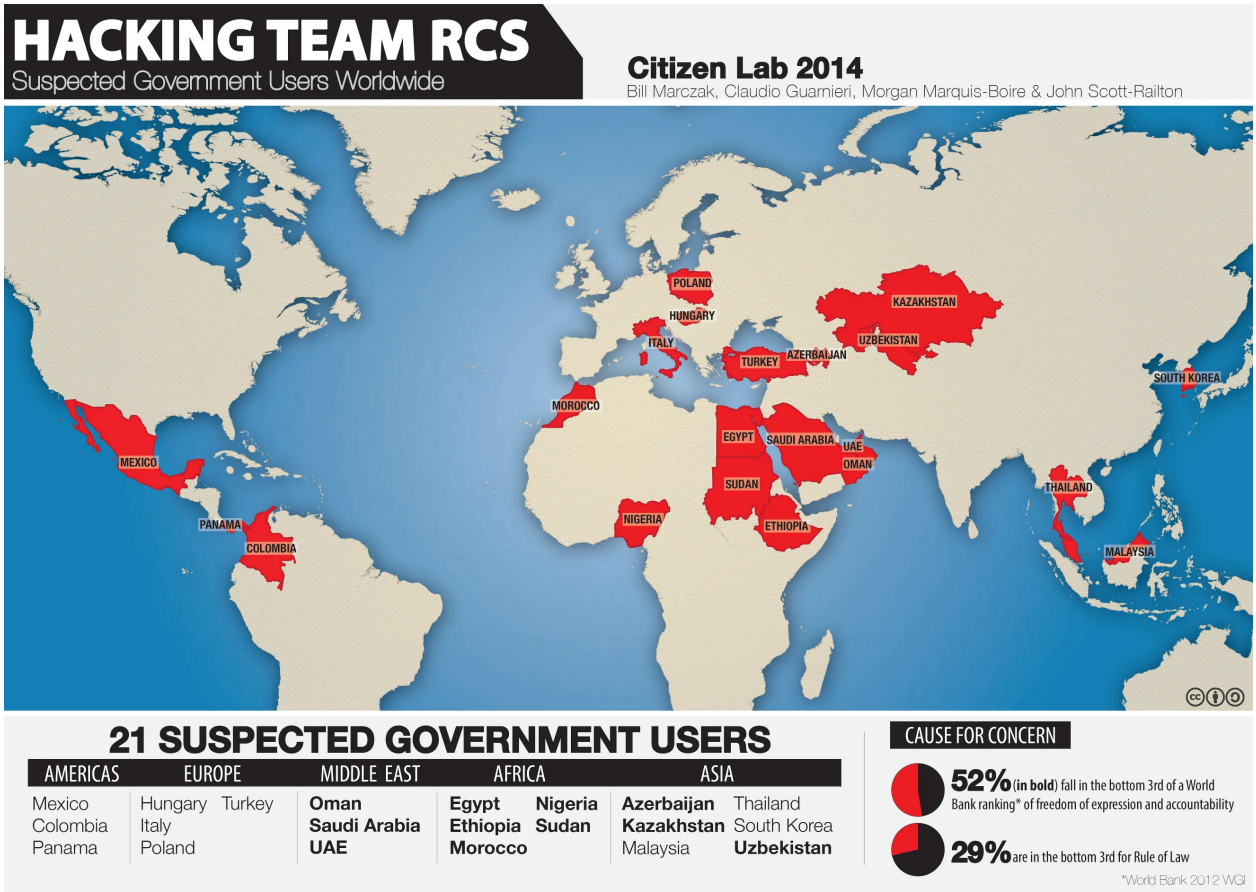
هاكينغ تيم: الشركة التي تعاقدت معها مصر والمغرب والسعودية للتجسس على مواطنيهم

