cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

العدد ٢

أكتوبر/تشرين الثاني ٢٠١١

cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

للإتصال بنا:

magazine@cyber-arabs.com

تابعنا على:

أخرج المجلة:

MGSA

لصالح شركة:

tm

مقدمة

سوزان فيشر

هذا هو العدد الثاني المنتظر من «Cyber Arabs»، المجلّة التي تعنى بالأمن الرقمي وخاصة في العالم العربي. نتقدّم بالشكر من جميع الذين ساهموا في إبداء آرائهم وملاحظاتهم المتعلّقة بالعدد الأول. تعليقاتكم الإيجابية وإقتراحاتكم كانت حقاً بمثابة تشجيع وإلهام.

منذ أطلاق موقعنا الإلكتروني ونشرنا مجلة «Cyber Arabs» في وقت سابق من هذا العام كنا نعمل على إضافة العديد من الميزات الجديدة وعناصر الإعلام الإجتماعي. بإمكانكم إيجاد «Cyber Arabs» على مواقع التواصل الإجتماعي مثل «فايسبوك» و«تويتر»، ونحن نأمل بمتابعتكم لنا على هذه المواقع وذلك من أجل إستخدام الأدوات اللازمة لنشر «علم الامن الرقمي»، خاصة أن نشرالأمن الرقمي يحتاج الى مجتمع مدرك للمخاطر والتهديدات التي تتربّص به على شبكة الانترنت.

تذكّروا دائماً أنّ أمنكم متعلّق بدرجة مباشرة بأمن الحلقة الأضعف في شبكتكم. هذا يعني أنّ عدم إدراك الناس الذين تعملون وتتواصلون معهم لأهميّة حماية أنفسهم قد يعرّض أمنكم للخطر حتى في حال إستعمالكم لجميع الأدوات الصحيحة وإتخاذكم الإحتياطات اللازمة. لهذا من مصلحتكم ومصلحتهم أيضاً أن تتعلّموا ويتعلّم أصدقاؤكم وجميع افراد شبكة إتصالاتكم الالكترونية، عن الطرق الصحيحة للحماية والوقاية عند استعمال الانترنت.

أما المنتدى فهو ميزة أخرى من ميزات الموقع الاكتروني. ونحن نشجعكم على استعماله من أجل طرح الأسئلة، وتبادل الخبرات مع الناشطين الآخرين والصحفيين وذلك للحديث عن المخاطر والتهديدات المكتشفة حديثاً وتقديم الإقتراحات حول الأداة التي تفضلونها على وجه الخصوص. حيث يمكنكم طرح المواضيع، والأسئلة والمشاكل الأمنيّة الإلكترونية التي تريدون التحدّث والمناقشة حولها. عندما تقومون بتوجيه سؤال في المنتدى سنحاول طرحه على خبير مختص وذلك للحصول على إجابة سريعة وتفصيليّة وسهلة الفهم في آن واحد. إنضموا للمنتدى اليوم وابدأوا بطرح الأسئلة واجراء المحادثات، فمن الممكن أن تساهموا في انقاذ ناشط في المستقبل.

أخيراً وليس آخراً، نحن منفتحون على أية أفكار ومقالات جديدة أو حتى اقتراحات، وفي بحث دائم عن مساهمين جدد. ولذلك اذا كنتم تهتمون بالمواضيع المتعلّقة بالأمن الرقمي وتودّون الكتابة عنها فما عليكم سوى إخبارنا. أرسلوا إلينا أفكاركم وسنقوم بالإجابة عليكم على التأكيد.

أما الآن فتمتّعوا بالعدد الثاني من مجلة «Cyber Arabs». نرجو أن تزوّدكم هذه المجلّة بالعديد من النصائح المفيدة والأدوات، وتجعل حياتكم وعملكم كنشطاء أو صحفيين أو مدوّنين أو حتى مجرّد مستخدمين للإنترنت أكثر أمناً وسهولة.

