
المبادرة المصرية
للحقوق الشخصية
EGYPTIAN INITIATIVE FOR PERSONAL RIGHTS
كيف تعمل مجموعة
نايل فيش على اختراق
المجتمع المدني تقنيا؟
تقرير حول أكبر هجمة تقنية منظمة
لاختراق منظمات المجتمع المدني
ونشطاء مستقلين

كيف تعمل مجموعة نايل فيش على اختراق المجتمع المدني تقنيًّا

تقرير حول أكبر هجمة تقنية منظمة لاختراق منظمات المجتمع المدني ونشطاء مستقلين

تصميم: محمد جابر

المبادرة المصرية للحقوق الشخصية

14 شارع السراي الكبرى (فؤاد سراج الدين) -جاردن ستي، القاهرة.

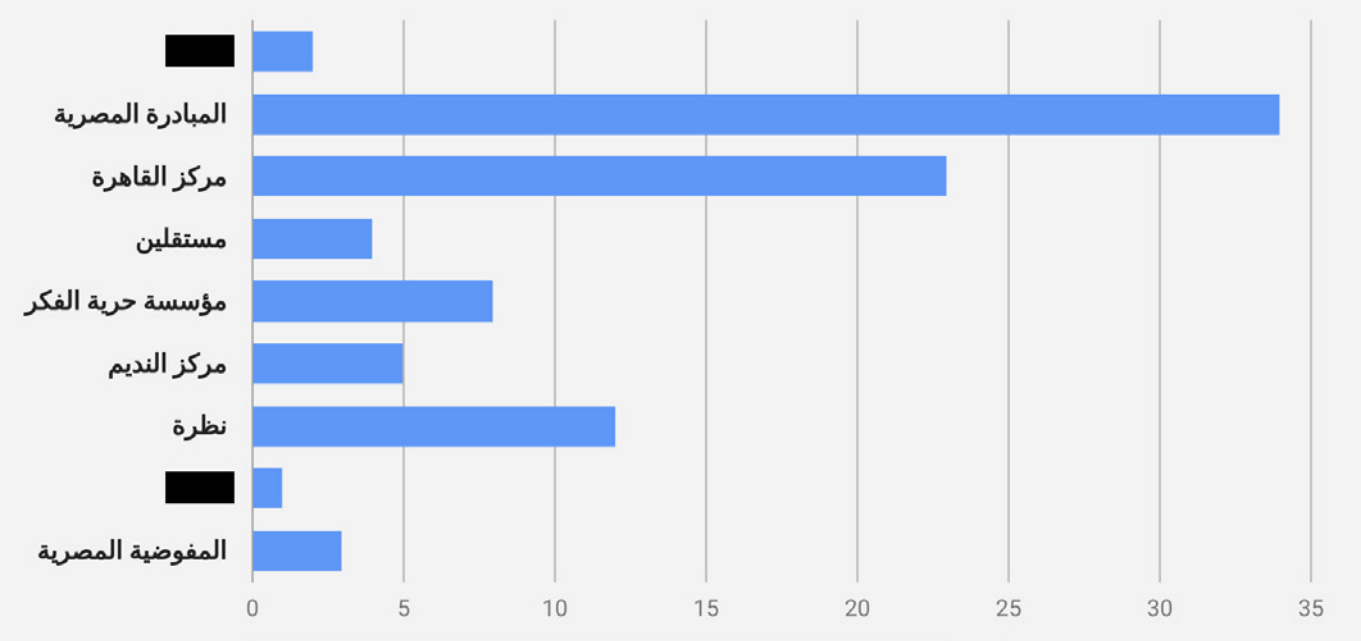
تليفون و فاكس: 27960158 / 27960197 (202)+

www.eipr.org - eipr@eipr.org

ملخص

- عدد الهجمات التي تم توثيقها على حسابات العاملين والعاملات في المنظمات محل البحث: 92.
- النطاق الزمني للهجمات محل البحث: 24 نوفمبر 2016 - 31 يناير 2017.
- الهجمات استهدفت الحسابات المؤسسية والحسابات الشخصية للعاملين والعاملات في المنظمات.
- القائمون بالهجمات اعتمدوا الهندسة الاجتماعية كوسيلة رئيسية لإلهاء المستهدفين باتخال هوية أفراد وصفة شركات مثل جوجل ودروبوكس وفيديكس للحصول على بيانات شخصية.
- بعد عدد من الهجمات المتتالية على الحسابات الشخصية تلقى بعض العاملين والعاملات إخطارًا رسميًّا من شركة جوجل بوجود فاعل حكومي يسعى لسرقة كلمة السر.
- بعض الهجمات اتسمت بتنسيق لا مثيل له بين القائمين بالاختراق وقوات الشرطة من حيث المزامنة في التوقيت.

من بين المنظمات المستهدفة وتوزيع الهجمات التي تم رصدها:



مقدمة

يقدم هذا التقرير رصدا وتحليلا لأكبر حملات الاختراق الإلكتروني عن طريق الاحتيال وأكثرها إتقانًا. تستهدف الحملة بالأساس المنظمات الحقوقية و النسوية المستقلة في مصر، والتي تتعرض أيضا إلى تضييق من الدولة فيما بات يعرف بقضية المجتمع المدني رقم 173، بالإضافة إلى حقوقيين مستقلين ومشتغلين بالصحافة. تمكن الباحثون من رصد 92 هجمة في الفترة من 24 نوفمبر 2016 إلى 31 يناير 2017 اعتمدت بالأساس على الهندسة الاجتماعية وبالتحديد على أحد تكتيكات انتحال الصفة يسمى الاصطياد phishing. يقدم الباحثون تحليلا طبيعة الهجمات والتقنيات المستخدمة والبنية التحتية، كما يطرحون قراءة تربط بين محاولات الاصطياد هذه واهتمام الدولة المصرية بالنطاق الرقمي والذي هو في تصاعد منذ أعوام. نهاية، يعرض التقرير الوضع القانوني للاختراق الإلكتروني من هذا النوع. يستخدم التقرير مسمى نايل فيش NilePhish لوصف القائمين بالحملة.

الهجمات التقنية

تعود بداية وقائع الهجمات التقنية إلى يوم 24 نوفمبر 2016، حين رُصدت دعوة أرسلت بالبريد الإلكتروني تنتحل صفة مركز النديم لتأهيل ضحايا العنف والتعذيب لمناقشة مسودة قانون الجمعيات الأهلية قبل إقرارها من البرلمان، وسردت الدعوة أن اللقاء بالشراكة مع منظمات حقوقية ونسوية مختلفة، تم استهداف بعضهم بعد ذلك في سياق نفس الهجمة.

