كيف تستعين الإمارات بقراصنة الإنترنت لإنشاء دولة الرقابة الكاملة؟

كتبه جنا ماكلولين | 1 نوفمبر 2016,

ترجمة وتحرير نون بوست

في تموز/ يوليو، امتطى الإيطالي سيمون مارجاريتيلي الباحث في الأمن المعلوماتي، طائرة البوينغ 777 من مطار روما باتجاه دبي، المدينة التي تقدم نفسها على أنها محور الشركات الناشئة في عالم التكنولوجيا.

كان سبب سفر سيمون مارجاريتيلي إلى الإمارات العربية المتحدة إجراء لقاء عمل مع شركة تدعى "داركماتر"، وقال بنفسه إن مهمته كانت تتمثل في "حماية أكثر المنظمات تعقيدًا" في الحكومة والقطاع الخاص، من خلال تجنب ومحاربة الهجمات الخبيثة على الشبكات، وتوفير طرق أكثر أمانًا للاتصال الرقمي، في مهمة عمل دفاعية وليست هجومية، تتضمن خرق الأنظمة على الشبكة العنكبوتية وأجهزة التجسس وإن أمكن هدمها.

دعي، مارجاريتيلي الذي قدم للشركة عن طريق صديق صديق له، لقضاء خمسة أيام في الإمارات العربية المتحدة على حساب الشركة لمعرفة معلومات أكثر عنها، عندما وصل إلى دبي، مدينة الذهب،

وجد جدولاً مليئًا بالرحلات والنزهات، وجناحًا فاخرًا في فندق جنة مارينا باي سويتس.

كان مارجاريتيلي "بلاكهات"، الشخص الذي يبحث عن سبل اختراق الأنظمة الإلكترونية، وهو يعمل الآن في شركة مختصة بأمن أجهزة الهواتف الذكية تدعى زيمبيريوم ومقرها تل الربيع بإسرائيل، ومهمته كشف الثغرات من دون أن يساعد في حلها، وقد كتب على موقعه: "أخترق الأجهزة والأنظمة من أجل جعل العالم أفضل"، كما أنه اشتهر باختراعه أداة محمولة يطلق عليها اسم "باتركاب"، تستخدم في التجسس على المحادثات الخاصة بين الأفراد.

عندما وصل للطابق 29 في مارينا بلازا من أجل اللقاء المرتقب، قدم ممثل الشركة مخططًا يتمثل في نشر مراصد إلكترونية تنتصب في مختلف مدن الإمارات، وسيعمل فريق من الهاكرز على اختراقها وضمان سيطرة "داركماتر" وزبائنها – الحكومة الإماراتية – على المرصد الإلكتروني، وقد وصفت الشركة أن المهمة تأتي في إطار الحفاظ على الأمن الوطني الإماراتي.

وقد كتب مارجاريتيلي في مدونته "إيفلسوكت" عن التجربة التي خاضها، وأنه قيل له "تخيل أن هناك شخص مهم يراد ملاحقته في دبي مول، لهذا نصبنا مراصد في كل المدينة، عندما نضغط على أحد الأزرار، تصبح كل الأجهزة في مركز التسوق مصابة وتحت إشرافنا".

وقد رفض مارجايتيلي عرض العمل المقدم له بعد أن نشر على مدونته تصريحًا كان عنوانه "كيف حاول جهاز الاستخبارات الإماراتي انتدابي للتجسس على شعبه"، في حين نشرت شركة "داركماتر" تغريدة مقتضبة على تويتر قالت فيها: "نحن نتحدث انطلاقًا من الواقع وليس من الخيال"، وذلك خلال رد على ما كشفه سيمون مارجايتيلي.

في حين قال كافن هالي، مدير الاتصالات في داركماتر، في رسالة إلكترونية لمجلة "ذي إنترسبت" إنه لم يلتق أي شخص من الشركة أو من فروعها بالسيد مارجايتيلي، وأضاف "الرجل الذي قابل مارجايتيلي لم يكن سوى مستشار لدينا وقد انتهت العلاقة منذ ذلك الوقت"، لكن العديد من المصادر صرحت أن الشركة وظفته لصالحها ولديها البريد الإلكتروني لدراكماتر.

وكتب هالي أيضًا: "في الوقت الذي نحترم فيه حق الكاتب في إبداء رأيه الشخصي، لا نرى المحتوى المطروح ذا مصداقية ولهذا ليس لدينا ما نعلق عليه".

وقد أنكرت شركة داركماتر تأكيدات مارجايتيلي حول انتدابه بصفة "هاكر" من أجل البحث عن تقنيات هجومية لاختراق الأجهزة، وأفاد كافن هالي في تلك الرسالة الإلكترونية للمجلة أنه "لم تشارك شركة داركماتر، أو أي من فروعها، أو مراكز البحوث التابع لها، أو أي إدارة استشارية، في النشاطات التي وصفها مارجايتيلي، نحن نفرض اختبارات صارمة على كل منتجاتنا لنضمن خلوها من أي ثغرة".

في الحقيقة، إن فكرة وجود شركة في الإمارات العربية المتحدة تنتدب جيشًا من "القراصنة" من خارج البلاد من أجل ملاحقة والتجسس على سكانها تبدو كأنها مستوحاة من أفلام جيمس بوند، ولكن بعد أشهر من الحوارات والبحوث التي قامت بها "ذي إنترسبت" تبين أن داركماتر تقوم فعلاً بذلك.

غالبية من تحدثنا معهم، طلبوا منا أن تبقى هوياتهم مخفية، مذكرين باتفاقيات الحفاظ على السرية، ومعبرين عن خوفهم من الاضطهاد السياسي المحتمل، والأعمال الانتقامية المحترفة، وحرصًا على عدم خسارة المنصب الوظيفي الحالي، هؤلاء الذين بقوا مجهولي الهوية تحدثوا عن وقائع، انطلاقًا من تجربتهم المباشرة مع دراكماتر.

