صعود كاسح وهبوط مفاجئ: لماذا يحذر العالم من شركة Zoom؟

كتبه أحمد سلطان | 7 أبريل ,2020

تداعت في الأيام الأخيرة أخبارٌ كثيرة على المنصات التقنية ومواقع التواصل الاجتماعي، يحذر خلالها مدونون وخبراء من الاستمرار في استخدام منتجات شركة "Zoom"، كنافذة اجتماعات افتراضية موثوقة، بعد اكتشاف عدد كبير من الثغرات الأمنية "الخطيرة" في هذه الأدوات.. فما القصة؟ وما حقيقة هذه الاتهامات؟

الجذور

تعود القصة إلى عام 2011، أي قبل تسعة أعوام من الآن، حينما فكر رائد أعمال صيني يبلغ من العمر نحو 30 عامًا، ويحمل شهادة جامعية في علوم الحاسب وعددًا كبيرًا من الإخفاقات "الشخصية" في مجال التقنية، أن ينشئ شركة متخصصة في مجال "Video Conferencing" أو اجتماعات العمل عن بعد.

وعلى نحو دقيق، فقد استغرق الأمر عامين قضاهما إيريك يوان في محاولة الانسلاخ عن ربقة بعض الشركات الناشطة في مجال "البرمجيات التعاونية" مثل "سيسكو" (ويبكس)، والسعي إلى جمع

التمويلات من كيانات دعم المشاريع الناشئة، وتجربة العمل على مساحات غير تقليدية في مجال "اجتماعات الفيديو"، مثل إدخال الهواتف النقالة في المعادلة، وبحلول مايو/آيار 2013 قفز عدد مستخدمي منتجات الشركة قفزةً هائلة من 10 آلاف مستخدم في البداية إلى مليون مستخدم.

وفي الفترة من 2014 إلى 2017، نجحت الشركة الصاعدة في استقطاب بعض الكوادر المهنية المرموقة من شركات منافسة مثل ديفيد بيرمان وبيتر جاسنر، وإطلاق مزيد من المنتجات غير التقليدية على غرار تقنية "Zoom For Telehealth" التي تمكن الأطباء من زيارة المرضى "افتراضيًا"، وتقنية "Zoom Connector For Polycom" التي أدخلت الشركة حقل "المؤتمرات" وجعلتها تتواصل أكثر مع كبرى شركات التقنية مثل "Google"، وبحلول سبتمبر/أيلول 2017، أعلنت الشركة تنظيم مؤتمر سنوي للمستخدمين كشفت خلال نسخته الأولى عن تطبيق أوسع لتقنيات الذكاء الاصطناعي والواقع المعزز على منتجاتها، بعد أن كسرت هذه المنتجات حاجز 20 مليار دقيقة عمل، وبلغ رأس مال الشركة مليار دولار أمريكي، وتوسعت مكانيًا في عدد من الدول خارج الولايات المتحدة مثل بريطانيا وأستراليا.

وفي أبريل/نيسان 2019، أعلنت الشركة تحولًا نوعيا جديدًا في نمط معاملاتها الاستثمارية، وهو طرح نفسها في اكتتاب بورصة شركات التقنية الأمريكية (ناسداك)، بعد أن تضاعفت قيمتها السوقية تسع مرات خلال عامين لتبلغ 9 مليارات دولار أمريكي، وفور تنفيذ الطرح، أغلقت سوق الأوراق المالية على سعر يتجاوز 60 دولارًا للسهم الواحد من الشركة، بعد أن كانت التقديرات الأولية تشير إلى متوسط 30 دولارًا للسهم.

> عدد مستخدمي منتجات شركة "Zoom" ارتفع من 10 ملايين مستخدم في ديسمبر/كانون الأول 2019 إلى 200 مليون مستخدم في مارس/آذار 2020

يصعب تحديد الأسباب الحقيقية وراء ذلك الصعود الكاسح الذي حققته الشركة في فترة قصيرة للغاية، لكن جيم بينتون المدير التنفيذي لشركة "Chorus.ai" يضع أيدينا على بعض المفاتيح المهمة التي تساعدنا على فتح صندوق أسرار هذه الشركة، فإيريك يوان الذي يتمتع بمهارات تواصل فريدة، ومتعطش إلى تحقيق نجاحات غير مسبوقة بعد كثير من الإخفاقات، أولى عناية فائقة بـ"دراسة السوق والمنافسين" قبل الشروع في العمل، وقد تميز عن أقرانه من أصحاب المشاريع الأخرى بالتركيز الكلي على "المنتجات التي تعطي قيمة مضافة للزبائن، وتجعلهم سعداءً"، في نفس الوقت الذي كرس خلاله جهود الشركة في الاهتمام بالموارد البشرية، ولو كان ذلك على حساب أقسام أخرى مثل التجهيزات الثانوية والتسويق.