وفي نفس الأسبوع لاحظ الفريق التقني لدى المبادرة المصرية استقبال فريق العمل مجموعة رسائل مشبوهة مكثفة في فترة زمنية محدودة مما أثار الحاجة إلى التحقيق في الأمر لبيان شبهة محاولة الاختراق. ومع زيادة كثافة الهجمات اتسع التحقيق التقني ليشمل النظر في هجمات استهدفت 7 منظمات مصرية من بينهم: المبادرة المصرية للحقوق الشخصية - مركز القاهرة لدراسات حقوق الإنسان - نظرة للدراسات النسوية - مركز النديم لتأهيل ضحايا العنف والتعذيب - مؤسسة حرية الفكر والتعبير - المفوضية المصرية للحقوق والحريات.

وانتهى التحقيق برصد وتوثيق 92 هجمة*، وتحليل طبيعة الهجمات والتقنيات المستخدمة والبنية التحتية للهجمات.

* تنويه: الأرقام الواردة وطرق الهجمات المذكورة في التقرير لا تعبر بالضرورة عن كل الهجمات والآليات والمستهدفين من المنظمات، ولكنها فقط تعبر عن ما تم رصده وتوثيقه في فترة زمنية محددة، ومنسوبة إلى مجموعة نايل فيش.

كيف تمت الهجمات؟

اعتمدت الهجمات محل الرصد التي وقعت في الفترة بين نوفمبر 2016 ويناير 2017 على الهندسة الاجتماعية، وهي إحدى مناهج الاختراق المعروفة التي تعتمد على السلوكيات الإنسانية لكسر حاجز الخصوصية والأمن، من خلال تنصيب مكيدة تعتمد على عنصر انتحال الصفة واستغلال ظرف ما للحصول على بيانات خاصة.

تعريفات تقنية مبسطة

- **الهندسة الاجتماعية:** عبارة عن تقنيات تواصل تهدف إلى تشجيع الناس على القيام بعمل ما أو الإفصاح عن معلومات شخصية ذات طابع سري أو طابع علني. وعادة ما تتسم أساليب الهندسة الاجتماعية بتحضير بيانات شخصية تساعد في إتمام المهمة قد تتضمن حصر العلاقات المهنية والاجتماعية، والحسابات الإلكترونية، وأرقام الهواتف، ومراقبة ما ينشره الشخص على مواقع التواصل الاجتماعي لرصد أسلوب الكتابة.. إلى آخره. وفي السياق الرقمي يتم تنفيذ الهجمة من خلال الهاتف أو البريد الإلكتروني عن طريق انتحال هوية شخص ذي سلطة أو شركة أو في منصب ما لتقليل إثارة الشبهات ويتم إرسال الأسئلة أو الصياغة التي عادة تكون محكمة وتطلب من المتلقي بيانات أو القيام بشيء ما. ومن بين أساليب الهندسة الاجتماعية ما يعرف باسم الاصطياد.

- **الاصطياد:** الوصول إلى معلومات خاصة بمستخدمي الإنترنت مثل المعلومات الشخصية أو البنكية أو كلمات السر، أو الموقع الجغرافي للشخص، أو بيانات نظام التشغيل على الحاسوب، عن طريق البريد الإلكتروني أو استمارات أو مواقع أو روابط، اعتمادا على انتحال هوية جهة ما. وبمجرد نجاح عملية الاصطياد تبدأ فعليا عملية الاختراق للحسابات باستخدام البيانات التي تم الوصول إليها.

- **اصطياد كلمات المرور:** اصطياد كلمات المرور تقنية بسيطة من حيث التكلفة المادية ودرجة التعقيد التقنية، بالمقارنة ببرمجيات اختراق الأجهزة. وهي الطريقة التي تم استخدامها في جميع الهجمات محل البحث في التقرير.

- **الاختراق:** يوجد أنواع كثيرة للاختراق تختلف تكلفتها ودرجة التعقيد التقني بها بناء على المراد اختراقه سواء كان حسابًا إلكترونيًّا أو حاسوبًا أو هاتفًا. وبطبيعة الحال فإن تقنيات الاختراق أكثر كلفة من تقنيات اصطياد كلمات المرور.

- **برمجيات خبيثة:** يقصد بها برمجيات تم تصميمها لإلحاق مستويات مختلفة من الضرر. ويستخدم مصطلح برمجيات خبيثة للإشارة إلى مختلف الأساليب الممكنة مثل: فيروسات - أحصنة طروادة.

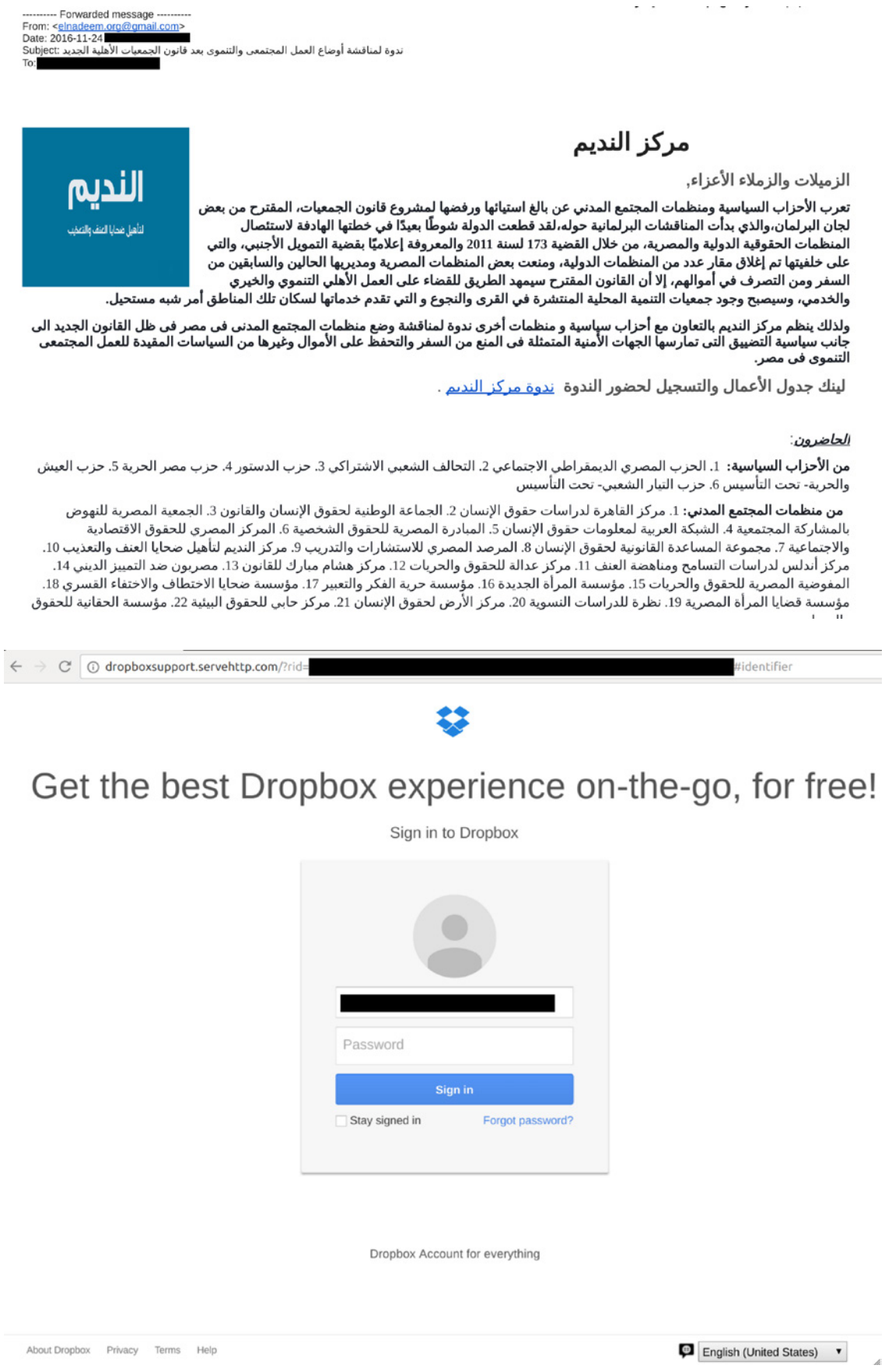
- **اختراق الحسابات:** قيام شخص أو جهة بالنفاذ إلى حسابات إلكترونية لشخص آخر من خلال سرقة كلمة السر، وقد يقوم المخترق باستخدام كلمات السر (التي حصل عليها من خلال الاصطياد) للنفاذ إلى الحسابات مع الإبقاء عليها دون تغيير أو مع تغييرها، وبالتالي عدم قدرة الشخص الأصلي على النفاذ وإدراك الاختراق. ويعتبر الإبقاء على كلمة السر دون تغيير في حالات الاختراق أشد خطورة حيث، فقد يقوم شخص بمطالعة البريد الإلكتروني لشخص آخر على مدار شهور بدون علم صاحب الشأن، وقد يعتبر هذا الأسلوب إحدى مصادر المعلومات للهندسة الاجتماعية لتطوير هجمة أكثر تعقيدًا.

