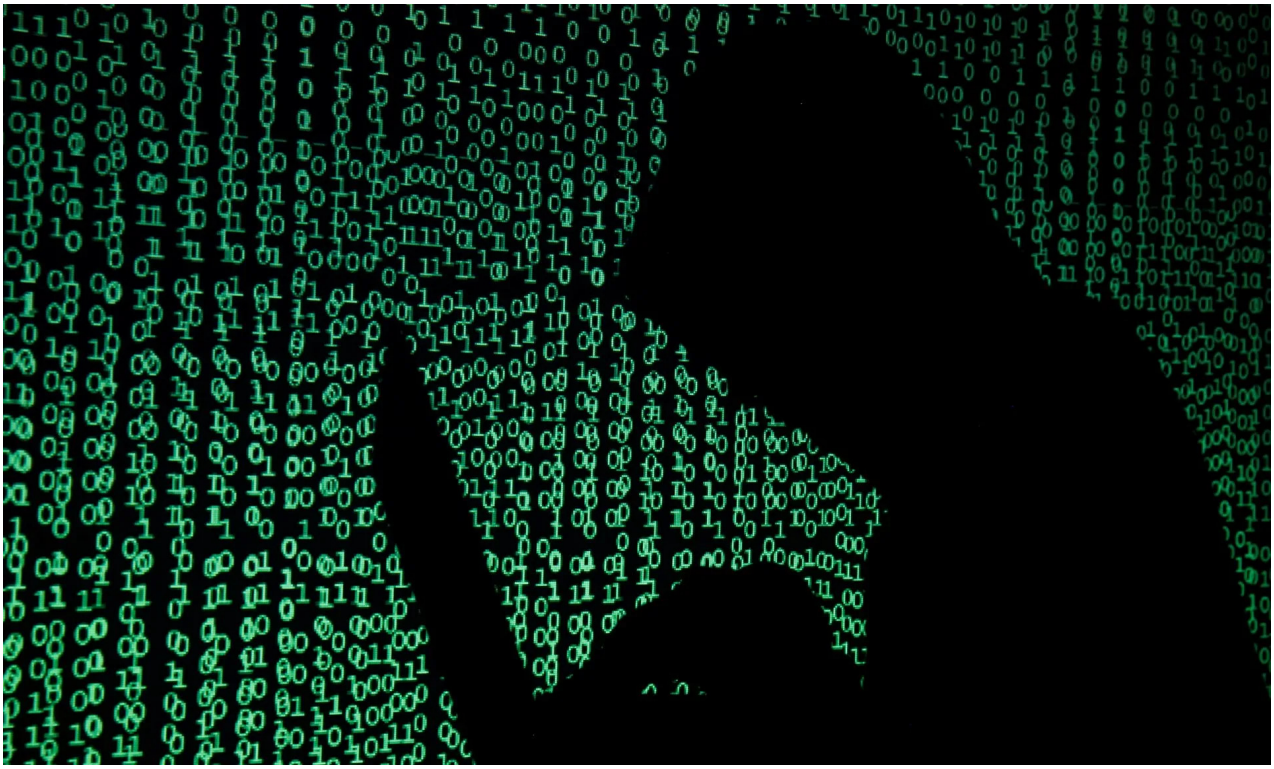
# ”وسطاء الظل“، والهجمات الإلكترونية، وما خفي أعظم!



ترجمة وتحرير نون بوست

تدّعي مجموعة القراصنة ”وسطاء الظل“، أن البيانات التي قامت بتسريبها مهّدت الطريق للهجوم الإلكتروني الأخير ”رانسوم وير“. فضلا عن ذلك، أعربت هذه المجموعة عن استعدادها لتسريب موجة جديدة من أدوات القرصنة التي استولت عليها من وكالة الأمن القومي الأمريكية.

وعلى خلفية الهجوم الإلكتروني الأخير، أفادت مجموعة وسطاء الظل، التي أعلنت عن مسؤوليتها في تسريب معلومات من وكالة الأمن القومي التي استخدمتها بدورها لنشر برمجية رانسوم وير الخبيثة واختراق منظومة هيئة الخدمات الصحية الوطنية في المملكة المتحدة والعديد من البلدان الأخرى، بأنها تملك مجموعة جديدة من الأدوات وعلى دراية بنقاط الضعف في البرامج الجديدة.

تشمل الأهداف المحتملة القادمة لوسطاء الظل آخر إصدار للنسخة الجديدة من نظام تشغيل الحواسيب ”ويندوز 10“، الذي يبلغ عدد مستخدميه في جميع أنحاء العالم 500 مليون مستخدم، علما وأن هذه البرمجية لم تتأثر بالهجوم الأول. وفي إحدى مقالات المدونة، التي كتبتها هذه المجموعة باللغة الإنجليزية، قالت المجموعة إنها تملك ”ديسك أوبس“، التي تدّعي أنها سرقته من وكالة الأمن القومي.

علاوة على ذلك، يزعم وسطاء الظل أنهم استغلوا متصفحات الويب، وأجهزة التوجيه، والهواتف الذكية، وبيانات شبكة تحويل الأموال الدولية ”سويفت“، فضلا عن ”بيانات شبكات البرامج النووية والصينية والإيرانية، أو الكورية الشمالية، والصواريخ النووية“ للوصول إلى أهدافهم.