كورونا: مصائب قوم عند قوم

"بعد أن تعرفت على برنامج Zoom صار الخروج من المنزل ترفًا وإسرافًا"، تخبرنا هذه العبارة القصيرة التي كتبها أحد أبرز أساتذة العلوم السياسية بمعهد الدوحة للدراسات العليا على صفحته بموقع "فيسبوك" يوم الثلاثاء الماضي، أمرين مهمين: أن منتجات الشركة التي تتيح "الاجتماع عن بعد" قد تمكنت – إلى حد كبير – من ملء الفراغ الذي أحدثته إجراءات "التباعد الاجتماعي" المطبقة بغرض التخفيف من تداعيات وباء "كورونا".

كما نجحت في كسب ثقة عدد كبير من الشخصيات والمؤسسات المرموقة في أنحاء متفرقة من العالم، إلى الحد الذي جعل بوريس جونسون رئيس الوزراء البريطاني، يلجأ إليها في إدارة بعض الاجتماعات الرسمية التي حالت تدابير الوقاية من الوباء دون انعقادها بشكل مباشر كما هو معتاد.

وفي هذا السياق، تقول التقارير إن عدد مستخدمي منتجات شركة "Zoom" ارتفع من 10 ملايين مستخدم في ديسمبر/ كانون الأول 2019 إلى 200 مليون مستخدم في مارس/آذار 2020، أي خلال ثلاثة أشهر فقط، كما ارتفعت أسهم الشركة بنسبة 100% منذ نهاية يناير الماضي، مع زيادة تصل إلى 40% في مراحل تالية أدت إلى وصول قيمة السهم الواحد إلى نحو 160 دولارًا، وقد بات تطبيق الشركة "الأكثر تنزيلًا" على أجهزة "iPhone" حسبما ورد في متابعة "Sensor Tower" لحركة التطبيقات خلال الأزمة الحاليّة.

صحيح أن شركة "Zoom" كانت تحقق نجاحاتٍ هائلة منذ إنشائها حسبما أكدنا في الفقرات الأولى، كما أنها تمتلك فرقًا مهنية عالية المستوى يصل عددها إلى نحو ثلاثة آلاف موظف، مزودين بالبنية التكنولوجية اللازمة لاستيعاب هذه الزيادة الهائلة في المستخدمين، حتى إنها تخلصت، بعد أزمة "كورونا" من قيد الأربعين دقيقة التي كانت تفرضه على الاجتماعات المجانية، ولكن جوناثان كيزر المحلل التقني بشركة "سوميت إنسايتس جروب" يفسر هذا الصعود الأخير بعوامل أخرى إلى جانب هذه العوامل.

يرجع كيزر هذا الإقبال الشديد على منتجات شركة "Zoom" في الفترة الأخيرة إلى الميل الطبيعي لدى المستخدمين نحو "التطبيقات المجانية والمعروفة" التي تؤدي الخدمة المطلوبة، وفي حالة "الاجتماعات عن بعد"، كانت تطبيقات مثل "مايكروسوفت تايمز" "وزووم" أشهر الموارد المتاحة لسد العجز الذي خلفه وباء "كورونا".

> تلقت "Zoom" خلال الأيام الأخيرة عددًا كبيرًا من الضربات المتتابعة التي تمس سمعة الشركة بشكل مباشر

وبحسب كيزر، فإن المفارقة تكمن في أن هذا النوع من التطبيقات استغل الأزمة الأخيرة ليرسي نمطًا

جديدًا من تنسيق الأعمال، وهو: الاجتماع عن بعد، حيث يتوقع أن تعتمد كثير من الشركات الناشئة في الفترة القادمة على التقنيات المشابهة لـ "Zoom"، بدلًا من تحمل تكاليف ثقيلة يمكن الاستغناء عنها في التنقلات والإيجار والتجهيزات... لكن، هل لا يزال مضمون هذا الاستشراف منطبقًا على شركة "Zoom"؟

ثغرات خطيرة

على عكس هذا الاستشراف، تلقت "Zoom" خلال الأيام الأخيرة عددًا كبيرًا من الضربات المتتابعة التي تمس سمعة الشركة بشكل مباشر، حيث رصدت بعض منصات الحماية الرقمية تساهلًا واضحًا من جانب الشركة في سياساتها المتعلقة بأمن المستخدمين وخصوصيتهم، خاصة خلال الفترة التي شهدت هذه الزيادة غير المسبوقة في الأعضاء الجدد.