- **اختراق الجهاز:** يتضمن وسائل مختلفة منها القيام بزرع برمجية خبيثة على الحاسوب أو الهاتف من أجل التحكم الكلي في الجهاز عن بعد والنفاذ في كل المحتوى بما فيها كلمات السر وفي هذه الحالة يتم زرع البرمجية من خلال إحدى أساليب الهندسة الاجتماعية لإقناع المتلقي بالضغط على رابط أو تنزيل ملف ما أو القيام بفعل مختلف، ويعتبر هذا النوع من أكثر الأنواع التقنية المعقدة والمكلفة. ومن بين الوسائل الأخرى البحث عن نقاط ضعف في إعدادات الحاسوب أو النظام أو الشبكة الداخلية لاستغلالها.

خريطة الهجمات

اعتمدت كل الهجمات على الهندسة الاجتماعية واستخدمت تقنية اصطياد كلمات المرور كوسيلة. ويمكن تقسيم إجمالي الهجمات إلى مرحلتين، اعتمدت المرحلة الأولى على استخدام قضية المنظمات كعنصر للمكيدة، واعتمدت المرحلة الثانية على انتحال هوية شركات شحن وشركة جوجل:

- بداية الهجمات كانت مع انتحال هوية مركز النديم وإرسال دعوة بالبريد الإلكتروني لمناقشة قانون الجمعيات الأهلية الجديد (قبل إقراره بأيام) واعتمدت الدعوة المزيفة على استخدام صياغات حقيقية صدرت سابقا عن مركز النديم ومنظمات شريكة لتبدو أكثر واقعية. وحملت الدعوة في نهايتها رابط لتسجيل الحضور والاطلاع على الأجندة وفي مرحلة من تتبع الرابط يطلب كلمة السر للقراءة ولكن ما يحدث فعليا هو إرسال كلمة السر إلى جهة الاختراق ولا يحدث شيء بالصفحة ولا يظهر الملف (صورة 1# للدعوة وصورة 2# الصفحة التي تظهر بعد الضغط على الرابط).



---------- Forwarded message ----------
From: <elnadeem.org@gmail.com>
Date: 2016-11-24 [redacted]
Subject: ندوة لمناقشة أوضاع العمل المجتمعى والتنموى بعد قانون الجمعيات الأهلية الجديد
To: [redacted]

النديم
لتأهيل ضحايا العنف والتعذيب

مركز النديم

الزميلات والزملاء الأعزاء,

تعرب الأحزاب السياسية ومنظمات المجتمع المدني عن بالغ استيائها ورفضها لمشروع قانون الجمعيات، المقترح من بعض لجان البرلمان،والذي بدأت المناقشات البرلمانية حوله،لقد قطعت الدولة شوطًا بعيدًا في خطتها الهادفة لاستئصال المنظمات الحقوقية الدولية والمصرية، من خلال القضية 173 لسنة 2011 والمعروفة إعلاميًا بقضية التمويل الأجنبي، والتي على خلفيتها تم إغلاق مقار عدد من المنظمات الدولية، ومنعت بعض المنظمات المصرية ومديريها الحالين والسابقين من السفر ومن التصرف في أموالهم، إلا أن القانون المقترح سيمهد الطريق للقضاء على العمل الأهلي التنموي والخيري والخدمي، وسيصبح وجود جمعيات التنمية المحلية المنتشرة في القرى والنجوع و التي تقدم خدماتها لسكان تلك المناطق أمر شبه مستحيل.

ولذلك ينظم مركز النديم بالتعاون مع أحزاب سياسية و منظمات أخرى ندوة لمناقشة وضع منظمات المجتمع المدنى فى مصر فى ظل القانون الجديد الى جانب سياسية التضييق التى تمارسها الجهات الأمنية المتمثلة فى المنع من السفر والتحفظ على الأموال وغيرها من السياسات المقيدة للعمل المجتمعى التنموى فى مصر.