لم يكن مارجايتيلي الشخص الوحيد الذي أكد أن داركماتر ليست صادقة حول عملياتها وانتداباتها، فأكثر من خمسة مصادر لديها معرفة بالشركة من الداخل، قالت لمجلة ذي إنترسبت إنه منذ بداية نشاط الشركة أوائل تشرين الثاني/ نوفمبر الماضي، قامت شركة داركماتر أو فروعها أحيانًا بالبحث عن "قراصنة" فائقي المهارة من مختلف دول العالم، بما في ذلك الولايات المتحدة، من أجل القيام بعدد كبير من الهجمات ضد أهداف مؤمنة في عالم الحاسوب.

سيمون مارجاريتيلي

وقالت هذه المصادر إن هدف الشركة هو استغلال أجهزة الرصد الموجودة في أغلب المدن الكبرى من أجل المراقبة وذلك من خلال صناعة برامج وزرع برمجيات خبيثة لتعقب واختراق أي شخص موجود في الإمارات العربية المتحدة وفي أي وقت، كما وصف لي مارجايتيلي هذا الأمر في رسالة إلكترونية حيث أفاد أنه "بالأساس هم مثل الأخ الأكبر في ترويج المنشطات".

وقد انطلقت شركة دراكماتر في العمل بعد خطاب المدير التنفيذي فيصل البناي، وهو محاط بموظفين من الحكومة، ومهندسين، ورجال أعمال، في القمة العربية السنوية الثانية بشأن مستقبل المدن الذي عقد في دبي، وقد قدمت الشركة نفسها على أنها "مدافع رقمي استخباراتي لصالح الأمة (الإماراتية)"، وقد تخلل خطاب البناي بخصوص أدوات التسويق الخاصة بداركماتر عديد من المفردات الغامضة مثل "الدفاع عن الشبكة الحاسوبية" و"حماية الاتصالات".

بعد انطلاقها تفاخرت الشركة على الشبكة العنكبوتية وخلال المؤتمرات واللقاءات الإذاعية بعزمها على أن تكون التغيير الذي سيحدث في عالم الحماية الرقمية، بما في ذلك تطوير منصتها الخاصة بالتشفير وحماية الهواتف في المنازل، والدفاع عن الشبكات الوطنية والشركات الموجودة بالإمارات، والقضاء على أجهزة التنصت ومقاومة التجسس وغيرها من الأمور.

كما أن المدونين المحليين المختصين بعالم التكنولوجيا استبشروا خيرًا بهذه المؤسسة وفرحوا لارتباطها بحكومة الإمارات، وقد وصفوا شركة داركماتر "بالمنقذة" لأعمال ومؤسسات الإمارات ضد الهجمات المتكررة على الشبكات المعلوماتية، مذكرين بالهجمات التي استهدفت عدة بنوك في سنة 2015، والتي شلت البنية التحتية على الشبكة العنكبوتية للبنوك.

بعد ذلك، انتدبت داركماتر مجموعة من أبرز المواهب من أضخم شركات التكنولوجيا حول العالم، من بينها غوغل، وسامسونغ، وكوالكوم، ومكافي، حتى إنها انتدبت المؤسس المساعد لشركة "ويكر" المختصة في خدمة تشفير الرسائل.

سافر هذا الحشد من النجوم إلى عديد من المؤتمرات مثل مؤتمر القمة "أر إس أي" بسان فرانسيسكو، وتحدثوا في الإذاعات وبرامج التلفزيون، كما وعدوا بإنشاء تطبيقات لحماية الأصوات والدردشة، وتعاقدوا مع شركة "سيمانتيك" من أجل تحسين تعقب التهديدات الرقمية في الشرق الأوسط، وفتحوا مركز بحوث وتطوير في كندا بالإضافة إلى فتحهم مكاتب في الصين.

وقد قالت مصادر متعددة لمجلة "ذي إنترسبت" إن شريحة من الشركة نمت في السنة الماضية من خلال توفير دراسات حول الهجوم الرقمي، والبحوث العلمية المتعلقة بتعقب الجرائم الرقمية، وتطوير فريق قوي قادر على القيام بهجمات على الشبكة العنكبوتية.

ووفق أحد المصادر، فإن التوجه الحديث لشركة داركماتر يتمثل في المرور نحو العمليات الهجومية، وتتزامن هذه التصريحات مع اكتشافات صدرت ضمن رسائل إلكترونية مسربة تخبر أن الشركة الإيطالية "هاكينغ تيم"، قد باعت أجهزة مراقبة لعدد كبير من الأنظمة القمعية، وبالتالي، فقد نمت داركماتر على رماد "هاكينغ تيم".

في الوقت الذي تهدف فيه الشركات التقليدية في الحماية الرقمية إلى ضمان أن كود البرمجيات والمعدات سليمة من أي عيب – أي أخطاء قد يعتمد عليها الهاكرز في عملهم – كانت داركماتر، وفق مصادر مقربة من نشاطات الشركة، تبحث عن هذه العيوب وتوظفها بهدف زرع البرمجية الخبيثة في ذلك الجهاز أو ذلك النظام، يمكن للشركة أن تسيطر على كاميرات المراقبة أو الهواتف الخلوية وبالأساس القيام بأي شيء تريده بها – كالمراقبة والتدخل أو تغيير محتوى أي رسالة إلكترونية ترسلها تلك الأجهزة أو الأنظمة أو حجب الإشارة بالكامل.

ليس من الواضح إن كان موظفو الشركة المختصين في المجال الدفاعي يعلمون هذا، في الحقيقة قالت عديد من المصادر إن مثل هذه المشاريع مخفية عنهم، وقد شرحت إحدى المصادر كيف أن ممثلي الانتدابات عن الشركة يحاولون إقناع المنتدبين أن البحوث الهجومية ستقام خارج الشركة، في شكل شراكة، نوعًا ما، أو قرابة، ولكن عديد من المصادر، من بينها مارجاريتيلي، قالوا إن القيادات العليا متورطة في مقابلات الانتداب وتعلم الحقيقة.