وقد لخصت صحيفة "الغارديان" البريطانية قصة هذه الثغرات وطبيعتها في تقرير متعدد المصادر يوم الخميس الماضي، قالت فيه إن شركة "Checkpoint" التقنية رصدت اختراق عدد من "الهاكرز" جلسات عمل وبث رسائل عنف وعنصرية، فيما بات يعرف بثغرة "Zoom Bombing" أو "قصف زووم".

كما أكد تقرير وارد عن "Intercept" أن شركة اجتماعات الفيديو "لا" تستخدم تقنية التشفير "End to End encryption"، التي تعني أن التشفير يبدأ عند المرسل وينتهي عند الملتقي في دائرة ثنائية مغلقة، مما يرجح أن "Zoom" تعترض مكالمات المستخدمين، وهو خلاف ما ادعته الشركة في السابق عن عدم قدرتها على الوصول إلى الرسائل الثنائية بسبب استخدام نظام التشفير المغلق.

وبحسب "الغارديان"، فإن شركة "Zoom" قد ركبت في منتجاتها العاملة على أنظمة "ماك" خوادم ويب مخفية، تسهل إضافة مستخدمي هذا النظام إلى الاجتماعات دون إذنهم، وتؤدي في النهاية إلى السيطرة على أجهزتهم، بما في ذلك الكاميرا والمايكروفون، كما سمحت الشركة، في سياق سعيها إلى استرضاء العملاء من ذوي السلطة مثل مديري الشركات ومعلمي الصف، بأن يعرف المضيف ما إذا كان الضيف (من الموظفين والطلاب) قد تحولوا إلى نوافذ أخرى، حال جمعهم تطبيقًا آخر مع تطبيق الشركة لمدة ثلاثين ثانية أو أكثر.

وفي نهاية التقرير، قالت "الغارديان" – نقلًا عن "Motherboard" إن شركة "Zoom" تواطأت مع "Facebook" على مستخدمي منتجاتها من مشغلي "IOS"، بحيث تنقل إلى المنصة الاجتماعية معلومات المستخدمين، لأغراض إعلانية، حتى لو لم يكن مالك الهاتف مستخدمًا لـ"Facebook".

وبشكل أكثر تفصيلًا، شرح محمد عبد الباسط المدير التنفيذي لشركة "Seekurity" المتخصصة في برامج الحماية الرقمية بعض الثغرات الأمنية غير المشار إليها في التقرير، ومنها ثغرة في إصدار "Zoom Desktop Client"، فقال إن هذه الثغرة من نوع "UNC Path Injection"، تقع في قسم

الدردشة المكتوبة، داخل نسخة "Zoom" المثبتة على نظام التشغيل "Windows"، وتسمح هذه الثغرة للقراصنة بإرسال رابط "UNC Path"

> الشركة سوف تتفرغ لمعالجة المشكلات المتعلقة بأمن المستخدمين وخصوصيتهم في الـ90 يومًا القادمة

وما إن تضغط الضحية على هذا الرابط، يرسل إلى "الهاكر" ملف يسمى "NLTMv2 and NLTM Hashes" يحتوي على اسم المستخدم وكلمة المرور ورابط الجهاز حال استخدامه "Domain Controlling"، وفي مرحلة تالية يفك المخترق هذه "الهاشات" ويتعرف على كلمة المرور، واستخدامها في الهجوم على جهاز المستخدم، خاصة إذا لم يكن مفعلًا لآليات الحماية المتعلقة بالحاسب والإنترنت، أو تمرير هذه "الهاشات" إلى طرف آخر بغرض السطو على خدمات "Microsoft" المثبتة لدى الضحية.

كيف ردت الشركة؟

يوم الأربعاء الماضي، أي قبل نشر التقرير، قال متحدث باسم الشركة لصحيفة "الغارديان" إنهم يخططون للتجاوب مع الطلب المقدم من الادعاء العام في نيويورك بخصوص الإجراءات التي اتخذتها "Zoom" لمعالجة المخاوف الأمنية والتكيف مع الزيادة في عدد المستخدمين، نظرًا لأن الشركة تأخذ خصوصية العملاء وأمنهم وثقتهم على محمل الجد، في نفس الوقت الذي تبذل قصارى جهدها لإبقاء المستشفيات والجامعات والمدارس والشركات، من جميع أنحاء العالم، على اتصال دائم، كما اعترفت الشركة ضمنيًا في نفس اليوم بعدم تشغيل تقنية التشفير المغلق في أنظمتها الداخلية، من خلال الاعتذار عما أسمته "ارتباكًا" بين ما ادعته على مدونتها من قبل وبين الواقع.