كتبه فريق التحرير | 9 يوليو, 2015



في عام 2001، قام مبرمجان إيطاليان، هما ألبرتو أورناغي وماركو فاليري، بكتابة برنامج باسم "إتركاپ" Ettercap، كأداة للتجسس ومعرفة الكلمات السرية والتلاعب بأجهزة الكمبيوتر الخاصة بمستخدمين آخرين، وقد طُرِح البرنامج بشكل مفتوح لتتمكن الشركات التي تريد اختبار مدى سرية وأمان أنظمتها من استخدامه، كما شرع المخترقون بالطبع في استخدامه لأغراضهم الخاصة، وقد سمي آنذاك بـ "مطواة" العالم الافتراضي، وكأن دوره في عالم الإنترنت يماثل دور المطواة البسيطة والخطيرة في آن في العالم الحقيقي.

انتشر إتركاپ بقوة حتى تلقى مؤلفاه الإيطاليان مكالمة من الشرطة في مدينة ميلان، لا لأنها شعرت بالقلق من انتشار البرنامج بين المخترقين، ولكن لرغبتها هي في استخدامه للتجسس على المواطنين، وقد كان طلب الشرطة من أورناغي وفاليري أن يكتبا برنامجًا يتيح لها أن تستمع للمكالمات التي يتم

إجراؤها على سكايب، ولم تكن تلك بالطبع آخر المشاريع التي يخوضانها، حيث تمخضت عن تلك الجهود شركة باسم هاكينغ تيم تمتلك حاليًا حوالي 40 موظفًا وتبيع منتجاتها لعشرات الدول لتقتفي آثار مواطنيها الإلكترونية.

تغطي أنشطة الشركة حاليًا بيع برامج يمكن لها أن تخترق أي ملفات مشفرة بكلمات سرية على الإنترنت، بدءًا من البريد الإلكتروني الخاص بك وحتى مكالمات سكايب والمحادثات التي يقومون بها عبر فيسبوك أو غيره، وكذلك موقع أي مستخدمين وصلاته بغيره، كما يمكن لها عن بُعد أن تتلاعب بالمايكروفون والكاميرا الخاصة بأي كمبيوتر إن أرادت ذلك بعد اختراقه، وكل ذلك عبر برنامجها الأشهر "دا فينشي" الذي يستطيع فعل ذلك مع آلاف المستخدمين في نفس الوقت.

ديفيد فينشِنزيتي هو رئيس الشركة الحالي وأحد مؤسسيها، وهو عدو للإنترنت المُظلِم DARKNET كما يسميه، وهو ببساطة مجموعة البرامج الشبيهة بـ "طور" Tor التي تساعد النشطاء على استخدام الإنترنت بعيدًا عن رقابة الحكومات، وكان ولا يزال الوصول إلى نظام يسمح للشركة باختراق برامج كتلك هو أحد أبرز أهدافها، والتي تجعلها وثيقة الصلة بحكومات عدة حول العالم، وبالطبع باسم مكافحة الجريمة، كما يقول ديفيد في إحدى الرسائل المسربة مؤخرًا، "دارك نِت يسُتخدم في 99% من الحالات لتعزيز النشاطات الإرهابية والإجرامية وغير القانونية"، هكذا يقول ديفيد مبررًا جهود شركته.

لم يكن غريبًا إذن أن تصبح الشركة "عدوًا لحرية الإنترنت" طبقًا لتوصيف منظمة مراسلين بلا حدود، ولم يكن غريبًا أيضًا أن تصبح هي نفسها هدفًا للمخترقين، والذين نجحوا بالفعل في الدخول إلى بياناتها ونشرها على الإنترنت منذ أيام.