وقد قال المتحدث الشخصي باسم داركماتر "الشركة تحت الملك الخاص ولا تتلقى أي تمويل من الحكومة الإماراتية"، ولكن يبدو أن العلاقة قوية جدًا بين الشركة والحكومة، فقد عرّفت الشركة نفسها في الصحف المنشورة على أنها "حليف استراتيجي لحكومة الإمارات العربية المتحدة"، بالإضافة إلى أن مكاتبها تقع بالطابق الخامس عشر في مبنى "الدار" بأبو ظبي، كما تبعد طابقين عن وكالة الاستخبارات الإماراتية المعروفة باسم "السلطة الوطنية الأمنية الإلكترونية"، كذلك، فإن نائب رئيس البحث العلمي في شركة داركماتر قد عمل سابقًا بالمنصب نفسه مع وكالة الاستخبارات الإماراتية.

المدير التنفيذي لشركة داركماتر فيصل البناي

في بداية الأشهر الأولى لسنة 2016، كان مخطط الانتداب في شركة داركماتر يسير على قدم وساق، فقد جاء الموظفون البارزون من إدارة الأمن القومي الأمريكي، ووفق ما وجد في الحسابات العمومية على لينكدين، فإن أحد الموظفين الحاليين في الشركة كان خبيرًا في استغلال الشبكة العامة في وزارة الدفاع الأمريكية، حيث يضع استراتيجيات أنشطة ضد شبكات محددة ويدعم عملية جمع المعلومات الاستخباراتية الأجنبية.

كما عثر على موظف آخر مكافح للتجسس و"عميل خاص" في البنتاغون، تحدث عن نفسه بكل فخر في موقع "لينكدين" وقال إنه شخص نشط فيما يتعلق بالتغلب ومحو السرية الأمنية العالية لجهاز كشف الكذب، كما خاض موظف آخر تجربة فك التشفير مع داركماتر، حيث كان سابقًا مستشارًا ساميًا في وكالة الأمن القومي الأمريكية وضليعًا، بشكل معقد، في تصميم أنظمة الصوتيات والبيانات الأمريكية.

ويرى مارجاريتيلي وغيره من المصادر أن الشركة ليست على علم بتعيين الوظائف التي تنتدب لها أمهر الموظفين، كما حاورت المجلة أكثر من عشرة باحثين في الأمن المعلوماتي وأكدوا أن موظفي الانتدابات في داركماتر قد تواصلوا معهم، مقدمين لهم وعودًا بأعلى الرواتب، والوظائف المثيرة التي ستهتم بالدفاع الرقمي، وقد عزز بعضهم كلامه بوثائق تثبت ذلك.

وأكد عدد من خبراء السلامة الرقمية من خلال تغريدات على تويتر أن موظفي الانتدابات في داركماتر قد اتصلوا بهم، من بينهم شارلي ميلر باحث بالأمن في "أوبر" ومحلل بيانات سابق في وكالة الأمن القومي الأمريكية، وكريس فاليسيك مخترق سيارات معروف يشكل فريقًا مع ميلر، وفابيو أسوليني باحث أمني لصالح كاسبرسكاي لابس.

ورد في إحدى الرسائل الإلكترونية التي اطلعت عليها مجلة "ذي إنترسبت" عرض مبهج يتمثل في حياة من دون ضريبة في دبي، مع مجانية السكن والطعام والرعاية الصحية وتعليم الأطفال والتنقل، كما قالت الرسالة الإلكترونية إن الوظيفة تخضع لشراكة خاصة أو عامة بشأن مزودي السلامة الرقمية مع الحكومة الإماراتية.

وفي رسالة إلكترونية أخرى، ورد أن مخطط الشركة هو انتداب 250 عبقريًا قبل نهاية سنة 2016، كما قال أحد الباحثين في الأمن الرقمي إن موظفي الانتدابات بالشركة قد اتصلوا به 5 أو 6 مرات في أوقات متباعدة على لينكدين.

لم يعر بعض الخبراء المستهدفين أي اهتمام للموضوع في حين تحمس البعض الآخر للعرض، فالوظيفة توفر فرصة الإبداع في الأمن الرقمي على نطاق دولة بالكامل، كما أن الراتب مثير جدًا، فوفق إحدى المصادر، التي طلبت عدم الكشف عن هويتها خوفًا من العمليات الانتقامية، فإن الرواتب كانت مرتفعة جدًا، أكثر من نصف مليون دولار في السنة، وهو رقم قريب جدًا من أحد العروض التي اطلعت عليه "ذي إنترسبت".

ووفق مصادر مقربة من الشركة، فإن المواطن الأمريكي فيكتور كوزنتسوف، الذي قسم وقته بين

الولايات المتحدة والشرق الأوسط، كان الموظف المنتدب الأبرز لدى دراكماتر في الولايات المتحدة.

وعندما أجرينا اتصالاً هاتفيًا مع الرقم المسجل للعموم تحت اسم فيكتور كوزنتسوف، أجابنا رجل وقال لنا إننا مخطئين في الرقم وقال إنه لا يعمل مع داركماتر وأن اسمه ليس فيكتور، وعندما سألناه لماذا قدمته رسالة البريد الصوتي على أنه فيكتور، أغلق الخط، وقد اتصلت به المجلة عبر البريد الإلكتروني فرفض كوزنتسوف الإجابة وكتب: "كما يمكنك أن تتخيل، فإن عقد السرية الذي وقعته مع داركماتر يمنعني من الكشف عما أقوم به بالتحديد لصالح الشركة، ولكن جل ما يمكنني أن أقوله هو أن أي من الباحثين المنتدبين لا صلة لهم بالأمن الرقمي الهجومي".