وفي هذا الإطار، تتمثل النقطة المثيرة للقلق بالنسبة لوكالات الأمن والشركات في جميع أنحاء العالم في منشور وسطاء الظل، الذي مفاده أنه ”خلال شهر حزيران/ يونيو سوف يطلق وسطاء الظل خدمة تفريغ البيانات“. في الواقع، يعني ذلك أنهم سوف يصدرون نموذج الاشتراك الشهري الجديد الذي

يجبر الناس على دفع رسوم العضوية للحصول على المزيد من البيانات، مع منح حرية التصرف لجميع الأعضاء في البيانات التي يتلقونها.

من جهة أخرى، أشارت مجموعة وسطاء الظل إلى أنها سوف تُفرج عن أدوات للمشتركين كل شهر وتختفي تماما؛ مضيفة أنها على استعداد لتسليم أدوات القرصنة المسروقة من وكالة الأمن القومي بمقابل. في حين لا تزال دوافع وسطاء الظل غير معروفة، يزعمون أنهم ليسوا مهتمين بالمبالغ الكبيرة التي تدفعها شركات البرمجيات لمعرفة نقاط ضعفها، فضلا عن أن هدفهم لا يتمثل في بيع قراصنة الإنترنت لمعلومات يمكن أن تفيدهم في أغراضهم القذرة.

فضلا عن ذلك، أشار وسطاء الظل إلى أنهم "يفخرون باستهداف خصم من ندّهم أو أفضل منهم، ويريدون تحدي وهزيمة خصم لائق. ويعتقد وسطاء الظل أن خصمهم الحقيقي هو "ذا إكوايشين غروب"، الذي يُعتقد أنه فريق قرصنة متطور يعمل بالتعاون مع وكالة الأمن القومي".

في الوقت الراهن، يحاول المجتمع الدولي تحليل المدونات التي ينشروها وسطاء الظل من أجل فهم نواياهم. وفي ذات السياق، غرّد الباحث ماتيو سويش، من شركة كوماي تكنولوجيز، على موقع تويتر، أن "وسطاء الظل عادوا مجددا". وتجدر الإشارة إلى أن ماتيو سويش، الذي درس إصدارات وسطاء الظل، يعتقد أن المجموعة يمكنها اختراق ملفات وكالة الأمن القومي بكل سهولة.

خلال شهر أغسطس/ آب، جلب وسطاء الظل اهتمام المجتمع الدولي عندما قاموا بمحاولة عرض مجموعة من أدوات التجسس السيبرانية القديمة بالمزاد العلني، التي ادعوا أنهم سرقوها من وكالة الأمن القومي. وقد فتحت التسريبات، والهجوم رانسوم وير" العالمي الذي أعقب ذلك، المجال للنقاش حول كيفية ومتى يجب على وكالات الاستخبارات الكشف عن نقاط الضعف المستخدمة في برامج التجسس عبر الإنترنت، بطريقة تمكن الشركات والمستهلكين الدفاع عن أنفسهم بشكل أفضل.

أثار هجوم واناكري المخاوف من أن الأسلحة السيبرانية القوية لجهاز التجسس يمكن أن تتحول الآن إلى أداة إجرامية، مما يجعلنا نستنتج أن تهديدات الأمن السيبراني قد وصلت إلى مستويات جديدة. والجدير بالذكر أن وكالة الأمن القومي لم تعلّق على منشورات وسطاء الظل، منذ أن ظهرت هذه المجموعة في السنة المنصرمة، ولا تردّ على محتويات التسريبات الماضية أو هجوم رانسوم وير الذي شنته هذه المجموعة يوم الجمعة الفارط.

ووفقا لهذه المعطيات، من غير المعروف ما إذا كان وسطاء الظل يملكون بالفعل المزيد من الأدوات المسروقة من وكالة الأمن القومي، أو ما إذا كانت المجموعة سوف تجني أموالا من التهديدات التي ترسلها. ولكن، من المحتمل أن يجعل تهديد وسطاء الظل لويندوز 10 مستقبل شركة مايكروسوفت على المحك، فضلا عن شركائها والشركات التي تستخدم أحدث نسخة من ويندوز، والتي لم تطلها إلى حد الآن هجمات رانسوم وير.

في تحليله لتهديد وسطاء الظل، كتب الباحث الأمني المستقل، مارسي ويلر أن "وسطاء الظل سوف يُصعّدون العداء بين مايكروسوفت والحكومة"، وذلك ببساطة عن طريق تهديدها بتسريب معلومات أخرى عن الشركة مايكروسوفت. وفي هذا الصدد، صرّحت شركة مايكروسوفت يوم الثلاثاء الفارط، أنها مطلعة على ادعاءات وسطاء الظل، لذلك تعمل فرق الأمن التابعة لها على رصد التهديدات المحتملة من أجل "مساعدتها على تحديد الأولويات واتخاذ الإجراءات المناسبة."

في نفس السياق، صرّح الرئيس التنفيذي لشركة مايكروسوفت، براد سميث، في وقت سابق من هذا الأسبوع أن "هجوم واناكري استخدم عناصر مسروقة من عمليات الحرب السيبرانية التي تملكها وكالة الأمن القومي". في المقابل، لم تعلق الحكومة الأمريكية مباشرة على هذه المسألة.

## المصدر: الغارديان

رابط المقال: https://www.noonpost.com/18058/