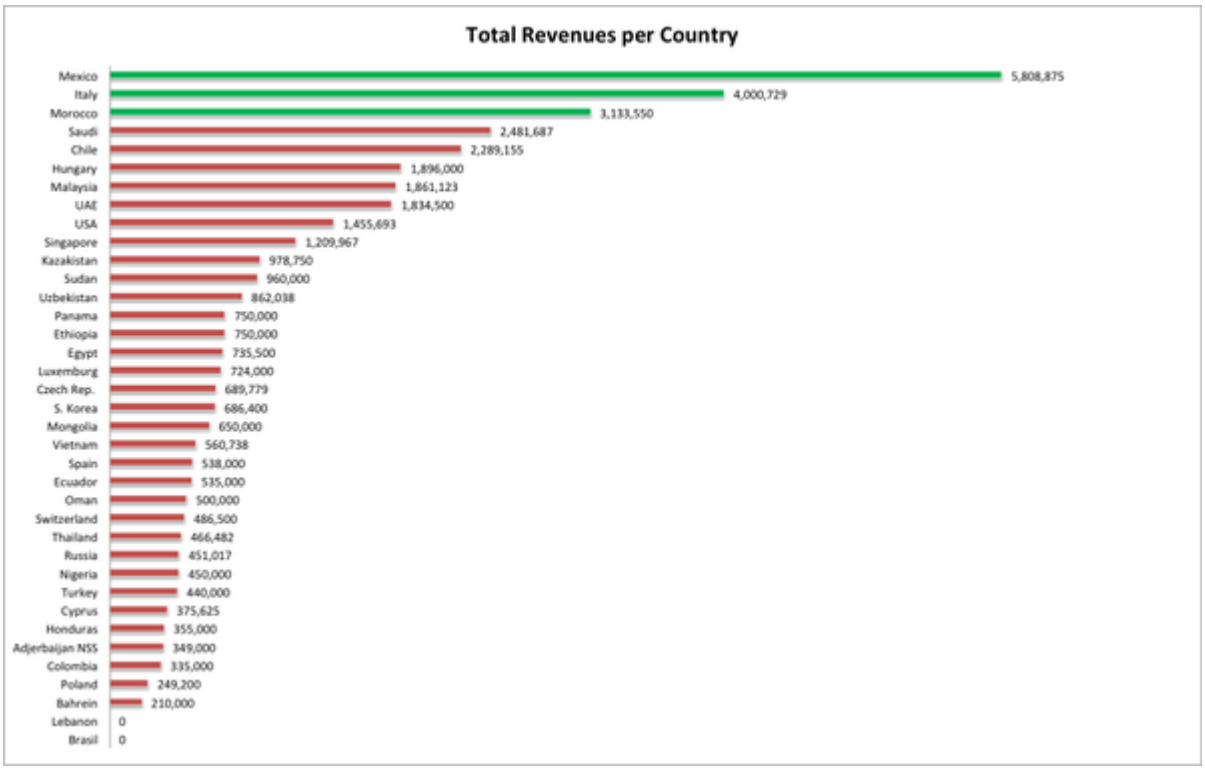
اختراق الشركة

قام المخترقون بتسريب حوالي 400 جيجابايت من الشفرات السرية والوثائق ورسائل البريد الإلكتروني والتسجيلات الصوتية والفواتير ووضعها على الإنترنت، كما اخترقوا حساب تويتر الخاص بالشركة، والذي استخدموه أيضًا لنشر بياناتها، وكذلك بعض حسابات تويتر للعاملين بها.

واحدة من أبرز الملفات المسربة هي قائمة لعملاء الشركة ومدة العقود التي وقعوها مقابل الحصول على خدماتها (والتجسس على مواطنيهم)، وهي القائمة التي تضم أذربيجان والبحرين ومصر وإثيوبيا وكازاخستان والمغرب ونيجيريا وعُمان والسعودية والسودان وغيرها، وعدة مؤسسات أمريكية مثل مكتب المباحث الفيدرالية FBI ووزارة الدفاع، وكذلك قائمة العملاء طبقًا لصافي الأرباح التي تعود بها على الشركة.

