحت كوادر الشركة الأمنية الأميركية FireEye، في شهر نوفمبر/تشرين الثاني 2014، في الكشف عنها وحمَّلتها مسؤولية استهداف شركات الاتصالات، وشركات النقل بالولايات المتحدة لجمع واستقصاء بيانات موسعة عن أشخاص محددين. كذلك تخصصت هذه المجموعة بممارسات التجسس الرقمي، والتي تستثمر مواردها في دعم العمليات التي يمارسها النظام الإيراني في دول المنطقة، ودول أخرى، ودعم أنشطة مجاميع أخرى للقرصنة المعلوماتية، ولدعم أنشطة مؤسسات أمنية واستخباراتية وتقنية بالبلاد(26).

لذا، نعتقد أن مصادر هذه الهجمة الشرسة تتأرجح بين جهتين، هما: روسيا وإيران(27)، لأن لكل منهما مبررات في المباشرة بها في هذا التوقيت. فالفرصة سانحة لروسيا في خضم التجاذبات العميقة بين الرئيس المنتخب وترامب والتنازع بشأن نتيجة الانتخابات وآليات تسليم السلطة. أما إيران، فإن هذا النمط من الهجمات يلبي رغبتها الأكيدة في الانتقام من الجهة التي اغتالت قاسم سليماني والخبير النووي الإيراني، محسن فخري زاده، بالإضافة إلى الهجمات السيبرانية المستمرة التي تمارسها الولايات المتحدة على الفضاء السيبراني للمنشآت النووية الإيرانية، وبنهج غير معلن، وبعيدًا عن الانتقام بالوسائل التقليدية والذي قد يورثها مجابهة عسكرية أكيدة مع الولايات المتحدة الأميركية.

وستفصح عملية تتبع الآثار التخريبية عن هذه الهجمة السيبرانية في المستقبل القريب، ونتائج المراجعة البرمجية للمعمارية الرقمية الخاصة بالأداة الخبيثة، واقتفاء الآثار التي قد غفل عنها المهاجمون في القطع بهوية إحدى هاتين الجهتين.

احتمالات الانتقام الأميركي

أصيبت الإدارة الأميركية (بشقيها، الحالية والمنتخبة) بصدمة كبيرة نتيجة لحجم الهجمة السيبرانية التي شملت عددًا كبيرًا من المؤسسات الفيدرالية الحساسة ومؤسسات الحكومة المحلية بالإضافة إلى عدد كبير من شركات المصنفة أولى في قائمة Fortune 500، بالإضافة إلى عدم وضوح مستوى تغلغل الهجمة السيبرانية في شبكات ونظم المعلومات، وحجم تأثيراتها، وطبيعة ومستوى حساسية البيانات التي استطاع قراصنة المعلومات حصادها من المستودعات الرقمية، مع عدم معرفة فيما إذا كانت الهجمة قد انتهت أم إن آلتها الخبيثة لا تزال مستمرة بالتغلغل في الفضاء السيبراني الاستراتيجي للولايات المتحدة لغاية هذا التاريخ.

وفي خضم التهديد غير المسبوق للأمن الوطني الأميركي، فإن الساحة السياسية لا تزال مشحونة بالنزاع المحتدم بين الرئيس المنتهية ولايته والرئيس المنتخب حول ادعاءات دونالد ترامب وأنصاره بوجود تزوير في نتائج الانتخابات.

فيلاحظ وجود تناقض كبير بين الرئيس المنتهية ولايته من جهة وإدارته من جهة أخرى بالتعامل مع هذا التهديد الخطير. فبينما لم يُبْدِ الرئيس الحالي، دونالد ترامب، اهتمامًا يُذكر بالهجمة السيبرانية، واقتصر في تصريحه للإعلام على حدوثها بعد مرور أسبوع على تناول الصحف الأميركية لتفاصيل الهجمة والانشغال بتحديد هوية المؤسسات الفيدرالية والحكومية وشركات القطاع الخاص التي بلغتها آثارها الضارة. وقلَّل من شأنها، وشكَّك في الاتهامات التي وُجِّهت نحو روسيا وتحميلها مسؤولية التخطيط والتنفيذ لعملياتها السيبرانية التجسسية(28).