وعلى الرغم من تأكيد الشركة على أن نشاطها سلمي ولا يستهدف أي جهة، إلا أن عديد من الباحثين المقربين، من بينهم مارجاريتيلي، أكدوا أنه قد قيل لهم إن واجبهم هو القيام بعمليات رقمية هجومية، وقد قيل للخبير الإيطالي سيمون مارجاريتيلي إن الشركة ستنصب مراصد في دبي، من بينها أجهزة ومحطات إرسال واستقبال، تسمح باختراق الاتصالات اللاسلكية بين الأجهزة الشخصية والشبكات الرقمية مثل نقاط الدخول اللاسلكية، والطائرات دون طيار، وكاميرات المراقبة وغيرها.

قد تنصب المراصد خلسة من قبل داركماتر أو بتسهيل من أنظمة الاتصالات من خلال الاتفاقيات الثنائية حول إعدادات المراقبة، ثم تتمكن الشركة من زرع أجهزة هجومية مباشرة، ضمن المراصد، قادرة على التعرض للتنقل الرقمي في شبكات "أي بي"، و"2 جي"، و"3 جي"، و"4 جي" والتعديل فيها، ثم يصبح بعدها أي شخص يستخدم الهاتف الخلوي أو أي جهاز متصل بالشبكة اللاسلكية المتصل بها أحد المراصد ضعيف الحماية ويمكن اختراقه وتتبعه بكل يسر.

وقد شرح مارجاريتيلي ما أريد له القيام به، فقال: "البرمجية التي صممتها داركماتر لاختراق المراصد لم تعمل بشكل جيد، ولهذا لم تستطع التعامل مع الحجم الكبير من البيانات المتنقلة في الشبكات، والتي من المفترض اعتراضها، لذا احتاجت الشركة إلى فريق ثانٍ ليقوم بالعمل، وفي هذا الإطار أرادت مني حل المشكلة".

كان حساب مارجاريتيلي الأكثر كشفًا لهذه الحقائق ولكن عديد من المصادر الأخرى أيضًا ناقشت مشاريع مشابهة مع داركماتر، من بين هذه المشاريع بحث وتطوير استغلال الثغرات الضعيفة، بالإضافة إلى نشر وتوظيف بعض البرمجيات الشبح التي طلب من مارجاريتيلي العمل عليها.

> "في المستقبل القريب سيصبح كل جهاز في الإمارات العربية تحت سيطرتهم"
>
> مارجاريتيلي

وقد طلبت داركماتر من أحد الباحثين والعاملين على اكتشاف الثغرات لشركة فيسبوك، وغوغل، وبعض الشركات الكبرى في عالم التكنولوجيا، أن يوظف بحوثه حول مواطن الضعف ليسمح لهم

بالوصول إلى المجالات الموثوق فيها، أي أنه سيقوم بالأساس بالعثور على الثغرات في مواقع الواب ويسمح للشركة استغلالها من أجل نشر البرمجيات الخبيثة لتتبع المستخدمين من دون أن ينتبهوا إلى ذلك.

قال هذا الباحث – الذي أراد أن يبقى مجهول الهوية – للمجلة إنه رفض العرض، حتى بعد أن عرضوا عليه المزيد من المال، لأن أهدافه مخالفة لأهداف الشركة، حيث قال "ما سأقوم به هو اختراق لا أخلاقي".

ولكن ما أثار اهتمام بعض المصادر التي اتصلنا بها والباحثين في الأمن الرقمي هو مخطط الشركة في الحصول على "شهادة السلطة سي أي"، وتعتبر شهادة السلطة الطرف الثالث الموثوق، أي هي شركة أو وكالة رسمية تهتم بالشهادات الرقمية بالأساس جوازات السفر "الإلكترونية" التي تتحقق من هوية المستخدم ومن شرعية البرمجيات.

إن البيانات المنقولة والشفرات التابعة لميكروسوفت، وفيسبوك، وموزيلا، وغيرها على الشبكة الرقمية موثوق فيها لأن هذه الشركات قد وقعت على الشهادة، ولكن ستتظاهر داركماتر عندما تمتلك هذه الشهادة بأنها جهة أخرى وستتمكن بعدها من تثبيت شهاداتها الخاصة.

هناك آلية يعمل بها الآن من أجل تجنب مثل هذه الهجمات وتدعى "تثبت الشهادة"، ولكن العديد من المواقع لا تستخدم هذه الاحتياطات، لذا لا يمكنها تجنب ولوج داركماتر للشفرة، في أثناء تحديث البرمجية مثلاً على أنها جهة أخرى، نظريًا يمكن للشركة الولوج للجهاز من خلال تحديث مضاد الفيروسات كأنه صادر من كاسبيرسكاي لابس، في حين أنها ترسل شفرة خبيثة.

وفق إحدى المصادر، فإن الشركة ستصبح قادرة على استخدام سلطتها على نشر جذورها الخفية – أدوات رقمية تسمح بالتخفي وتجاوز سلطة الدخول لأنظمة الحاسوب – بهدف تعقب أي شخص، وقد علق المصدر عن هذا قائلاً: "هذا أمر عظيم".

وقد أكد هالي أن الشركة لديها وحدة أعمال تهدف إلى نشر مفاتيح أو "جذور وطنية من شهادات السلطة للدول المجاورة وعالميًا"، وقال: "ولأن داركماتر ليست بنية تحتية لمفتاح عام للسلطة في الإمارات، لذا فنحن نوفر الآن المشورة والخدمات الإدارية ونهدف إلى إطلاق خدمات شهاداتنا التجارية قريبًا".

في الوقت الذي رفضت فيه داركماتر وجود أي مخطط لاستخدام قدراتها في الهجوم الرقمي، إلا أنه إن واصلت الشركة تطوير منصة رسائل أمنية أو أجهزة من بينها هواتفها الخاصة فستتمكن من الوصول إلى كل المخططات الداخلية لتلك المنتجات: تقارير الثغرات، ومقاييس السلامة الرقمية، وغيرها.