سوزان فيشر – مديرة برنامج الشرق الأوسط لدى «معهد صحافة الحرب والسلام» (IWPR)

عشر أخطاء تقنية يقع بها ناشطو الإنترنت.

لا يوجد معايير إلكترونية ثابتة تؤمن لك الحماية بنسبة ١٠٠٪ ولكن، توجد عدة خطوات إحترازية بإمكانك اتباعها وإعتبارها جزءً روتينياً من عملك الإلكتروني على جهاز الحاسوب، والتي بدورها تستطيع توفير حماية لا يستهان بها لك ولغيرك من الأشخاص الذين تتواصل معهم.
تختلف النقاط بحسب استخدامك للإنترنت، فمن الممكن أن تساعد الأشخاص العاديين المتصفحين للانترنت، او المحررين والمراسلين او هؤلاء الأشخاص الذين يمتلكون أرشيفاً من البيانات قد يعرضهم للخطر.

١. التصفح من المقاهي

أحمد أحد الناشطين العاملين على الإنترنت، ينشط على صفحته على الفيس بوك بالإضافة إلى مدونة يعمل على نشر تدويناته عليها. في إحدى المرات تحدثت مع احمد عبر الدردشة وتفاجئت

بإنه متواجد في مقهى للانترنت في منطقته، وانه يستخدم احد الحواسيب الموجودة في المقهى.
الدخول إلى الإنترنت وخصوصاً للناشطين من مقاهي الإنترنت يعتبر انتحاراً سريعاً، حيث ان جميع الأجهزة مجهزة بما يسمى Key logger وهي برامج خبيثة تقوم بتسجيل ما يتم كتابته على لوحة المفاتيح من كلمات سر ومحادثة ويتم تقسيم ما يكتب بحسب البرنامج المستخدم، بالاضافة إلى كون الأداة الخبيثة تقوم بتصوير سطح المكتب وإرسال البيانات جميعها على شاكلة تقرير للجهات الأمنية فوراً. ونجد في دمشق العديد من حالات الإعتقال للناشطين من مقاهي الإنترنت، لذا من المفضل عدم إستخدام الإنترنت من المقاهي وفي حالات الضرورة من الممكن استخدامها عن طريق جهازك المحمول المزود ببرامج تشفير للاتصال.

٢. استخدام الحاسوب بدون الجدار الناري Firewall

يعتبر الجدار الناري من اهم البرامج التي يجب ان تتوافر على الحواسيب الشخصية للناشطين: وظيفة الجدار الناري هي أيقاف الهجمات القادمة من خارج الشبكة والتي تحاول استغلال الثغرات الموجودة في حاسوبك، بالاضافة إلى إغلاق الطريق امام البرامج الخبيثة التي قد تتواجد على حاسوبك وتحاول إرسال البيانات الى جهات معينة. وقد تتفاوت البيانات التي يتم تسريبها ما بين ما يتم كتابته على لوحة المفاتيح، والمواقع التي يتم زيارتها بالاضافة لسجلات كاملة عن النشاط القائم للمستخدم.

٣. استخدام برامج البروكسي بدون التشفير

انتشرت مجموعة من البرامج الخاصة لكسر المواقع المحجوبة كبرنامج Ultra surf الذي يمّكن المستخدم من فتح المواقع المحجوبة، ولكن المشكلة تكمن بأن هذا النوع من البرامج لا يوفر حفظ الخصوصية. فجميع المواقع التي يتم زيارتها والنشاط الذي يتم مزاولته عبر الإنترنت مكشوف بالنسبة للسلطات المسؤولة عن المراقبة، لذا ينصح باستخدام برامج تشفير الاتصال كبرنامج Tor الذي يقوم بتشفير البيانات الصادرة من جهازك ومن ثم الوصول لإحدى الأجهزة المزودة ببرنامج Tor خارج نطاق الدولة ليتم فك التشفير هناك. وبعد عودة الطلب لنفس الجهاز يتم تحويل الطلب مشفراً لجهازك والذي بدوره يقوم بفك التشفير واظهار نتيجة طلبك.