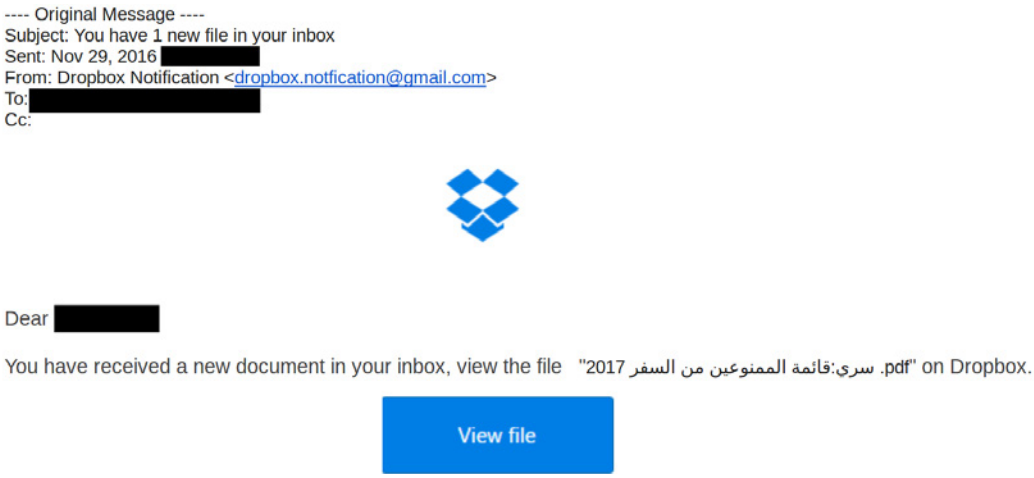
لينك جدول الأعمال والتسجيل لحضور الندوة ندوة مركز النديم .

الحاضرون:

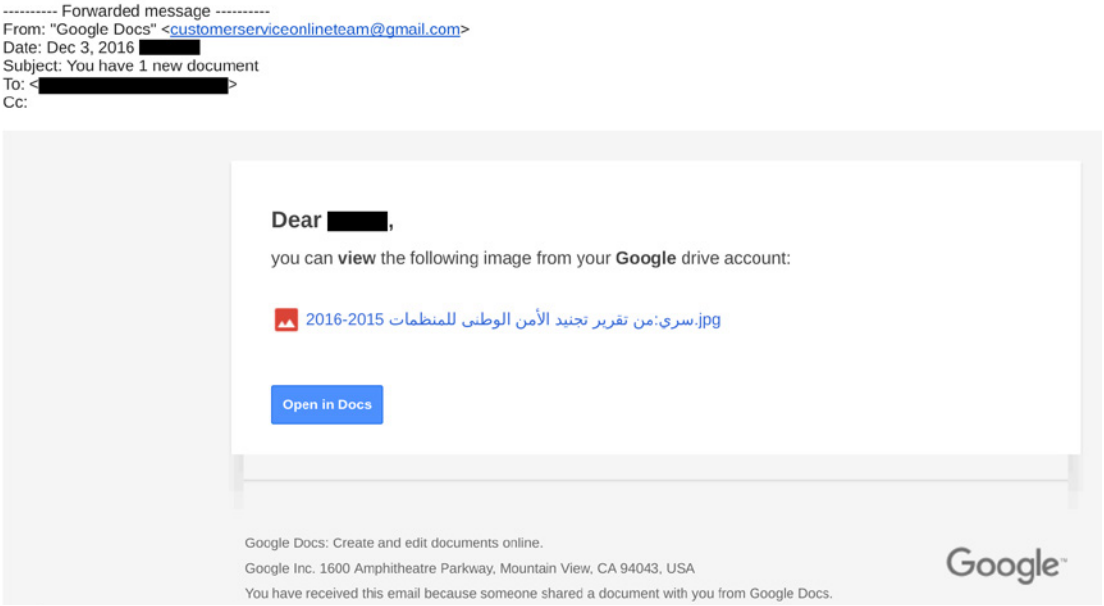
من الأحزاب السياسية: 1. الحزب المصري الديمقراطي الاجتماعي 2. التحالف الشعبي الاشتراكي 3. حزب الدستور 4. حزب مصر الحرية 5. حزب العيش والحرية- تحت التأسيس 6. حزب التيار الشعبي- تحت التأسيس

من منظمات المجتمع المدني: 1. مركز القاهرة لدراسات حقوق الإنسان 2. الجماعة الوطنية لحقوق الإنسان والقانون 3. الجمعية المصرية للنهوض بالمشاركة المجتمعية 4. الشبكة العربية لمعلومات حقوق الإنسان 5. المبادرة المصرية للحقوق الشخصية 6. المركز المصري للحقوق الاقتصادية والاجتماعية 7. مجموعة المساعدة القانونية لحقوق الإنسان 8. المرصد المصري للاستشارات والتدريب 9. مركز النديم لتأهيل ضحايا العنف والتعذيب 10. مركز أندلس لدراسات التسامح ومناهضة العنف 11. مركز عدالة للحقوق والحريات 12. مركز هشام مبارك للقانون 13. مصريون ضد التمييز الديني 14. المفوضية المصرية للحقوق والحريات 15. مؤسسة المرأة الجديدة 16. مؤسسة حرية الفكر والتعبير 17. مؤسسة ضحايا الاختطاف والاختفاء القسري 18. مؤسسة قضايا المرأة المصرية 19. نظرة للدراسات النسوية 20. مركز الأرض لحقوق الإنسان 21. مركز حابي للحقوق البيئية 22. مؤسسة الحقانية للحقوق

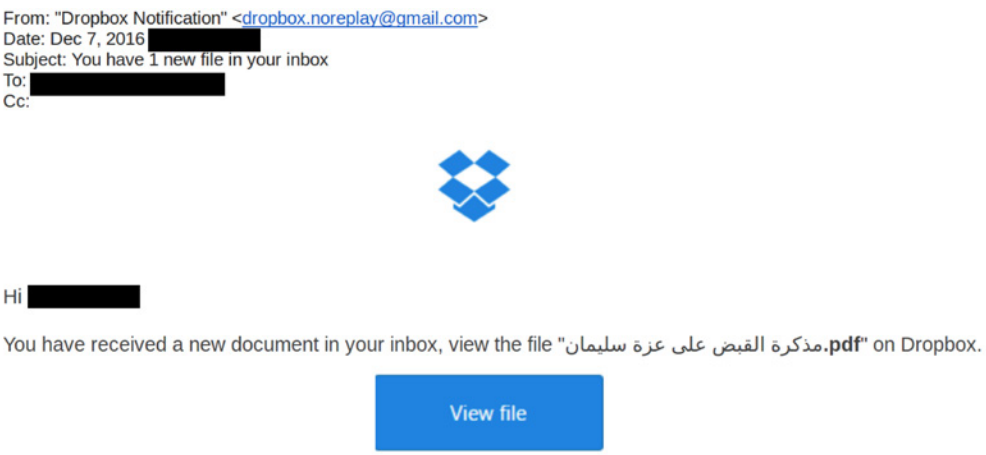
- ازدادت كثافة الهجمات على جميع المنظمات بالتزامن مع زيادة الأخبار والقرارات الخاصة بالمنع من السفر ضد العاملين والعاملات في منظمات حقوق الإنسان على خلفية القضية، ومن بين الهجمات التي وقعت توزيع رسالة إلكترونية تتضمن ملفًا وهميًّا بعنوان «سري: الممنوعين من السفر 2017». (صورة 3#)