وسيتمكن مخترقو داركماتر من السيطرة على تلك المعلومات بينما يقوم طاقم العمل الدفاعي بإصلاح تلك الثغرات والدفع نحو تحديث البيانات على أجهزة المستخدم، وهو إجراء قد يستغرق سنوات، وعندما سئل هالي عن فرضية بيع الشركة لهواتفها الخاصة كتب لنا أن الشركة تعمل على

تطوير الأجهزة.

ليس الانتداب هو الباب الوحيد الذي طرقته داركماتر من أجل الحصول على المواهب الهجومية، ففي الشتاء الماضي، استخدمت الشركة عددًا كبيرًا من الموظفين في شركة أمريكية مقرها بالتيمور تدعى "سايبربوينت إنترناشيونال"، ولدى هذه الشركة اتصال رسمي مع وزارة الداخلية الإماراتية، أسس شركة سايبربوينت مديرها التنفيذي كارل غومتوو وزوجته فيكي في سنة 2009، وقدمت نفسها على أن أغراضها دفاعية وتتمثل في حماية المعلومات المالية، والملكية الفكرية، والسجلات التجارية، وغيرها من أشكال التواصل.

كارل غومتوو المدير التنفيذي لشركة سايبربوينت في أحد المؤتمرات في أبو ظبي

وقد فازت هذه الشركة بعديد من العقود في مناطق مختلفة مع الحكومة الأمريكية، من بينها عقد بقيمة 6 ملايين دولار من وكالة مشاريع البحوث الدفاعية المتقدمة في البنتاغون، كما رشح غومتوو السنة الماضية عن منطقة ماريلاند لجائزة "أنتروبرونور" السنوية، وتحدثت التقارير الإخبارية أن سايبربوينت كانت من بين الشركات التي أرسلت موظفيها إلى الإمارات العربية المتحدة، من أجل تدريب موظفي وكالة الاستخبارات هناك، والشبيهة جدًا بنظيرتها في الولايات المتحدة "وكالة الأمن القومي".

ولكن في الصيف الماضي قالت سايبربوينت إنها تعمل في فريق واحد وباعت أجهزة الرقابة لشركة "هاكينغ تيم" الإيطالية، التي اخترقت رسائلها البريدية الداخلية، وكشفت عن أن كميات كبيرة من مبيعاتها كانت مع الأنظمة القمعية، وأشارت تلك الرسائل البريدية التي سربت إلى أن ممثلي سايبربوينت عملوا مع "هاكينغ تيم" أجل تسهيل العمل على ما بدا أنه أجهزة مراقبة لحكومة الإمارات.

وقد قالت خمسة مصادر مختلفة مقربة من الشركة الأمريكية لمجلتنا أنه مع نهاية سنة 2015، كان هناك صراعًا داخليًا ضمن سايبربوينت بخصوص عقد الإمارات، وقد صرح بهذا موظفون سابقون في الشركة لذي إنترسبت، اشترطوا بقاء هوياتهم في كنف السرية، خوفًا من الإجراءات الانتقامية، وخوفًا على سلامتهم، لأنهم ما زالوا يعيشون في الإمارات.

وبعد تسريب الرسائل الإلكترونية لهاكينغ تيم في تموز/ يوليو، كانت هناك اجتماعات غاضبة وأصوات عالية في مكاتب سايبربوينت، أشخاص يقررون ماذا سيفعلون الآن بعد أن كشفت عملياتهم الداخلية في الشرق الأوسط للعالم.

ونتيجة لهذه النقاشات حصل أمران: قفزت أجزاء كبيرة من طاقم سايبربوينت في سفينة داركماتر، التي كانت تقدم رواتب سنوية عالية وخدمات فاخرة، وقالت إحدى المصادر للمجلة إن شركة داركماتر ساعدت بعض الموظفين على تحويل إقامتهم إلى ساوث داكوتا من أجل تمتعهم بالمزيد من الفوائد الضريبية عندما يعيشون وراء البحار.

وقد كتب هالي، مدير الاتصالات في داركماتر، للمجلة فقال "إن الشركة لا تنظر لعقود التوظيف الفردية، في المجمل نحن نخضع لقانون السلطات التشريعية في عمليات التوظيف وفي النشاطات العملية التي نقوم بها".

تنتدب داركماتر المواهب من مختلف أنحاء العالم ولديها الآن 400 موظف

بينما وعدت سايبربوينت موظفيها الذين لم يقدم لهم أي عرض – أو رفضوا – في داركماتر بتمديد عقودهم، قال أحد الموظفين إنه في كانون الأول/ ديسمبر، أعلنت سايبربوينت تمديدها للعقود بشهرين، أما بالنسبة للذين غادروا الشركة، كانت تلك مفاجأة ولم يدركوا ما حدث بعدهم في الشركة على وجه اليقين، بينما قال بعضهم إن شركة داركماتر كانت مهتمة بانتداب المزيد من التقنيين.

وقد وصفت إحدى مصادرنا هجرة العمالة بعملية "استيلاء عدائية" تديرها حكومة الإمارات العربية، أي إنهاء العقود الأصلية مع سايبربوينت، والتي هي بالأساس عقود إماراتية، وتوفير عقود جديدة داخل الدولة حتى تضمن أن المهندسين تحت سقفها.

كما أكدت داركماتر أن بعض موظفي سايبربوينت التحقوا بالشركة في الإمارات العربية المتحدة، وقالت إن هذا ليس بالأمر الغريب، وقد قال هالي: "داركماتر تنتدب المواهب من مختلف أنحاء العالم ولديها الآن 400 موظف، بعضهم جاؤونا من سايبربوينت، ويقومون الآن بالواجب المناط بهم داخل مختلف الأقسام".