٤. استخدام برامج البريد الإلكتروني مثل الأوتلوك

يعتبر برنامج الأوتلوك وغيره من برامج جلب البريد الإلكتروني

واجهات مكشوفة وغير آمنة من عدة جهات. فبمجرد إجراء المصادقة والتحقق من كلمة السر وإسم المستخدم، تقوم مخدمات البروكسي الخاصة بالسلطات بمعرفة العنوان الذي يتم فتحه بالاضافة لتسجيل كلمات السر. لذا لا ينصح نهائياً باستخدام هذه البرامج ويفضل فتح البريد عبر واجهات الويب وباستخدام برامج التشفير كبرنامج Tor.

٥. التعامل مع البريد الألكتروني

كثرت في الآونة الاخيرة عمليات سرقة حسابات البريد الإلكتروني، والتي من الممكن ان تقع عن طريق البرامج الخبيثة والتي اشرنا لها في فقرة (الجدار الناري)، بالاضافة إلى الصفحات المزورة والتي تعتبر الاكثر انتشاراً.

لذا يجب الانتباه وعدم فتح أي رابط او ملفات مرفقة تأتيك من اشخاص ليس لديك الثقة الكاملة بهم، بالإضافة إلى عدة خطوات احترازية تتلخص بما يلي:

i. فحص جميع المرفقات ببرنامج مكافحة الفايروسات قبل الإقدام على فتحها.

ii. اهمال جميع المرفقات التي ترسل كتطبيقات.

iii. في حال قمت بفتح رابط تم إرساله لك وظهرت واجهة البريد الإلكتروني التي تتطلب منك إدخال إسم المستخدم وكلمة السر، قم بالتحقق من العنوان في الأعلى إن كان كالتالي على سبيل المثال بريد الغوغل : https://mail.google.com. وإن كان الرابط مغايراً لهذا فهو مزور. نقطة مهمة أخرى: بما أنك قد قمت بتسجيل الدخول أصلاً فلماذا يطلب منك البيانات مرة آخرى؟ لذا فهي روابط مزورة قم بإهمالها فوراً.

iv. إهمال الرسائل غير المرغوب بها Spam والتي تتضمن إعلانات ونشرات شهرية او أسبوعية، وقم بحذفها دون العودة لها او فتح اي من محتوياتها.

v. قم بحفظ السؤال السري وبيانات البريد الإلكتروني كالمواليد وغيرها، فهي السبيل الوحيد لإستعادة البريد في حال تمت سرقته.

vi. غير كلمة السر الخاصة بك كل فترة وإجعلها معقدة.

٦. ترك المحفوظات والملفات المؤقتة

يقوم بعض الناشطين بترك المحفوظات والملفات المؤقتة التي تم تحميلها والإنتهاء منها، هذا عمل غير آمن. فعندما تصادر السلطات الأمنية أجهزة الحواسيب،

تستطيع تحليل المواقع التي يتم زيارتها بالاضافة إلى كشف البيانات الموجودة على الحاسب مما يؤدي الى كشف النشاط الخاص بالشخص. لذلك يجب حذف المحفوظات والمواقع التي تم زيارتها بالاضافة إلى ملفات الكوكيز وكلمات السر المحفوظة والتخلص من الملفات الموجودة في الـ Downloads التي تم تحميلها والإنتهاء منها سابقاً.

وفي حال تم استخدام برنامج التشفير Tor المزود بمتصفح فايرفوكس خاص به والذي يعتبر آمناً ١٠٠٪ لكونه عند إغلاق المتصفح، يقوم من تلقاء نفسه بحذف المحفوظات والمواقع التي تمت زيارتها.