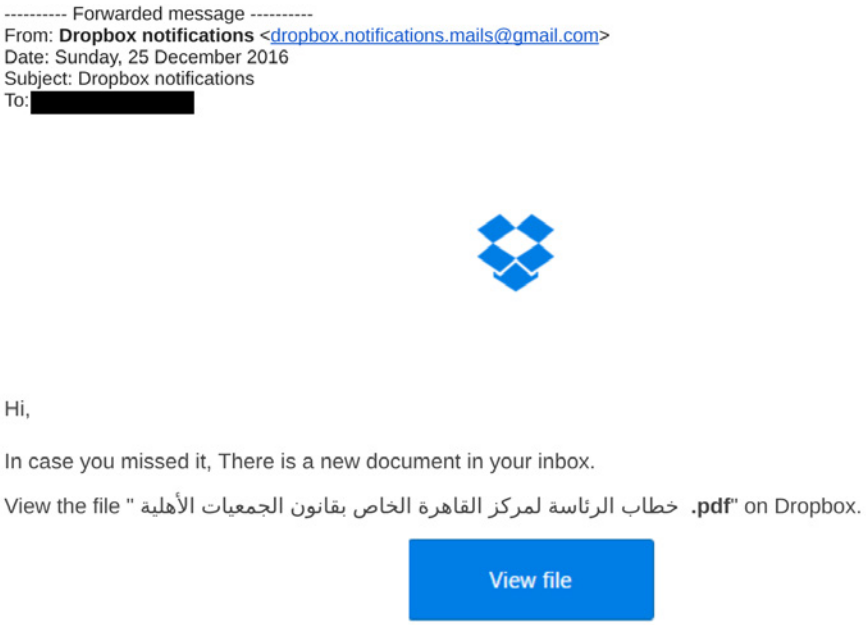
- ثم بدأت الهجمة التالية لتوزيع ملف وهمي باسم «سري: من تقرير تجنيد الأمن الوطني للمنظمات 2015-2016» صور #4).



- ومن بين الهجمات اللاتفة للنظر التي وقعت في نفس أسبوع الهجمة السابقة كانت يوم إلقاء القبض على المحامية الحقوقية عزة سليمان، مديرة مركز قضايا المرأة، يوم 7 ديسمبر 2016 في القاهرة، والتي تعرضت للمنع من السفر يوم 19 نوفمبر، حيث تم إرسال ملف وهمي باسم «مذكرة القبض على عزة سليمان » إلى مختلف المنظمات والنشطاء بعد ساعات قليلة من القبض عليها وقبل انتهاء التحقيق على خلفية قضية منظمات حقوق الإنسان وتم إخلاء سبيلها بكفالة في نفس اليوم، وبالتالي فإما أن يكون القائم بالهجمة فاعلًا حكوميًّا أو إما أن يكون هناك تنسيق قوي بين نايل فيش وجهة حكومية (صورة #5).



- في بعض الهجمات تم استهداف نشطاء وباحثين غير عاملين في المنظمات.
- وفي بعض الحالات رصدنا إعادة توزيع ملفات تحمل أسماء إنتاج حقيقي للمنظمات سواء كان تقريرًا أو بيانًا صحفيًّا ولكن بعد استبدال الروابط الحقيقية بروابط الهجمة (صور 6#).


---------- Forwarded message ----------
From: **Dropbox notifications** <dropbox.notifications.mails@gmail.com>
Date: Sunday, 25 December 2016
Subject: Dropbox notifications
To: [redacted]

Hi,

In case you missed it, There is a new document in your inbox.

View the file " خطاب الرئاسة لمركز القاهرة الخاص بقانون الجمعيات الأهلية **.pdf**" on Dropbox.

View file

- بعض الهجمات انتحلت هوية جوجل لإرسال تنبيهات وهمية لتأمين الحساب أو تنبيه باستخدام الحساب من جهاز جديد، وكانت جميع الرسائل تقوم بالإبلاغ عن وقائع وهمية (صورة 7#) وتطلب من المتلقي الضغط على رابط ما لتغيير كلمة السر بعد إدخال كلمة السر الحالية - والتي تصب بطبيعة الحال لدى طرف المخترق. كما تم انتحال هوية شركات مثل أرامكس وفيديكس وإرسال تنبيهات عن وجود شحنة وتطلب بيانات شخصية. ولاحظ الباحثون في بعض الهجمات وجود أخطاء لغوية في الصياغات (لاحظ الخطوط الحمراء في صورة 8#)

---------- Forwarded message ----------
From: **Support team** <secure.policy.check@gmail.com>
Date: Mon, Jan 2, 2017[redacted]
Subject: Unsuccessful login attempt
To: [redacted]

Google

Login failed

Hi [redacted]

We have recognize untrusted device trying login your account [redacted]

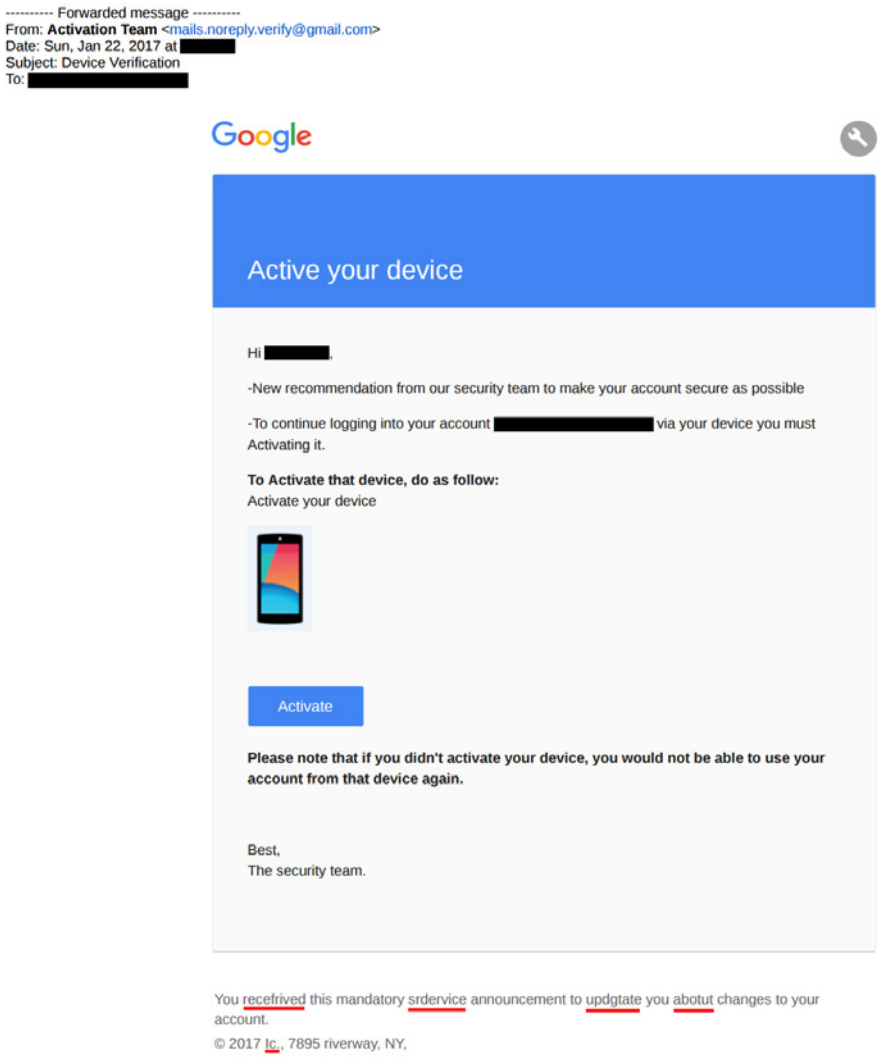
(login failed due to your complex password).

