العرب
الأحد 2020/04/19
السنة 42 العدد 11682

أزمة كوفيد - 19 تنعش التجسس التجاري

الموظفون المسرّحون الغاضبون صيد سهل وثمين تتلقفه أجهزة المخابرات

تداعيات الأزمة قد تكون قاتلة

يمثل الملايين من العمال والموظفين المسرحين من شركاتهم نتيجة الأزمة المالية التي تسببت بها إجراءات مواجهة أزمة انتشار فايروس كورونا المستجد صيدا سهلا لأجهزة المخابرات التي تجد في مواقع التواصل الاجتماعي بيئة خصبة تزخر بالموظفين المسرّحين الغاضبين فتستقطبهم عن طريق الإغراءات المادية وكذلك عن طريق تنمية الرغبة في الانتقام من الشركة التي تخلت عن موظفيها وقت الأزمة.

واشنطن - مع حظر الاجتماعات العامة وإغلاق الحانات والمطاعم وتقييد السفر كان انتشار البطالة من بين آثار أزمة فايروس كوفيد – 19 الأخرى، حيث أصبح الملايين عاطلين عن العمل. ولا يقتصر الأمر على العمال والموظفين في الشركات والمصانع، بل يشمل عشرات الآلاف من الموظفين في الصناعات التي تستهدفها وكالات الاستخبارات مثل التكنولوجيا والفضاء والطاقة والنفط والغاز.

على سبيل المثال أعلنت شركة جنرال إلكتريك للطيران، وهي شركة استهدفتها حملات استخباراتية صينية لسرقة تكنولوجياتها في تصنيع المحركات أكثر من مرة، عن تسريح 10 في المئة من قوتها العاملة في قطاع تصنيع المحركات.

> الأمن من أكثر القطاعات تضررا في الشركات مما يجعل الموظفين في هذا القطاع عرضة للتجنيد في عمليات التجسس

وليس عمال الياقات الزرقاء هم الوحيدون المتأثرون بالأزمة بل يتم تسريح المديرين التنفيذيين والمهندسين وغيرهم من الموظفين من ذوي الياقات البيضاء ويعانون من تخفيضات في الرواتب. فعلى سبيل المثال، وفي شركة سي آي إي الكندية لخدمات التدريب على الطيران، سجّل الفريق التنفيذي تخفيضات في الأجور بنسبة 50 في المئة ونواب المديرين بنسبة 30 في المئة والمديرين بنسبة 20 في المئة وجميع الموظفين الآخرين المتبقين بنسبة 10 في المئة.

ويلفت محلل قضايا الإرهاب والأمن في مركز ستراتفور للأبحاث الأمنية الاستخباراتية سكوت ستيورات إلى أن هذه الوضع يمثل بيئة نشطة للجواسيس ولتجنيد العملاء، مشيرا إلى أن خطر التجسس على الشركات أصبح أكثر حدّة من أيّ وقت مضى في ظل أزمة كوفيد – 19.

شهية مفتوحة

يبدو أن شهية أجهزة المخابرات الصينية أو الروسية (أو غيرها، بما في ذلك الشركات المحلية المنافسة) للتجسس على أسرار الشركات زادت خلال هذه الفترة الاقتصادية الصعبة لأنها تجعل سرقة التكنولوجيا أقل كلفة وأسرع من بدء المشاريع من الصفر.

ويشير ستيورات إلى أن منصة لينكدْ إنْ اليوم تعج بالوكلاء والجواسيس. وقد تبين في حالات كثيرة سابقة إلى أيّ مدى تعتمد هذه المنصة في عمليات الجوسسة التجارية، حيث يستخدمها المجنّدون لرصد أهداف قبل الاتصال بهم، من ذلك توظيف كيفن مالوري المسؤول السابق في وكالة الاستخبارات الأميركية للتجسس لصالح الصين، وقصة الحسناء الروسية المزيفة كيتي جونز، ذات العيون الزرقاء الجذابة والشعر الأحمر، التي استخدمت شبكة التواصل المهنية لينكدْ إنْ للدخول في دوائر المسؤولين الأميركيين.

لا يقتصر دور المنصة على الاكتشاف فقط، بل تُستخدم لإقامة الاتصال والبدء في تطوير علاقة مع الأهداف. ويسمح لينكدْ إنْ للمجندين بالبحث عن موظفين في شركة معينة يرغبون في استهدافها بسرعة. وفي الكثير من الحالات يسرد الأشخاص تفاصيل البرامج أو التقنيات التي يعملون عليها، ويتباهون بأيّ تصاريح أمنية قد تكون ضمن امتيازاتهم. في بعض الأحيان سيشير الأشخاص إلى أنهم عاطلون عن العمل أو يبحثون عن وظيفة في ملفاتهم الشخصية على الموقع، ويسهّل هذا النوع من المعلومات مرحلة اكتشاف دورات التوظيف أكثر.

وفي ظل الوضع الراهن يلجأ الكثير من العاطلين الجدد إلى هذه المنصة. ومن خلال تقديم مشاريع تشمل العمل في المنزل براتب معين لخداع العاطلين عن العمل المتمتعين بإمكانية الوصول إلى التقنيات التي يستهدفها المجنّدون، لا تصعب رؤية الطريقة التي تمكّن الجهات الخبيثة من إقامة علاقة قوية مع الهدف لاصطياده.

ويزعم المجنّدون أنهم يرغبون في مساعدة الهدف ماليا خلال هذه الأزمة لاعتماد هذه المساعدة في وقت لاحق كوسيلة ضغط بعد عودة الشخص إلى العمل في شركته الحالية، أو عندما يجد وظيفة في شركة أخرى في منصب يمكّنه من الوصول إلى التقنيات أو المعلومات التي تبحث عنها الأطراف المنافسة.