٧. استخدام برامج المحادثة بدون تشفير

تعتبر برامج المحادثة كـYahoo – Windows Live Messenger Messenger من البرامج المكشوفة لمخدمات البروكسي والجدران النارية الخاصة بالسلطات، لذا من السهولة كشف المحادثات ما بين

الناشطين، أي معرفة مجريات المحادثة بالإضافة إلى الجهات التي يتم الحديث إليها. لذلك ينصح بعدم إستخدام برامج المحادثة الواردة من الشركات الأم لكونها غير مشفرة، وينصح باستخدام برامج تشفير محادثة كـ Pidgin الذي من الممكن تحميله مجاناً من الموقع www.pidgin.im والذي بدوره سيتحول إلى بديل عن جميع برامج التراسل الموجودة لكونه يستطيع فتح محادثات اغلب الشركات كـGoogle - Facebook – Windows Live -Yahoo .

٨. عدم تشفير الملفات الموجودة على وحدات التخزين

قد يمتلك الناشطون مجموعة من الملفات التي تعرضهم للخطر، كملفات الفيديو او نسخ من وثائق معينة، مقالات الخ...، لذا من غير المعقول ترك الملفات على وحدات التخزين الخاصة بالحاسوب، او الأقراص المنقولة بدون تشفير. وبدوره تعتبر برامج التشفير

من أفضل الوسائل التي تقدم هذه الخدمات، حيث انها تقوم على إنشاء مجلدات غير مرئية ومخفية ومشفرة، يتم فتحها بواسطة برنامج ومن ثم يتم إدخال كلمة السر، عندها يستطيع الناشط رؤية الملفات وإجراء التعديل عليها.
ينصح ببرنامج Truecrypt المجاني ومفتوح المصدر وهو الأشهر على الإطلاق الذي يقوم بإنشاء محركات أقراص مشفرة يستطيع الناشط بواسطتها تشفير اجزاء من القرص الصلب ، او وحدات التخزين المحمولة. ومن الممكن تحميل البرنامج الذي يعمل على كافة انظمة التشغيل (ويندوز – لينوكس – ماكنتوش) من الموقع التالي www.truecrypt.org

٩. من الممكن استعادة الملفات بعد الحذف – إذاً كيف السبيل إلى تدميرها؟

عندما تقوم بحذف بعض الملفات من على وحدات التخزين بغض النظر عن نوعها، يستطيع المستخدم إستعداتها عن طريق إحدى برامج استعادة الملفات. عندما تقوم بحذف ملف ما، فإن الملف لم يتم حذفه في الظاهر إنما تم تحرير المساحة التي يستغلها وبإمكانك الكتابة عليها، لذا عندما تقوم بالكتابة على تلك المساحة يتم عندها الإستغناء عن الملف (المحذوف سابقاً) المتواجد على تلك المساحة. لذلك يجب إستخدام برامج خاصة بالحذف النهائي، كبرنامج Eraser المجاني، الذي يقوم بحذف الملفات نهائياً مع عدم إمكانية استعادتها. استخدام البرنامج بسيط جداً، وبإمكانكم تحميله من على الرابط eraser.heidi.ie

١٠. استخدام برامج إدارة المواقع بدون تشفير

يمتلك أغلب ناشطي الإنترنت مواقع إلكترونية يقومون بإدارتها، لذا قد يستخدم الناشطون ما يسمى بتطبيقات الـ FTP التي تقوم بتقديم خدمة رفع الملفات الى المخدمات الخاصة بالموقع. من الخطأ استخدام تلك التطبيقات بدون تشفير، حيث أن مخدمات البروكسي الخاصة بالسلطة تستطيع كشف جهة الاتصال والجهة التي يتم الاتصال بها بالاضافة إلى اسم المستخدم وكلمة السر مما يعرض المخدم كاملاً لخطر الإختراق والناشط لكشف هويته. لذلك ينصح باستخدام برنامج Tor وربط البرنامج الخاص بالـ FTP ببرنامج تور، على سبيل المثال برنامج FileZilla المجاني. بإمكانك تحميله من الرابط http://filezilla-project.org وبعد التحميل قم بفتح البرنامج، أختر إعدادات من قائمة التحرير، من ثم ملقم وكيل عام، حدّد الخيارSOCKS في مربع الملقم الوكيل. قم بكتابة الرقم التالي ١٢٧.٠.٠.١ ، ثم اكتب في مربع منفذ الملقم الرقم ٩١١٨ ، بعد الانتهاء افتح برنامج Tor ودعه يعمل، عد لبرنامج الـ Filezilla واستخدمه بشكل آمن.
أغلب المواقع تمتلك لوحة تحكم يتم الدخول إليها عن طريق الروابط، على سبيل المثال، www.example.com/admin لذا ينصح بعدم الدخول إلى رابط الإدارة إلا عن طريق برامج التشفير كـ Tor حيث انه وبكل سهولة تستطيع السلطات كشف الشخص الذي يقوم بإدارة هذا الموقع وتحديد هويته، بالاضافة إلى إمكانية الحصول على كلمة السر واسم المستخدم وتدمير الموقع.