أما موقف إدارته(29) فقد ناقض بوضوح ما ذهب إليه دونالد ترامب عندما وجَّه كل من وزير الخارجية الأميركي، مايك بومبيو، والمدعي العام، وليام بار، أصابعي اتهامهم إلى روسيا، ذلك لأن تعقيد الهجمة السيبرانية والتطور التقني الذي اتسمت به يتسق إلى حدٍّ كبير مع التفوق السيبراني الذي يتمتع به القراصنة السيبرانيون الذين يعملون بمعيَّة المخابرات الروسية#a30. من جهة أخرى، نقل المسؤول في وزارة الدفاع الأميركية (البنتاغون)، جيسون ريد Jason Reed، موقف الرئيس المنتخب، جو بايدن، الذي أكَّد أنه متى ما زالت الشكوك واتضحت هوية الجهة التي مارست هذه الهجمة فإنه سيتخذ القرارات التي ستضمن توجيه عقوبة صارمة ضدها، وأنه لن يقف مكتوف الأيدي وهو يلاحظ أن المؤسسات الفيدرالية والمحلية وكبريات الشركات الأميركية الخاصة قد تعرضت لمثل هذه الهجمة الشرسة(31).

أما فريق الرئيس المنتخب، جو بايدن، فقد ذكروا أن أمامهم أكثر من خيار لمعاقبة روسيا على هذه الهجمة السيبرانية وذلك من خلال سلسلة إجراءات عقابية اقتصادية، على التوازي مع ممارسة هجمات سيبرانية شرسة على البنية التحتية للمعلومات والاتصالات في روسيا. وأكدوا على أن من الضروري أن يكون الرد قاسيًا لتوجيه ضغوط اقتصادية وتقنية على كيانات الفضاء السيبراني الروسي ولكن بعيدًا عن أي تصعيد للنزاع والأجواء المشحونة مع النظام. وفي الوقت نفسه، أكد الرئيس المنتخب، بايدن، على ضرورة إعادة مراجعة أداء المؤسسة الأمنية السيبرانية الوطنية، وتخصيص مبالغ إضافية لتطوير أدواتها، والارتقاء بأداء مواردها البشرية بحيث تحافظ الولايات المتحدة على مكانتها المتقدمة بامتلاك مقومات الردع السيبراني الأمثل على المستوى العولمي لدرء مثل هذه المخاطر ومنع تكرار حدوثها بالمستقبل(32).

ويبدو واضحًا أن إجابة مستشاري إدارة الرئيس المنتخب، جو بايدن، تتسم بكونها بعيدة عن التعامل الرشيد مع مثل هذا التهديد والذي يحتم مراجعة دقيقة لملابسات الهجمة، وتقدير حجم الأضرار التي نتجت عنها، والتأكد من هوية القراصنة السيبرانيين، والغايات التي رُسِمت لها لكي يكون القرار قريبًا من الواقع(33). يضاف إلى ذلك إلى أن وجودهم خارج البيت الأبيض، وبعيدًا عن الجهات المسؤولة عن تقدير مستوى الردع السيبراني الذي تمتلكه الولايات المتحدة قبالة القدرات السيبرانية للجهة التي مارست الهجمة سيجعل من قراراتها غير ذات قيمة معنوية ما لم تصدقها قدرات ردع سيبراني يمكن أن تحقق التأثير المناظر لما حصل في نظم وشبكات المعلومات بالولايات المتحدة، وبعكسه فسوف تقتصر الإجراءات على فرض المزيد من العقوبات التي لن ترقى إلى مستوى الأضرار التي نجمت عن الهجمة السيبرانية غير المسبوقة(34).

لا تزال سحابة الغموض تحيط بحجم تأثير هذه الهجمة السيبرانية على صعيد المؤسسات الفيدرالية والمحلية، ومستوى الاختراق الذي نجح القراصنة بتحقيقه في كل منها، وطبيعة البيانات والمعلومات التي ظفروا بها، ودوافع القراصنة السيبرانيين سواء كانت عملية تجسس أم محاولة لخلخلة نظم المعلومات في عموم الولايات المتحدة الأميركية(35).

كذلك، أكد مجموعة من خبراء الأمن السيبراني أن المؤسسات التي تعرضت لهذه الهجمة السيبرانية ستكون بحاجة إلى مدة لا تقل عن عام لتحديد عمق تأثيرها والآثار التي ترتبت على البيانات الموجودة في مستودعاتها الرقمية(36). كذلك، فإن حجم التداعيات المحتملة على نظم معلومات المؤسسات الفيدرالية والمحلية وشركاتFortune500 لم تتضح بعد أن ذهب بعض خبراء الأمن السيبراني إلى عدم وجود أدلة قاطعة على انتهاء العملية، وإمكانية وجود أهداف بعيدة المدى لا يمكن التنبؤ بها بالوقت الحالي(37).