ALFAHAD-PROD	Morocco	Minister of Interior	12/31/2014	Active
CSDN-01	Morocco	Intelligence Agency	12/31/2014	Active
BSGO	Nigeria	Bayelsa Government	11/30/2013	Expired
ORF	Oman	Excellence Tech group Oman	12/31/2014	Active
PANP	Panama	President Security Office	5/31/2014	Expired
KVANT	Russia	Intelligence Kvant Research	11/30/2014	Not officially supported
GIP	Saudi Arabia	General Intelligence Presidency	12/31/2015	Active
MOD	Saudi Arabia	Minister of Difence	7/15/2015	Active
TCC-GID	Saudi Arabia	Genaral Intelligence Direcotrate	6/1/2015	Active
IDA-PROD	Singapore	Infocomm Development Agency	2/28/2015	Active
SKA	South Korea	The Army South Korea	12/31/2014	Active
NISS-01	Sudan	National Intelligence Security Servic	12/31/2014	Not officially supported
THDOC	Thailand	Thai Police - Dep. Of Correctoin	7/31/2014	Expired
ATI	Tunisia	Tunisia (demo)	7/3/2011	Expired
TNP	Turkey	Turkish Police	11/10/2014	Active
MOI	UAE	Minister of Interior	12/31/2014	Active

روسيا والسودان على قائمة لعملاء الشركة على عكس ما أنكرت، وبوضع غير رسمي كما يقول الملف المسرّب



أرباح الشركة من عملائها باليورو

"هؤلاء هم، إدوراد سنودن، عالم البرمجة والتجسس"، هكذا قال إريك كينغ نائب مدير شركة برايفاسي إنترناشونال Privacy International عمّن قاموا بالاختراق والتسريبات، "لطالما حاولت شركة هاكينغ تيم أن تخفي وتشوه الحقائق فيما يخص تعاملاتها مع الأنظمة الديكتاتورية، بيد أن هذا التسريب يلقي الضوء بوضوح على كل نشاطاتها، ويظهر نفاقها وكذبها المستمر".

من ناحيتها لم تعلق الشركة بشكل رسمي على التسريبات الأخيرة، بيد أن أحد موظفيها، وهو كريستيان بوتزي، قد دافع عنها على حساب تويتر الخاص به، وقال بأن الهجوم على الشركة غير دقيق، وأن الكثيرين يروجون أكاذيب عن الخدمات التي تقدمها الشركة، وهي تغريدات دفعت بالمخترقين على ما يبدو لاختراق حسابه هو شخصيًا، وإطلاق تغريدات ساخرة من خلاله، وهذه

لقطات من حساب كريستيان بوتزي قبل وبعد اختراقه

> #Hackingteam may be awake, but clearly groggy. Violating the 1st rule: Shut up and let the lawyers talk. pic.twitter.com/2JNcnGrm8S
>
> Paul D (@Paulmd199) July 6, 2015 —

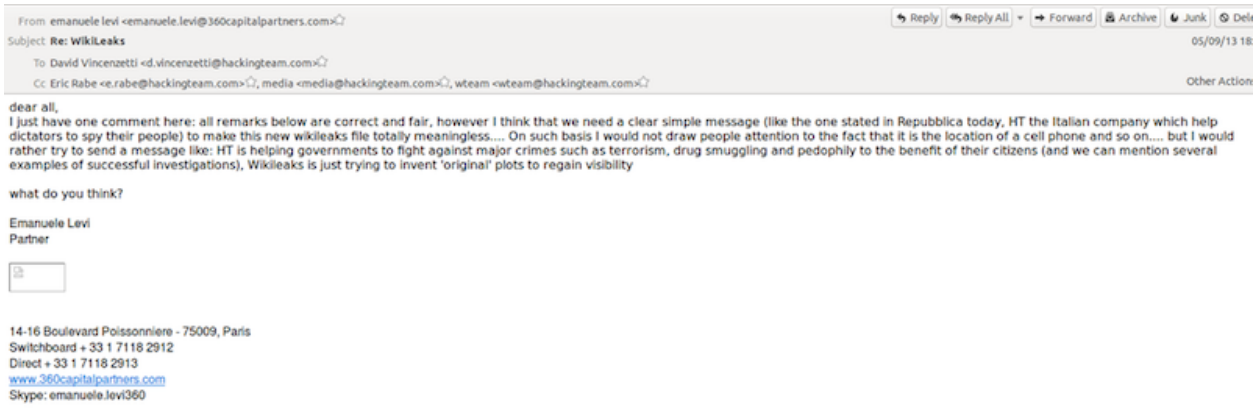
تغريدات من بوتزي دفاعًا عن الشركة قبل اختراق حسابه