Click button below to get the location where the attempt to logon occurred.

location used	Egypt - December 26, 10:40 AM

Unknown device

Get Location



---------- Forwarded message ----------
From: **Activation Team** <mails.noreply.verify@gmail.com>
Date: Sun, Jan 22, 2017 at [redacted]
Subject: Device Verification
To: [redacted]

Google

Active your device

Hi [redacted],

-New recommendation from our security team to make your account secure as possible

-To continue logging into your account [redacted] via your device you must Activating it.

To Activate that device, do as follow:
Activate your device

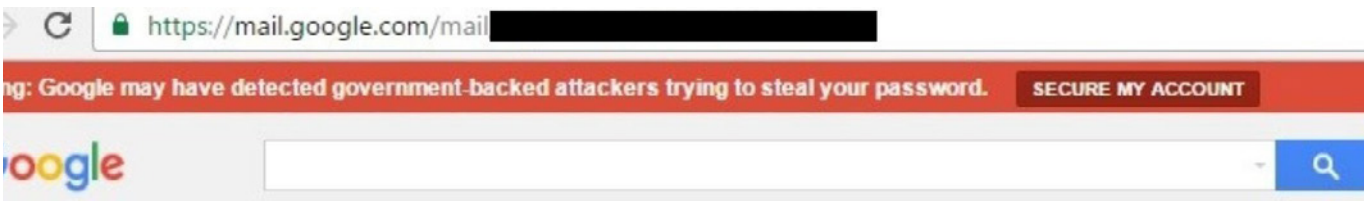
Activate

Please note that if you didn't activate your device, you would not be able to use your account from that device again.

Best,
The security team.

You recefrived this mandatory srdervice announcement to updgtate you abotut changes to your account.
© 2017 Ic., 7895 riverway, NY,

- في بعض الأحوال عند تعرض مستخدمي خدمة ما للهجوم أو محاولة الاختراق تقوم الشركة مقدمة الخدمة بإخطار المستخدم، وفي هذا الشأن تعتمد الشركات على معايير تقنية للدفاع ضد أغلب الهجمات الشائعة وتستخدم آليات فحص لمحاولة تحديد مصدر الهجمات من حيث البنية التحتية للهجمة ومصدرها الجغرافي وطريقة الهجوم. وفي بعض الهجمات محل البحث في التقرير تلقى عدد من العاملين والعاملات في منظمات المجتمع المدني يوم 14 ديسمبر 2016 تحذيرات رسمية من شركة جوجل بوجود فاعل حكومي يسعى لسرقة كلمة (صورة رقم 9# وصورة 10#) وتلك التحذيرات لا تظهر إلا إذا أدى تحليل مهندسي الشركة للهجمات إلى بنية تحتية يرجح أنها حكومية من حيث الكلفة ودرجة التعقيد ومعايير أخرى.



جدول 1 | أمثلة للهجمات

السياق	المنظمة المستهدفة	مصدر استضافة الهجمة
إرسال ملف «الممنوعين من السفر 2017»	المبادرة المصرية	dropboxsupport.servehttp[.]com
إرسال صورة ضوئية من «تقرير تجنيد الأمن الوطني للمنظمات»	مركز النديم مؤسسة حرية الفكر	googledrive-sign.servehttp[.]com
"خطاب ومذكرة قانونية إلى رئيس الجمهورية لوقف إصدار قانون العمل الأهلي"	مركز القاهرة	dropbox-sign.servehttp[.]com
تنبيه من جوجل بحجب محاولة تسجيل دخول إلى الحساب - تنبيه لتغيير كلمة السر - تنبيه تعقب جهاز	المفوضية المصرية المبادرة المصرية نظرة مؤسسة حرية الفكر	secure-team.servehttp[.]com
تنبيه بخصوص شحنة مرسلة	نظرة	aramex-shipping.servehttp[.]com
إرسال ملف "سري:بخصوص الحقوقية عزة سليمان" - إرسال ملف "مذكرة القبض على عزة سليمان"	مركز النديم مستقلين	dropbox-service.serveftp[.]com

جدول 2 | أمثلة للعناوين الإلكترونية مصدر الهجمات محل البحث

انتحال الصفة	اسم المستخدم الظاهر والبريد الإلكتروني
شركة جوجل (خدمة جيميل)	<Mail Support <mails.acc.noreply[@]gmail.com>, <Support Team <mails.noreply.verify[@]gmail.com>, <Support team <secure.policy.check[@]gmail.com>, <L'Equipe-des Comptes <user.protection45874[@]gmail.com>
شركة جوجل (خدمة درايف)	<Google Docs <customerserviceonlineteam[@]gmail.com>, <Google Drive <drive.noreply.mail[@]gmail.com>

شركة دروبوكس	<Dropbox notifications <dropbox.notifications.mails[@]gmail.com>, <Dropbox Notification <dropbox.noreplay[@]gmail.com>, <Dropbox <customerserviceonlineteam[@]gmail.com>, <Dropbox Notification <dropbox.notfication[@]gmail.com>
شركة فيديكس	<FedEx <fedex.noreply[@]gmail.com>, <FedEx Notification <fedexcustomers.service[@]gmail.com>, <Fedex Services <fedex.mails.shipping[@]gmail.com>, <FedEx Tracking <fedex_tracking[@]outlook.sa>
شركة أرامكس	<Aramex shipment <aramex.shipment[@]gmail.com>
مركز النديم	<elnadeem.org[@]gmail.com>