لذا، من الصعوبة التكهن بطبيعة وحجم الرد المتوقع من الولايات المتحدة الأميركية بعد الإنكار القاطع لروسيا ممارسة أي دور في هذه العملية غير المسبوقة(38). على صعيد آخر، لا يُتوقع أن تكون هناك انعكاسات مباشرة على أمن الفضاء السيبراني في منطقة الخليج العربي لأن العملية استهدفت بيانات حساسة بالولايات المتحدة ما لم ينشب عنها نشر مراسلات سرية، أو قرارات غير معلنة عن علاقات بعض الدول العربية قد تسهم في نشوء أزمات بينها وبين إيران في ظل الأزمة الخانقة التي تعيشها مع الحصار الخانق الذي تفرضه الولايات المتحدة الأميركية عليها.

***حسن مظفر الرزو**، مدير مركز الموصل للدراسات الاستراتيجية والمستقبلية.

مراجع

1. Nakashima, Ellen, Russian Government Spies Are Behind A Broad Hacking Campaign That Has Breached U.S. Agencies And A Top Cyber Firm, National Security Dec.13th 2020, https://web.archive.org/web/20201213220635/https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html , Accessed on Dec.22nd 2020.
2. Bing, Christopher, Suspected Russian Hackers Spied on U.S. Treasury Emails – Sources, Reuter Dec. 13th 2020, https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive-idUSKBN28N0PG , Accessed on Dec. 21st 2020.
3. Cyber Attack on US Government Poses 'Grave Risk', RTE, Friday Dec. 18th 2020, https://www.rte.ie/news/world/2020/1218/1185191-us-cyber-attack/ , Accessed on Dec. 22nd 2020.
4. https://www.almaany.com/en/dict/ar-en/grave+threat /, Accessed on Dec. 22nd 2020.
5. 5. يقع مقر شركة SolarWinds في ولاية تكساس، والتي تأسست عام 1999 في مدينة تولسا بولاية أوكلاهوما، وقد استقرت بعد حين في ولاية تكساس. وتمتلك الشركة منصة برمجيات توفر أنماطًا متعددة من الخدمات على صعيد مراقبة شبكات الحواسيب. وقد لاقت هذه البرمجيات إقبالًا كبيرًا في إدارة نظم المعلومات بالمؤسسات الفيدرالية والحكومية الأميركية وشركات القطاع الخاص، كما شاع استخدامها في دول أوروبية وآسيوية متعددة بسبب كفاءة أداءها وسهولة استخدامها.
6. 6. زرعت البرمجية الخبيثة في الإصدارات البرمجية HF 5 2020.22019.4HF 1 2020.2التي أعدتها الشركة لتحديث وتطوير برمجياتها خلال السنتين 2020/2019.
7. 7. What Happened? , Solar Winds, Dec. 20th 2020, https://www.solarwinds.com/securityadvisory/faq , Accessed on Dec. 22nd 2020.
8. 8. تلتحق هذه الهجمة بهجمات سلسلة التوريدSupply Chain Attack أو هجمات الطرف الثالث Third-Party Attack، وذلك لأن الهدف الابتدائي للهجمة لم يكن مؤسسات الحكومة الأميركية وإنما وُجّهت الهجمة نحو إحدى كبريات الشركات المجهزة للخدمات المعلوماتية، وهي شركة SolarWinds والتي اتخذت وسيطًا لنقل الأداة الخبيثة عن طريق حزمة تحديث البرمجيات التي تجهز بها للمؤسسات الفيدرالية والمحلية الأميركية بالإضافة إلى كبريات شركات القطاع الخاص الأميركي (Fortune500)، وقد أنشأ قراصنة المعلومات بوابة خلفية Backdoor في منصة برمجيات Orion التي تزودها الشركة لزبائنها ليستطيعوا الولوج من خلالها إلى نظم وشبكات المعلومات.
9. 9. SolarWinds Hack Could Affect 18K Customers, KREBSON security, Dec. 20th 2020, https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/ , Accessed on Dec. 22nd 2020.
10. 10. Solarwinds: Hacked Firm Issues Urgent Security Fix, BBC News, Dec.25th 2020, https://www.bbc.com/news/technology-55442732 , Accessed on Dec.25th 2020.
11. 11. Novinson, Michael, VMware Flaw Used To Hit Choice Targets In SolarWinds Hack: Report, CRN, Dec.18th 2020, https://www.crn.com/news/security/vmware-flaw-used-to-hit-choice-targets-in-solarwinds-hack-report, Accessed on Dec. 23rd 2020.
12. 12. MicEvoy, Jemima, Major Cyberattack Breached Government Agency In Charge Of Nuclear Weapons Stockpile, Forbes, Dec. 17th 2020, https://www.forbes.com/sites/jemimamcevoy/2020/12/17/federal-government-private-sector-at-grave-risk-from-hack-warns-us-cyber-security-agency/?sh=a8f51887bc0f , Accessed on Dec. 23rd 2020.
13. 13.SolarWinds Hack Could Affect 18K Customers, KREBSON security, Dec. 20th 2020, https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/, Accessed on Dec. 22nd 2020.
14. 14. MicEvoy, Jemima, Major Cyberattack Breached Government Agency In Charge Of Nuclear Weapons Stockpile, Forbes, Dec. 17th 2020, https://www.forbes.com/sites/jemimamcevoy/2020/12/17/federal-government-private-sector-at-grave-risk-from-hack-warns-us-cyber-security-agency/?sh=a8f51887bc0f, Accessed on Dec. 23rd 2020.
15. 15. SolarWinds Hack Could Affect 18K Customers, KREBSON security, Dec. 20th 2020, https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/ , Accessed on Dec. 22nd 2020.