وفق غومتوو، المدير التنفيذي لسايبربوينت، فإن الشركة مرت ببعض "التغييرات" منذ أن انسحبت من الإمارات للحفاظ على مصالحها، وقد أرسل أجوبة حول أسئلة طرحتها "ذي إنترسبت" من خلال رسائل عبر موقع لينكدين، وكان من بين ما كتب لنا: "لا يوجد الآن أي موظف لسايبربوينت في الإمارات، ولم يتم بيع أو امتلاك أي جزء من الشركة من قبل داركماتر أو أي جهة أخرى، ولم تتعاقد سايبربوينت أبدًا مع داركماتر".

ثم أوضح غومتوو مضيفًا "سايبربوينت لا تعمل على تطوير أسلحة رقمية، على العكس، فإن الشركة تقود اختبارات اختراق وتقييمات أمنية، نحن نستخدم أدوات تجارية موجودة على نطاق واسع حول العالم".

على الرغم من أن هذه الأدوات التي تستخدم لتحسين الدفاع الرقمي يمكن أن تستخدم لإصابة أهداف آمنة، حتى وإن استخدمت أجهزة الاستخبارات بعض هذه الأدوات لإصابة أنظمة محددة خلال التحقيقات الأمنية القومية، فإن البعض يسرق ويعدل في الكود، من أجل اختراق صحفي أو ناشط محمي في العالم الرقمي.

وقد كتب نيكولاس وافر، الباحث في الأمن الرقمي في المعهد الدولي لعلوم الحاسوب، في رسالة إلكترونية لمجلة "ذي إنترسبت" فقال: "الهوة كبيرة جدًا بين الدفاع والهجوم، خاصة عندما يتعلق

الأمر بالرقابة الشبكية، فالأدوات نفسها يمكن أن تستخدم لمراقبة شبكتك للتعرف على الهجمات وللمراقبة أيضًا".

وقد قال موظف سابق في سايبربوينت: "لقد فعلت الشركة الصواب وربما النبيل، ولكن النسبة الصغيرة من عملها خفي"، معتبرًا أن جزءًا من بحوثها الهجومية يستهدف بعض المنصات الرقمية على الشبكة العنكبوتية.

بينما قال مصدر آخر إن تلك البحوث والتطورات وعمليات صياغة الشفرات التي تقودها سايبربوينت تهدف في نهاية المطاف إلى إجراء هجمات تجسس على الصحفيين والناشطين في الإمارات منذ سنة 2012 إلى الآن، بعض تلك الهجمات تستهدف عمليات تجسس على تغريدات توتير، والتصيد الاحتيالي للبريد الإلكتروني "سباير فشينغ"، وخدمة اختصار الوصلات "يو آر إل".

هذا النوع من الهجمات معروف لدى ناشط حقوق الإنسان الإماراتي، أحمد منصور، فقد قال لمجلتنا إنه لم يقابل أي ممثل للشركة وجهًا لوجه، ولكن سبق أن حذره صديق له منها قائلاً: "إنهم يقومون بهجوم لاختراق الهيئات الأمنية الإماراتية".

وقد أطلقت مجموعة من الباحثين اسم "ستيلث فالكون" على هذا الهجوم، كما ذكر الباحثون أن "حقائق مباشرة تثبت وجود رابط بين ستيلث فالكون والحكومة الإماراتية" بالاستناد إلى القطع الرقمية.

وقد أصاب هجوم ستيلث فالكون أهدافًا متعددة في الإمارات العربية بعد مغادرة سايبربوينت البلاد، كما التحق الموظفون الذين كانت لهم صلة بالشركة الأمريكية أو عملوا على برامج التجسس بداركماتر، وذلك وفق مصدرنا الذي قال "ليس كل هجمات البرامج الضارة تم رصدها، هناك عديد منها لم يرصد بعد".

أما هالي فقال: "ليس لدي علم بستيلث فالكون أو أي أدوات هجومية استخدمت لاختراق الصحفيين والوصول لبياناتهم، فكما شرحنا سابقًا، نحن لا نملك ولم نطور أي برمجية في الأمن المعلوماتي لأغراض عدائية".

> عالم التصدير الرقمي عالم ضبابي وذلك بحسب ما تقوم به داركماتر الآن، كما أن مبيعاتها قد تخضع لقوانين عدة هيئات، كما كان من بين المنتجات تكنولوجيات التشفير، فهناك حواجز تمنع تصدير الأسلحة

كما شرحت لنا إحدى المصادر قائلة: "في وقت ما كانت سايبربوينت قادرة على اختراق ملايين الأجهزة على اختلاف مصادرها حول العالم محذرة من الثغرات – أي ثغرات لم تكتشف أو لم يتم معالجتها – في برمجياتها"، ويشمل هذا مناطق ضعف أو ثغرات في المتصفح "تور"، و"فايرفوكس"، و"إنترنت إكسبلورر"، و"ميكروسوفت أوفس".

وقال مصدر آخر لنا: "بدا أن الإمارات العربية تطمح لبناء فريقها الخاص من المهاجمين، تشمل هذه القدرات فريقًا قادرًا على القيام بهجمات على الشبكات الرقمية، لإبطال الخصوم على الشبكة العنكبوتية، وأيضًا فريق قادر على التجسس والتلاعب بالبيانات" وهي قدرات طورت في مختلف الحكومات حول العالم بمستويات مختلفة للمراقبة والحجب.

ووفقا لما قاله ريان داف، وهو باحث في الأمن الرقمي وقائد تكتيكي للعمليات الرقمية في الولايات المتحدة، فإن "استغلال الشبكات الحاسوبية وشن الهجمات عليها هما شيئان مختلفان بالاستناد إلى الغرض من الاختراق وهو جمع البيانات الاستخباراتية".

وقال إن "الاستغلال يعني بالأساس القدرة على الولوج إلى الجهاز بغرض جمع البيانات، لذلك يجب أن تمتلك بعض البرمجيات، والبرامج الضارة، أو زرع أداة داخل ذلك الجهاز لمراقبته"، وقال أيضًا "الهجمات الشبكية تعمل أيضًا من خلال القدرة على الولوج ولكن لأغراض تدميرية، مثل مسح قرص صلب أو تدمير خادم، أو استخدام حواسيب مصابة من أجل إطلاق هجوم رفض الخدمة"، هذه الأنواع من الهجمات الشبكية مرتبطة بالأنشطة العسكرية أو لتغطية المهام الأمنية.