جدول 3 | أمثلة للنطاقات مصدر الهجمات محل الرصد

تم رصد النطاقات التالية من تحليل البنية التحتية للهجمات (إما تم استخدامها بالفعل في هجمات أخرى وضد مجموعات مختلفة، أو إما جزء من هجمات محتملة)	تم رصد النطاقات التالية من تحليل الهجمات:
device-activation.servehttp[.]com, docs-mails.servehttp[.]com, dropbox-verfy.servehttp[.]com, dropboxnotification.servehttp[.]com, fedex-notification.servehttp[.]com, fedex-s.servehttp[.]com, fedex-sign.servehttp[.]com, googledriver-sign.ddns[.]com, moi-gov.serveftp[.]com, notification-team.servehttp[.]com, quota-notification.servehttp[.]com, restricted-videos.servehttp[.]com, secure-alert.servehttp[.]com, securityteam-notify.servehttp[.]com, verification-team.servehttp[.]com, watchyoutube.servehttp[.]com,	mailgooglesign.servehttp[.]com, dropboxsupport.servehttp[.]com, fedex-sign.servehttp[.]com, googledrive-sign.servehttp[.]com, dropbox-service.serveftp[.]com, googledriver-sign.ddns[.]net, fedex-mail.servehttp[.]com, verification-acc.servehttp[.]com, dropbox-sign.servehttp[.]com, myaccount.servehttp[.]com, security-myaccount.servehttp[.]com, fedex-shipping.servehttp[.]com, aramex-shipping.servehttp[.]com, googlesecure-serv.servehttp[.]com, googlesignin.servehttp[.]com, googleverify-signin.servehttp[.]com, secure-team.servehttp[.]com, google-maps.servehttp[.]com, account-google.serveftp[.]com,

أي جهة وراء الهجمات؟

تقترح مؤشرات وجود رابط بين نايل فيش والسلطات. وفي حال افتراض أن القائم الفعلي بالهجمات ليس فاعلًا حكوميًّا فعلى أقل تقدير يوجد درجة من التنسيق المباشر مع السلطات. ومن بين تلك المؤشرات:

- تزامن الحملة الإلكترونية مع استهداف الدولة للمنظمات على خلفية قضية 173.
- المزامنة بين القوات الشرطية في القبض على عزة سليمان ونايل فيش من حيث استخدام ملف وهمي باسم "مذكرة القبض على عزة سليمان" لاختراق المنظمات، حيث يرجح وجود إخطار مسبق أو مشاركة معلومات للتحضير للهجمة التقنية.
- تحذيرات شركة جوجل بوجود فاعل حكومي وراء الهجمات، وهي تحذيرات تؤخذ على محمل الجد لأنها تعتمد على تحليلات فنية معقدة لا تستخدمها الشركة إلا إذا رأت ضرورة لذلك.

تكلفة وأدوات الهجمة

يصعب الجزم بالتكلفة للهجمات التي وقعت في الفترة نوفمبر 2016 ويناير 2017 خصوصا أن في هذه المرة لم يتم استخدام برمجية مكلفة للاختراق مثل استخدام برامج تابعة لشركات مثل هاكينج تيم وجاما الدولية التي تكلف ملايين الجنيهات، ولكن درجة التعقيد هذه المرة نابعة من توظيف الهندسة الاجتماعية على نحو مختلف وجديد. وبخصوص الأداة المستخدمة في الهجمات، كشف التحقيق التقني أن نايل فيش استخدموا برنامج اصطياد مفتوح المصدر يحمل اسم Gophish.

لماذا الاصطياد بتلك الطريقة؟

اعتمدت مجموعة نايل فيش في الهجمات على برنامج مجاني مفتوح المصدر متاح على الإنترنت يمكن لأي شخص أو جهة تعديله واستخدامه بحرية. ولم تستخدم المجموعة، في حدود البحث، تقنيات تجارية مكلفة مقفولة المصدر. ويرجح العدد الكبير للهجمات تفضيل نايل فيش استخدام وسيلة اصطياد كلمة المرور كمحور للهجمات لأنها غير مكلفة وتتيح تجربة الهجمات وإتمامها بدون قيد في الاستخدام أو عدد محدود مثل الحال في البرمجيات المكلفة التي يمكن أن تستخدم في الاختراق بشراء البرنامج ومواد الإصابة حسب عدد المستهدفين دون إتاحة مساحة للخطأ والتجربة مثل ما يمكن إتمامه مع برمجيات مفتوحة المصدر.

بالإَضافة إلى عنصري التكلفة وحرية الاستخدام، فلقد تعرض عدد من الشركات المهمة العاملة في مجال برمجيات الاختراق، وتتعامل حصريا مع جهات الأمن والاستخبارات حول العالم، لاختراق في الأعوام الماضية بما في ذلك إتاحة قواعد بيانات العملاء والتعاملات المالية والكود المشغل للبرمجيات ما يفقدها أي أهمية وفاعلية. قد يبدو أكثر فاعلية استخدام الميزانية نحو تطوير مجموعات محلية أقل تكلفة وربما أكثر فاعلية باستخدام تقنيات مفتوحة المصدر، وأسهل في تنسيق الهجمات.

جدير بالذكر أنه في أثناء تحليل الهجمات، لاحظ الباحثون في بعض الأكواد المرتبطة بالهجمة وجود تعليقات منسية بين فريق نايل فيش، ويرجح من اللهجة المستخدمة أن المجموعة من مصر.

هل يوجد سند قانوني للاختراق والاستهداف التقني؟

حرصت الحكومة في عهد "محلب" على تعزيز الإطار القانوني لتيسير مهام المراقبة وتحسين التعاون الأمني بين مختلف السلطات في الأمور التقنية.

- حيث قرر مجلس الوزراء في 15 ديسمبر 2014 إنشاء المجلس الأعلى للأمن السيبراني (قرار 2259 لسنة 2014).
- وفي فبراير 2015 أصدر مجلس الوزراء قرارا يهدف إلى منح المحاكم صلاحية النظر في محتوى الإنترنت.
- وفي مارس 2015 وافق مجلس الوزراء على مسودة قانون جرائم تقنية المعلومات (تعليق مشترك).
- وفي 30 إبريل 2015 قرر مجلس الوزراء تشكيل لجنة لتفعيل منظومة مراقبة بواسطة الكاميرات (قرار 1032 لسنة 2015).

وتتنوع أجهزة الاستخبارات المصرية بين أربع جهات: المخابرات العامة - إدارة المخابرات الحربية والاستطلاع - جهاز مباحث الأمن الوطني - هيئة الرقابة الإدارية. وبالنظر إلى القوانين المصرية لا يوجد نص مباشر يمنح القدرة القانونية على المراقبة أو التجسس في الأماكن الخاصة أو الاختراق، بدون إذن من النيابة، ماعدا هيئة الرقابة الإدارية التي وفقا لقانونها لها القدرة على استخدام الأدوات الفنية اللازمة لمراقبة الموظفين في الجهات التي تقع في نطاق سلطتها. وتشمل أجهزة الأمن القومي الجهات التالية: رئاسة الجمهورية - وزارة الداخلية - هيئة الأمن القومي - هيئة الرقابة الإدارية.