16. 16. https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach#federal, Accessed on Dec. 24th 2020.

17. منحت الأداة الخبيثة التي زُرعت في منصة برمجيات Orion للقراصنة السيبرانيين فرصة التسلل إلى نظم المعلومات الخاصة بالمؤسسات والشركات، وأتاحت لهم فرصة سرقة كمية كبيرة من البيانات والمعلومات، مع مراقبة فيض البريد الإلكتروني والاتصالات الداخلية والتي تشكّل كنزًا ثمينًا.

18. راعينا في بيان تسلسل الدول المرتبة التي بلغتها كل منها على صعيد السلطان الرقمي في الفضاء السيبراني.

19. انتقد عضو الكونغرس ومرشح الرئاسة الأميركية السابق، ميت رومني Mitt Romney، صمت ترامب وتعامله بلا مبالاة مع هذا التهديد الخطير واعتبره سلوكًا غير مقبول قبالة هذا المستوى من التهديد لأمن الولايات المتحدة الأميركية.

20. 20. Center for Strategic & International Studies (CSIS), Significant Cyber Incidents Since 2006, December 2020, pp.1-11.

21. 21. Nakashima, Ellen, Russian Hackers Compromised Microsoft Cloud Customers Through Third Party, Putting Emails And Other Data At Risk, Washington Post, Dec. 25th 2020, https://www.washingtonpost.com/national-security/russia-hack-microsoft-cloud/2020/12/24/dbfaa9c6-4590-11eb-975c-d17b8815a66d_story.html, Accessed on Dec. 25th 2020.

22. 22. Solarwinds: Hacked Firm Issues Urgent Security Fix, BBC News, Dec.25th 2020, https://www.bbc.com/news/technology-55442732 , Accessed on Dec.25th 2020.

23. يطلق مصطلح Advanced persistent threat (APT) على نمط محدد من الهجمات المعلوماتية المتقدمة والتي تتميز بكونها تستهدف شبكات المعلومات وكياناتها الرقمية خلال مدة زمنية متطاولة، مع بقائها بعيدًا عن أنظار ضحاياها، والإدارات المعلوماتية لبيناتها الرقمية.
Wikipedia, APT Attacks, https://en.wikipedia.org/wiki/Advanced_persistent_threat#Characteristics, Accessed on Dec 24, 2020.

24. FireEye, Advanced Persistent Threat Groups Who's Who of Cyber Threat Actors, APT Groups, FireEye, https://www.fireeye.com/current-threats/apt-groups.html, Accessed on Dec. 24th 2020.

25. نجحت هذه المجموعة باختراق موقع اللجنة الديمقراطية الوطنية قبيل الانتخابات الرئاسية عام 2016، كما أن أصابع الاتهام قد وُجّهت صوبها من قبل الولايات المتحدة والمملكة المتحدة عند اكتشاف عملية اختراق لقواعد بيانات المراكز البحثية التي تعمل على إنتاج لقاح COVID-19 في شهر يوليو/تموز 2020.

26. كذلك يلاحظ أن مجموعة القراصنة هذه قد سخَّرت قدراتها لممارسة هجماتها النوعية على شركات النفط والغاز في منطقة الخليج العربي، مع السعي إلى الحصول على معلومات وبيانات لغرض بيعها لجهات أخرى واستثمار العوائد المتحققة عنها في ترسيخ حضورها في فضاء النزاع الرقمي، وتطوير معماريتها التنظيمية، وتوفير دخل لائق لأفرادها.