ولكن عديد من الحقائق تشير إلى أن الشركة تعمل في مجال التجسس، فقد انتدبت عددًا من أعضاء سايبربوينت، لديهم معرفة معمقة في كتابة الشفرات، وقادرين على إصابة مستخدمي تويتر وغيرها من المنصات للمساعدة في عمليات التجسس.

وقد قال موظف سابق للمجلة: "بحسب ما فهمته هناك بعض الأنواع من الأعمال الهجومية التي لم ترغب أو لم تتمكن سيابربونت من القيام بها لصالح الزبائن، والزبون يرفض أن يجابه بالصد، لذا عملت إلى إعادة هيكلتها حتى لا تتمكن أي شركة أجنبية من إهدار جهودها".

وأردف قائلاً: "هناك شيء واحد واضح جدًا، وهو أن الإجراءات الجديدة أجبرت العشرات من الموظفين على مغادرة الإمارات عوض الالتحاق بداركماتر، فبعض الذين غادروا تحدثوا عن سجل حقوق الإنسان في الإمارات العربية المتحدة، بما في ذلك الاعتقالات العشوائية وعمليات التعذيب والانشقاقات السياسية، وقد قال أحدهم إن المشكل مرتبط بحرية التعبير، وهي النقطة التي تعد حساسة".

السؤال الكبير المطروح الآن هو: هل استخدام داركماتر لأدوات "القرصنة" الأمريكية المتطورة قانوني أم لا خاصة وأنها من مشمولات قوانين التصدير الأمريكية؟

ووفق ما صدر في صحيفة واشنطن بوست، فإن وزارة الخارجية منحت سايبربوينت الإذن بتقديم المشورة للإمارات العربية حول الأمن الرقمي، ولكن هناك شخصان تحدثا مع ذي إنترسبت تساءلا حول ما إذا كانت داركماتر، التي على ما يبدو أنها قد ابتلعت عمل سايبربوينت في الإمارات في وقت لاحق، تندرج ضمن هذا الإذن.

خلال مكالمة هاتفية مع إيفا غالبرن، وهي محللة سياسية عامة في إلكتريك فرونتيار فاونديشن، ومستشارة تكنولوجية في فريدم فور براس فاونديشن أفادت أن "عالم التصدير الرقمي عالم ضبابي

وذلك بحسب ما تقوم به داركماتر الآن، كما أن مبيعاتها قد تخضع لقوانين عدة هيئات، كما كان من بين المنتجات تكنولوجيات التشفير، فهناك حواجز تمنع تصدير الأسلحة"، بينما أدوات الاختراق والثغرات ليس مقننة إلى ذلك الحد، وقال أيضًا "إن أردت شراء برمجية ضارة للمراقبة في الإمارات العربية، فلا شيء يمنعك من ذلك".

في المقابل، حاولت الولايات المتحدة تقنين هذا النوع من الأسلحة الرقمية، كما أراد العديد من موظفي حكومة الولايات المتحدة فرض المزيد من الرقابة من خلال القوانين، وذلك في استجابة لما قامت به شركة "هاكينغ تيم" التي باعت أدوات مراقبة لأنظمة قمعية غير أن نقاد هذا الاقتراح أشاروا إلى أن تلك التكنولوجيات قد تستخدم لأغراض شرعية مثل اختبار منتجات الأمن الرقمي أو تجربة اختراق الأجهزة.

ووفق غولبي غودمان، مدير مراقبة المساعدة الأمنية وخبير قوانين نقل الأسلحة، فالأمر غير واضح، بحسب مكان عمل داركماتر فربما تخضع لقانون التصدير، وإن كان العمل يتطلب تكنولوجيا أمريكية بالأساس أو خبرة تقنية في التشفير، فالترخيص يجب أن يصدر من قبل وزارة الخارجية الأمريكية.

وأضاف أن "أي موظف أمريكي يعمل على منتج يخضع للقانون سيحتاج إلى ترخيص تصدير، حتى إن انتقل إلى ما وراء البحار وبدأ العمل في شركة أجنبية"، وقد ضرب غولبي غودمان مثلاً ليوضح الأمر فقال: "لو كنت مواطنًا إماراتيًا وكنتُ أخبرك شيئًا خاضعًا لسيطرة قوانين الاتجار الدولي بأنظمة الأسلحة، فهذا يعتبر تصديرًا لذلك الشيء، إلا إذا كان لدي ترخيص بذلك".

وأردف قائلاً: "والأمر قياس مع المعلومات السرية، فلا يعني أن تغادر البلاد أنك ستنسى المعلومات السرية، وإن قدمتها إلى جهة أخرى فهذا يعتبر اعتداء".

كما رفضت وزارة الخارجية التعليق حول وجود "تصريح تصدير" صدر للتغطية على الشركة أو موظفيها، بما في ذلك تلك التراخيص السابقة لسايبربوينت، ولم تجب وزارة التجارة الأمريكية، التي صاغت بعض القوانين حول بيع الأجهزة الأمنية، عن سؤالنا ولو بتعليق، بينما قالت داركماتر من جانبها أنها حاصلة على تراخيصها الخاصة، ولكن لم تقدم تفاصيل أكثر.

وقد قال هالي، المتحدث باسم الشركة الإماراتية: "وفرت داركماتر لزبائنها تكنولوجيات تقدر قيمتها بمئات الملايين من الدولارات، من خلال الأمن العالي وبائعي التكنولوجيا، كما أن هناك عدد من هذه العقود يضمن مستوى عاليًا من الأنظمة الأمنية، طبقتها الشركة، حصلت على التراخيص من سلطات قضائية، من بينها في الولايات المتحدة الأمريكية ودول مختلفة في أوروبا".