يمكن تحقيق كل ذلك عن بُعد عبر لينكدْ إنْ أو تطبيقات وسائل التواصل الاجتماعي الأخرى. ولن يكون تحويل الأموال إلى حساب مصرفي إلكتروني صعبا عبر شركة وهمية، كما يمكن إرسال بعض العملات المشفرة إلى الجاسوس كمكافأة يصعب تتبعها تقليديا.

توجد أمثلة كثيرة على صبر الروس والصينيين في جهودهم الاستخباراتية، وغالبا ما ينتظرون سنوات قبل أن يستغلوا ما استثمروه في أحد العملاء لتحقيق نتائجهم المرجوة. وفي الظاهر قد تبدو صلة الموظفين بمؤسساتهم وأسرارها قد قطعت بمجرد انتهاء عقد العمل بينهما، حيث تقطع معظم الشركات وصول الموظفين المسرّحين إلى المعلومات الحساسة الموجودة في أنظمتها.

لكن حسب ستيورات لا تعرف هذه الشركات كمّ المعلومات التي يمتلكونها في أجهزتهم الخاصة، وما يستطيعون الحصول عليه من زملائهم السابقين، وما بقي في ذاكرتهم. في هذا السياق يذكر مثال تجنيد الصينيين لكيفن مالوري الذي على الرغم من أنه كان ضابطا سابقا في وكالة المخابرات المركزية ولم يكن يتمتع بنفس درجة وصول الموظفين النشطين إلى معلومات الوكالة، إلا أنه كان صيدا ثمينا لبكين.

إغراء مادي

من حيث استراتيجيات التوظيف تعد المكافآت المالية أبرز نهج يستخدم في حالات الموظفين المسرّحين من العمل، فهم في وضع مالي صعب. ويمكن أن يكون النهج المالي فعالا أكثر مع الابتزاز إذا قرر الهدف عدم التعاون في المهمات المستقبلية.

ويشير سيتورات إلى أن الصينيين يفضلون هذا الأسلوب وانتهجوه في قضية مالوري وقضية المهندس السابق بشركة جنرال إلكتريك لشياوكينغ زينغ الذي اتهم بالتجسّس لأغراض اقتصادية والتآمر لسرقة أسرار تجارية. وفي حالة كانديس كلايبورن، التي كانت موظفة في وزارة الخارجية، اتهمت أيضا بتهمة التخابر مع الصين وتزويدها بمعلومات حساسة.

وإذا كان المال هو المحفز الرئيسي في القضايا السابقة، فإن الانتقام قد يكون دافعا أيضا في عمليات قد يتم اكتشافها لاحقا. ويفسر ستيورات ذلك مشيرا إلى أن الكثير من الموظفين قد يشعرون بالغضب ومع تأزم أوضاعه قد يتحول الأمر إلى رغبة في الانتقام من الشركة التي استغنت عنه في هذا الظرف الحساس.

هنا يمكن أن يكون التجنيد عن بعد سهلا، حيث يستطيع المجنّد استغلال غرور الهدف وتعطشه للانتقام بمجرد التواصل معه عبر وسائل التواصل الاجتماعي والتطبيقات الصوتية، في طرق تشبه تلك التي يعتمدها عدد من الإرهابيين في الخارج لتجنيد عملائهم في الغرب.

مفارقة الأمن

يعتبر سكوت ستيورات أن ما تمرّ به الشركات وعمال الأعمال اليوم أصعب مما شهته خلال الأزمة العالمية في سنة 2008. ويقارن بين الأزمتين لافتا إلى أن الشركات عندما تواجه أزمة مالية تقوم بتسريح الموظفين والعمال وفق فئات محددة، وتبدأ بأولئك الذين لا يبدون أساسيين في تحقيق الأرباح.

غالبا ما يكون المسؤولون عن أمن الشركات أنفسهم من ضمن المسرّحين الأوائل. وعادة ما يُثقل قسم الأمن ميزانية الشركة إذ يشمل رواتب الموظفين وأجهزة التحكم في الوصول والكاميرات وأجهزة الإنذار. ورغم أهميته، يُنظر إلى قسم الأمن كعالة تُنقص من صافي أرباح الشركة بدلا من المساهمة فيه. لذلك تعتبر الميزانية الأمنية أول قسم يسرع إليه بعض المدراء لخفض التكاليف بسرعة في محاولة لتحقيق التوازن بين بيان الربح والخسارة.

واعتمد الكثيرون هذا المبدأ اليوم. وكان الأمن من أكثر القطاعات تضررا في الشركات والمؤسسات، مما جعلها أكثر عرضة للتجسس مع تقليص البرامج والوظائف التي تحمي من سرقة معلوماتها الحساسة التي يستهدفها المنافسون.

سكوت ستيوارت

خطر التجسس على الشركات أصبح أكثر حدّة من أي وقت مضى في ظل أزمة كوفيد – 19

كما يتزايد تهديد التجسس على الشركات مع الارتفاع في أعداد الموظفين المسرّحين. وحتى إذا لم تتخلّ الشركات عن البرامج الأمنية تبقى معرفة الموظفين المسرّحين بالبرامج والإجراءات الأمنية تهديدا للشركة.

ويخلص ستيورات في تحليله إلى أنه بسبب أزمة كوفيد – 19، ستكون الأشهر القليلة القادمة صعبة على أيّ شخص يحاول تنظيم هذه العمليات عبر الحدود. وقد تكون هذه الفترة الأصعب بالنسبة إلى الشركات حيث يعدّ خطر التجسس الناتج عن عمليات التسريح عاملا آخر يزيد من حدّة التحدي الهائل الذي تعيشه اليوم.