27. أظهرت التحريات التي قام بها خبراء مؤسسة FireEye أن هذه المجموعة قد هاجمت أهدافًا حيوية في أكثر من سبعة بلدان في منطقة الشرق الأوسط، بين السنوات 2014-2018 مستهدفة كيانات رقمية تعود إلى مؤسسات مالية، ومؤسسات إدارة وتجهيز موارد الطاقة، ومؤسسات اتصالية بقصد سرقة المعلومات التقنية، وبيانات تخص الموارد البشرية العاملة في هذه الجهات

28. . Hunnicutt, Trevor, David Lawder & Daphne Psaledakis, Biden's Options For Russian Hacking Punishment: Sanctions, Cyber Retaliation, Reuters Dec. 20th 2020, https://www.reuters.com/article/usa-cyber-breach-biden/bidens-options-for-russian-hacking-punishment-sanctions-cyber-retaliation-idUSKBN28U0DV, Accessed on Dec. 25th 2020.

29. . قام فريق من إدارة ترامب بإعداد بيان وُجّهت فيه أصابع الاتهام إلى روسيا كونها الجهة التي خططت ورعت هذه الهجمة السيبرانية، لكن الرئيس ترامب أمر (في الدقائق الأخيرة قبل إعلان البيان) بالتوقف عن ذلك الأمر، فبقي البيت الأبيض صامتًا إزاء هذه الهجمة رغم خطورتها.

30. . Sanger, David, Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect, The New York Times Dec. 13th 2020, https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html, Accessed on Dec. 24th 2020.

31. . Mandalia, Bhavi, United States Kremlin Suspected Of Mole-Laying Cyber Attack Expands Further, U.S. Nuclear Laboratories And Department Of Defense Potential Victims, Pledge Times, December 18, 2020, https://pledgetimes.com/united-states-kremlin-suspected-of-mole-laying-cyber-attack-expands-further-u-s-nuclear-laboratories-and-department-of-defense-potential-victims/ , Accessed on Dec. 24th 2020.

32. . Hunnicutt, Trevor, David Lawder & Daphne Psaledakis, Biden's Options For Russian Hacking Punishment: Sanctions, Cyber Retaliation, Reuters Dec. 20th 2020, https://www.reuters.com/article/usa-cyber-breach-biden/bidens-options-for-russian-hacking-punishment-sanctions-cyber-retaliation-idUSKBN28U0DV, Accessed on Dec. 25th 2020.

33. . ذكر ستيفن لينش Stephen Lynch، الخبير في الأمن السيبراني بمؤسسة John Hopkins ، أن حجم نطاق هذه الهجمة واسع جدًّا بحيث إن خبراء الأمن السيبراني بالولايات المتحدة لا يمتلكون فكرة واضحة عن مستوى الاختراق، وأن حجم المعلومات التي نجح المهاجمون في حصادها كبير، بحيث إن المحققين لا يمتلكون رؤية واضحة عن مستوى أهمية ما حصلوا عليه لغاية هذا التاريخ.
. عندما سُئل جو بايدن، في لقائه الأخير على قناة CBS News عن طبيعة الإجراءات التي سوف تتخذها إدارته للتعامل مع الهجمة السيبرانية الروسية، ذكر أنه سيفرض عقوبات اقتصادية على كيانات وأفراد في روسيا ممن سيثبت تورطهم بهذه الهجمة.

34. .35Sebeniu, Alyza, The Facts and Mysteries About Russia's Hack of the U.S., The Washington Post, Dec. 24th 2020, https://www.washingtonpost.com/business/the-facts-and-mysteries-about-russias-hack-of-the-us/2020/12/23/8a0cefc2-4552-11eb-ac2a-3ac0f2b8ceeb_story.html, Accessed on Dec. 24th 2020.

35. . أصدر الخبير الأمني شين كوسيلSean Koessel ، من شركة الأمن السيبراني Volexity، تحذيرًا لهذه الشركات بضرورة التأكد مما يمكن أن يكون قد تخفَّى تحت الحجارة. في إشارة إلى ضرورة التنقيب في جميع تفاصيل ومكونات نظم المعلومات ومستودعات البيانات للتأكد من خلوها من أي نوع من الآثار التخريبية، وخلوها من بصمة الأداة الخبيثة.

36. 37. Paul, Kari & Lois Beckett, What We Know – And Still Don't – About The Worst-Ever US Government Cyber-Attack, The Guardian Dec.19th 2020, https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government, Accessed on Dec. 24th 2020

37. . وصفتها شركة مايكروسوفت بالهجمة اللافتة للنظر بسبب سعة نطاقها، وتعقيد هيكلتها وحجم تأثيرها غير المسبوق.