وبوجه عام يوجد في القانون المصري سند يسمح للسلطات بالتدخل المباشر في الشبكات والتحكم في البنية التحتية، مثلما حدث يوم 28 يناير 2011، حيث تنص المادة 67 من قانون تنظيم الاتصالات رقم 10 لسنة 2003 على: "للسلطات المختصة في الدولة أن تخضع لإدارتها جميع خدمات وشبكات اتصالات أي مشغل أو مقدم خدمة [...] وذلك في [...] وأي حالات أخرى تتعلق بالأمن القومي". ولكن لا يوجد أي سند قانوني يمنح السلطات حق ممارسة الاصطياد والاختراق ضد المواطنين.

لمحة تاريخية عن الموارد التقنية

شرعت الجهات الأمنية في تعزيز إمكانياتها التقنية منذ 2011 لتكون قادرة على استهداف أفراد بعينهم بالمراقبة وكذلك ممارسة المراقبة الشمولية على مواقع الإنترنت وخدمات الاتصالات بوجه عام، بدون ضرورة التعاون مع قطاع الاتصالات سواء كانت شركات هواتف المحمول أو مقدمي خدمات الإنترنت، مثلما جرت العادة في الفترات السابقة لعام 2011.

- كشفت اختبارات تقنية على شبكات الإنترنت في مصر تم إجراؤها بين 27 أغسطس و26 أكتوبر 2016 عن وجود ممارسات تقنية بهدف مراقبة خدمات الاتصالات الآمنة وتعطيلها في بعض الأحيان، وحقن أنشطة التصفح ببرمجيات ضارة.

- أشارت مراسلات إلكترونية عديدة، تم إتاحتها علانية في يوليو 2015 على خلفية اختراق شركة هاكيج تيم وهي واحدة من أكبر الشركات في مجال تقنيات الاستخبارات والمطور لواحدة من أقوى البرمجيات آنذاك، إلى اتفاقيات ومفاوضات (بدأت منذ إبريل 2011) بين جهات أمنية مختلفة في مصر من خلال شركات وسيطة لشراء برمجيات تسمح بزرع ملفات تجسس في الحواسيب والهواتف للتحكم فيها عن بعد والنفاذ في كل المحتوى. كما تشير بعض المراسلات (نوفمبر 2012) إلى رغبة السلطات في شراء معدات وبرمجيات واسعة النفاذ لاستخدامها في المنبع بإصابة مقدمي خدمات الإنترنت مباشرة.

- ومن بين أدوات المراقبة المستخدمة في البلاد حزمة عتاد بلو كوت التي يمكن من خلالها حجب خدمات ومواقع، ومراقبة أنشطة التصفح

بشكل عام وتتبعها. وأشار مسح تقني على أدوات بلو كوت على شبكة الإنترنت أجراه سيتزن لاب في النص الثاني من 2012 حتى مطلع 2013 إلى وجود عدد منهم في مصر.

- كما كشف مسح تقني على برمجيات هاكينج تيم على شبكة الإنترنت أجراه سيتزن لاب عن وجود استخدامات لتلك البرمجيات في مصر في الفترة بين 10 مارس 2013 و29 أكتوبر 2013.

- وفي وقت سابق كشفت وثائق، تم إتاحتها علانية في الربع الثاني من 2011، عن علاقات تعاقدية بين جهات أمنية وشركة جاما (وهي الشركة المنافسة لهاكينج تيم) لشراء واستخدام واحدة من برامجها وتبين من تلك المستندات أن الجهات الأمنية كانت على تواصل مع شركة جاما منذ على الأقل أغسطس 2009.

تنويه

- هذا التقرير يستند إلى جهود بحثية بواسطة فريق بحثي مشترك من المبادرة المصرية للحقوق الشخصية وسترن لاب بمدرسة مونك للشؤون الدولية في جامعة تورنتو. يمكن مطالعة التقرير التقني بالإنجليزية هنا.

- الأرقام الواردة وطرق الهجمات المذكورة في التقرير لا تعبر بالضرورة عن كل الهجمات والآليات والمستهدفين من المنظمات، ولكنها فقط تعبر عن ما تم رصده وتوثيقه في فترة زمنية محددة، ومنسوبة إلى مجموعة نايل فيش.

للإبلاغ

- إذا تلقيت رسالة إلكترونية من إحدى العناوين المذكورة أعلاه أو باستخدام إحدى طرق الخداع المماثلة فرجاء تمرير الرسالة كما هي إلى العنوان التالي nilephish@eipr.org.

قراءات ومراجع

- تقرير يتناول بأدلة تقنية وجود معدات بلو كوت المستخدمة في المراقبة والتعقب حول العالم بما فيها مصر - صادر عن ستزن لاب التابع لجامعة تورنتو العامل في مجال التكنولوجيا وحقوق الإنسان ويختص في فحص الشبكات عن برمجيات المراقبة - يناير 2013 - التقرير.

- تقرير يتناول بأدلة تقنية وجود برمجيات هاكينج تيم حول العالم التي كانت تعتبر واحدة من أخطر وأقوى تقنيات الاختراق لدي أجهزة الأمن، ومن بين مستخدمي البرمجيات مصر - صادر عن ستزن لاب - فبراير 2014 - التقرير.

- تقرير يتناول عينة من قدرات الجهات الأمنية والموارد التقنية لديها - صادر عن منظمة الخصوصية الدولية - فبراير 2016 - التقرير.

- قرار رئيس مجلس الوزراء بتشكيل لجنة لتعديل القوانين المتعلقة بالأمن القومي لمنح المحاكم صلاحية البت في محتوى شبكة الإنترنت في مصر. تاريخ قراءة المرجع 27 يناير 2017.

- خلفية عن قضية منظمات المجتمع المدني 173: تعود وقائع الحملة ضد المنظمات في مصر إلى يوليو 2011 عند قيام مجلس الوزراء بتشكيل لجنة لتقصي الحقائق للنظر في التمويل الأجنبي بواسطة وزير العدل وتم إدراج التقرير من بين الأدلة ضد المنظمات. في 2012\2013 تم استهداف المنظمات الأجنبية العاملة في مصر وفي يونيو 2013 حكمت إحدى محاكم الجنايات بالقاهرة على 43 من العاملين المصريين والأجانب في بعض المنظمات الأجنبية بالسجن لمدد تتراوح بين سنة و5 سنوات، وكانت معظم الأحكام غيابية، أما العاملون المصريون الذين ظلوا داخل البلاد فقد حصلوا على أحكام بالسجن لمدة عام واحد مع وقف التنفيذ. ومنذ ذلك الحين يتم التلويح بالقضية كل فترة لتهديد المنظمات الحقوقية والنسوية المستمرة في عملها، وعلى مدار 2016 تم تصعيد الملاحقة القانونية ضد المنظمات الحقوقية والنسوية باستخدام قرارات المنع من السفر، وتجميد الأموال، والأمر بالإغلاق، والاستدعاء للاستجواب.