> It seems Pozzi didn't even change his twitter password. #hackingteam. pic.twitter.com/r5bbf1Crhe
>
> Paul D (@Paulmd199) July 6, 2015 —

حساب بوتزي بعد اختراقه

ليس ذلك مجرد موقف فردي، بل إن الشركة قد حاولت وضع إستراتيجية لتحسين صورتها والرد على الادعاء بكونها شركة تساعد الحكومات في التجسس على مواطنيها، ونشر صورة مفادها أنها تقدم خدمات فقط لمكافحة الجريمة والإرهاب وغيرها، وهو ما تقوله إحدى الرسائل الإلكترونية المسربة منذ عام 2013 على إثر وقائع تسريبات ويكيليكس آنذاك، والتي يقول فيها أحد المرتبطين بالشركة:

> "علينا أن نبحث عن رسالة واضحة وبسيطة لكي تصبح تسريبات ويكيليكس الجديدة بلا أي معنى، كأن نقول بأن هاكينغ تيم تساعد الحكومات في مكافحة الإرهاب وتهريب المخدرات، وذلك لمصلحة مواطنيها، ويمكننا في هذا الصدد ذكر أمثلة ناجحة على قيامنا بذلك".



From emanuele levi <emanuele.levi@360capitalpartners.com>
Subject Re: WikiLeaks
To David Vincenzetti <d.vincenzetti@hackingteam.com>
Cc Eric Rabe <e.rabe@hackingteam.com>, media <media@hackingteam.com>, wteam <wteam@hackingteam.com>

Reply | Reply All | Forward | Archive | Junk | Dele
05/09/13 18:
Other Action

dear all,
I just have one comment here: all remarks below are correct and fair, however I think that we need a clear simple message (like the one stated in Repubblica today, HT the Italian company which help dictators to spy their people) to make this new wikileaks file totally meaningless.... On such basis I would not draw people attention to the fact that it is the location of a cell phone and so on.... but I would rather try to send a message like: HT is helping governments to fight against major crimes such as terrorism, drug smuggling and pedophily to the benefit of their citizens (and we can mention several examples of successful investigations), Wikileaks is just trying to invent 'original' plots to regain visibility

what do you think?

Emanuele Levi
Partner

14-16 Boulevard Poissonniere - 75009, Paris
Switchboard + 33 1 7118 2912
Direct + 33 1 7118 2913
www.360capitalpartners.com
Skype: emanuele.levi360

رسالة مسربة من الشركة تكشف محاولات الوصول لخطاب رسمي بخصوص تسريبات ويكيليكس يحفظ صورتها

على موقع مجلة فوربز المعروفة، كتب الصحافي توماس فوكس بروستر، المتخصص في الجرائم الإلكترونية والخصوصية وثقافات الاختراق، أن الشركة التي تتوسع بقوة داخل الولايات المتحدة وتتمتع بعلاقة قوية مع الحكومة الأمريكية، تهدف إلى تشكيل قدرات يمكنها اختراق برامج هواتف الآي فون الذكية، وبرامج أندرويد وجوجل، ومجموعة مختلفة من تطبيقات الهواتف المستخدمة على نطاق واسع، وهو ما يجذب اهتمام الحكومة الأمريكية بالتأكيد، وغيرها من الحكومات، أما بعد تلك التسريبات فلا نعرف حتى الآن كيف ستوثر على صورة الشركة وقدرتها على الاستمرار، وهو أمر ستكشف عنه الأيام المقبلة.

رابط المقال : https://www.noonpost.com/7440/