جلس ممثلو داركماتر تحت بعض مظلات المعرض في صالة المؤتمرات في لاس فيغاس في شهر آب/ أغسطس، حيث كان أحدهم يحمل سيجارة ملفوفة يدويًا، وأمامهم قوارير الخمر، وديناصور آلي سيقدم كهدية لمن يفوز في لعبة المراهنة.

يقول مارجاريتيلي إن درجة الإصرار في الشركة لا نظير لها، فهي تسعى إلى إنشاء جيش من أجهزة الزومبي المصابة، تحت الطلب إن أُريد مراقبتها أو تعقبها

بدأت داركماتر في الظهور في مجال الأمن الرقمي في الولايات المتحدة في الأشهر القليلة الماضية – بما في ذلك مؤتمر بلاكهات، أكبر مؤتمر سنوي للأمن الرقمي والهاكرز في لاس فيغاس – بعد أن قدمت للحضور أقلامًا ومذكرات مزينة بشارة داركماتر، وقد قال ممثل الشركة إن "الشركة ما زالت منشغلة بالانتدابات".

في مدونته الخاصة كتب مارجاريتيلي في شهر تموز/ يوليو واصفًا اللقاء الذي أجراه في الإمارات، آملا في أن يقدم حسابه الخدمة لهؤلاء "الذين هم مثلي، وقد يجدون أنفسهم يومًا ما متورطين في عمل مشبوه بعلم مسبق سواء كان نسبيًا أو كليًا، أو هؤلاء الذين يبحثون عن عروض عمل تتطلب التواجد في الإمارات العربية المتحدة، فاعلم أنك ستقدم خصوصيتك والأهم من ذلك حريتك في التعبير مقابل المال".

ليس كل من حادثته وافق على وجهة نظر مارجاريتيلي، فقد قال الباحث الفرنسي في الأمن الرقمي مات سويش، الذي يعمل مع "كوماي تكنولوجيز" المنتصبة في الإمارات أيضًا: "كل الدول تسعى إلى امتلاك آليات المراقبة، وانتداب عمال أجانب ليس بالأمر الغريب في الإمارات، فالدولة تحاول ببساطة إنشاء قاعدة تكنولوجية خاصة بها"، وشبّه مهمته بأنها "مثل مهمة في مريخ الإمارات".

كما قال البعض ممن عملوا سابقا بسايبربوينت في الإمارات، إنهم لا يجدون مانعًا في القيام بأعمال الرقابة، وتعاملوا معها على أنها عمل ضروري لا يمكن تجنبه وهو سبيل طبيعي لدولة حديثة تواجه تهديدات الشرعية. وقد قال أحدهم لي: "لم أكن نزيهًا في العمل الذي قمت به".

ثم أضاف مصدرنا قائلًا: "استخدام الإمارات للرقابة بهدف تتبع مواطنيها أصبح أمرًا طبيعيًا"، واصفًا نفسه بالواقعية على الرغم من إقراره أنه حاول التقليل من تعرضه لبعض المهام التي قامت بها الشركة، وقال: "لا يمكن لوم رجل الحقيبة على عمل قدمته له".

ففي ردهة فندق لاس فيغاس في مؤتمر بلاكهات، تحدثت مع مارجاريتيلي حول شعوره بالإحباط من شركة داركماتر، الداعم البلاتيني للحدث، كانت بادية على "الهاكر" الإيطالي ملامح "هاكرز" الأفلام، بما في ذلك الثقوب الموجودة في أنفه ولسانه، والنظارة المستطيلة التي يضعها، والسيجارة التي يدخنها، كما أنه يتحاشى استخدام الهاتف الخلوي ولكنه أوجد طريقة للتواصل الرقمي.

مؤتمر البلاكهات في أمريكا في أغسطس 2015

ذهب إلى المدرسة لدراسة الفيزياء والهندسة ولكنه لم يكمل دراسته حتى الحصول على شهادة

علمية، كما أن لديه ذاكرة من صغيرة من الأرقام المحددة، وبعض المجالات الشبكية، والعناوين، والأشخاص، وقال إنه على الرغم من أن لغته الإنجليزية ليست جيدة، إلا أنه قادر على ترجمة النص الإيطالي إلى الإنجليزية في وقت صغير.

قال لي مارجاريتيلي إنه بدأ في الحذر من داركماتر منذ البداية، كان يعرف سمعة حكومة الإمارات العربية المتحدة بشأن حجز المنشقين أو اختفائهم وشرائها أجهزة مراقبة من دول أخرى، بالإضافة إلى أن لقاءه مع موظف الانتداب، الذي كان في وقت سابق يعمل مع شركة مثيرة هي الأخرى للجدل وهي شركة "فيرانت"، بدا عليه الاهتمام بأداة "باتركاب" – أداة "الهاكرز" التي اشتهر بها مارجاريتيلي.

قد يجادل بعض الباحثين ويدافعون عن مساعي داركماتر بالقول إنها تقوم بواجبها في الحماية الرقمية، يقول مارجاريتيلي إن درجة الإصرار في الشركة لا نظير لها، فهي تسعى إلى إنشاء جيش من أجهزة الزومبي المصابة، تحت الطلب إن أُريد مراقبتها أو تعقبها، وقال "الهاكر" الإيطالي: "في المستقبل القريب سيصبح كل جهاز في الإمارات العربية تحت سيطرتهم".

ثم كتب مارجاريتيلي في وقت لاحق عبر رسالة إلكترونية لي، قائلاً إنه عمل مع كل أنواع تكنولوجيات "الهاكرز"، ولكن يبقى مشروع داركماتر صادمًا، فهدفه مراقبة أمة بالكامل، كما تساءل قائلاً: "ماذا يريدون فعله؟ إنهم مجانين بحق".

المصدر: صحيفة ذي إنترسبت

رابط المقال : https://www.noonpost.com/14840/