وعلى نحو مفصل، قال المتحدث إن الشركة بدأت العمل على تثقيف مستخدميها، عبر المدونات والندوات التعليمية، بشأن وسائل الحماية اللازمة لمنع تسلل أشخاص غير مرغوبين إلى جلسات الفيديو، في إشارة إلى ثغرة "قصف زووم"، كما حلت الشركة المشكلة الأمنية المتعلقة بأجهزة "ماك" بشكل عاجل، فيما نفت كليًا أن تكون قد سربت أي معلومات خاصة عن المستخدمين إلى "Facebook" في السابق، مؤكدةً في الوقت ذاته أنها لن تفعل بذلك أبدًا.

وفي تعليق من مدير الشركة "إيريك يوان"، يوم الخميس، على هذه المستجدات، اعتذر رائد الأعمال الصيني عما أسماه "عدم رقي" المؤسسة إلى مستوى التوقعات المرجوة من العملاء بشأن الخصوصية والأمن، مفسرًا ذلك "بالمهمة الجسيمة" التي أُلقيت على عاتق شركته، كنايةً عن الزيادة الهائلة وغير المتوقعة، في أعداد المستخدمين خلال الأسابيع الأخيرة.

خبراء ينصحون بالاستعاضة عن "Zoom" في الوقت الحالي بمنصات منافسة مثل "Jitsi"

وبحسب ما أورده إيريك في بيانه، فإن الشركة سوف تتفرغ لمعالجة المشكلات المتعلقة بأمن المستخدمين وخصوصيتهم في الـ90 يومًا القادمة، وذلك عبر إيقاف خطط العمل على الأدوات التكنولوجية الجديدة، وانتداب خبراء تقنيين من جهات خارجية، يشاركون في كتابة تقرير شفافية مفصل سيتم نشره عالميًا عن نتائج عمل هذه الفرق، "حتى يعود نمو الشركة إلى سياقه الصحيح".

بدائل عاجلة

إذًا لم تعد "Zoom" وسيلة اتصال موثوقة بالشكل الكافي كما كان الجميع يعتقد في الماضي، وسوف تحتاج إلى ثلاثة أشهر لضبط أوضاعها الأمنية والعودة كمنافس قوي من جديد كما قال مدير الشركة، وفي نفس الوقت، لن ينتظر أرباب العمل والمعلمون والأطباء طوال هذه المدة دون اجتماعات في ظل غياب أي حلول لعودة الحياة لطبيعتها بشكل عاجل.. فما البدائل؟

ينصح علاء غزال من فريق "أضف" المهتم بتوفير البرمجيات الحرة والتعاونية بشكل آمن ضمن جهوده في توفير بيئة إبداعية لشباب الوطن العربي، بالاستعاضة عن "Zoom" في الوقت الحالي بمنصات منافسة مثل "جيتسي| Jitsi"، حيث تتميز هذه الخدمة بتوفير كل أنواع الاتصال، المرئي والمسموع والمكتوب، بشكل مشفر ومجاني، دون طلب أي معلومات شخصية مثل الاسم ورقم الهاتف والبريد، سواء من الضيف أو المضيف.

وبعد هذا التطبيق، يوصي علاء باستخدام تطبيق "وايرWire|"، الذي يقدم خدمات أقل، مثل الاجتماع الصوتي والمكتوب، ويقيد مكالمات الفيديو بشخصين فقط، بيد أنه يحافظ على نفس مستوى الخصوصية والأمان الذي توفره "جيتسي"، أي لا يطلب من المشاركين أي معلومات شخصية، ولو كانت بسيطة. كما يمكن استخدام "Google Meet" بالنسبة للشركات والمؤسسات، ولكنه يأتي في مرتبة تالية بعد كل من جيتسي ووايرز.

وفي حالة الاضطرار إلى استخدام "Zoom" لأي سبب في الوقت الحاليّ، يشدد علاء على ضرورة إنشاء كلمة سر للاجتماع كي يكون اجتماعًا مغلقًا لا اجتماعًا عامًا، بالإضافة إلى التأكد من كون جميع الأعضاء المشاركين في الجلسة يستخدمون آخر تحديثات البرنامج، وأن يكون خيار مشاركة الشاشة مقصورًا على خيار "Host Only"، مع التنبيه على أن يستخدم الأعضاء برامج تشفير ذاتية (Vpn) مثل "Psiphon" في أثناء الاتصال.

وبالتوازي مع هذه الالتزامات، يشير علاء إلى ضرورة "تجنب" عدد من الأخطاء التي وقع فيها الضحايا السابقون، مثل تشغيل ميزة "Zoom Waiting Room"، أو مشاركة رابط الاجتماع

ورقمه على منصات التواصل الاجتماعي، أو التفاعل مع الروابط الواردة من شخص أو جهة غير موثوقة، وهي إجراءات تهدف إلى تقليص فرص تعرضك للاختراق لحدودها الدنيا، حيث لا توجد في عالم الإنترنت حماية كاملة أبدًا.

رابط المقال : https://www.noonpost.com/36602/