• تعتبر الخطوات العشر التي تم تناولها مجموعة شبه متكاملة للحماية الشخصية. في حال تطبيق نقطة وإهمال أخرى يكشف الناشط عن نفسه ويصبح في خطر. لذلك يتوجب تنفيذ كل تلك الخطوات بشكل متكامل واعتبارها جزءً من خطوات التعامل مع الإنترنت في سبيل الحصول على الحماية القصوى التي ستقلل من احتمال تعرض الناشطين للإعتقال.

كاردوخِ كال.

مشكلة المشاركة في كلمة السر، تحايلات، وإقتراح حل

ميراي رعد

المشاركة الحقيقية، في مجتمع الانترنت، بحاجة إلى مشاركة صادقة، ناشطة وآمنة من الجميع، إلا أن هناك دائماً الصراع على السيطرة، لا سيما حينما يتعلق الأمر بإسم الموقع الالكتروني (domain names) والإستضافة (hosting) وحساب «تويتر» وتسجيل الدخول، الخ..

عادة يقوم صاحب فكرة الموقع أو الصفحة بإعداد المصادر المختلفة اللازمة لما سبق، غير أن التعاون الحقيقي لا يعني أن صاحب(ة) الفكرة «يمتلك» ما يصدر عن المجتمع الافتراضي، أو أن له صلاحيات أكبر في التعاطي معه. فهذا النوع من السيطرة قد لا يشجع الناس على الانخراط في مشروع ما، أو أنه على الأقل يقلل من نسبة إندماجهم فيه. من جهة أخرى، ليس آمناً ولا ذكياً ولا فعّالاً أن تتم مشاركة كلمة السر مع أشخاص كثر. فماذا لو قرر أحدهم تغييرها؟ أيذهب كل العمل هباء؟

هكذا، تبدو مسألة الثقة مهمة جداً، والأهم علاقتها بالتعاون/التشارك. فإذا كان صاحب الفكرة يثق بالشخص «أ»، فذلك لا يعكس أن «أ» استحق تلك الثقة عن جدارة، أي بالمشاركة والأفعال، وبالتالي أنه أهل ليدير موقعاً أو صفحة أو شبكة. يجب على «المدير» أن يكسب ثقة المجتمع الافتراضي، إلى جانب ثقة صاحب المشروع، فهذا هو المهم.

إذاً، وبالنسبة إلى «شخص لطيف يحاول أن يكون مدير موقع جيد»، فإنه يحمل عبء ومسؤولية القرار بشأن من يسيطر. ومن جهة ثانية، يستحيل العمل على تحديث منتديات التواصل الاجتماعي (البريد الالكتروني، تويتر، فايسبوك، البلوج، فليكر، يوتيوب...)، والبقاء على إتصال مع المجتمع الافتراضي، والقيام فعلاً بالرد والتشارك مع الآخرين... كل ذلك، في الوقت نفسه، وعلى المدى الطويل.

وتخلق مسألة كلمة السر مشاكل أخرى أيضاً تهدد المشروع المُنشأ، في حال إعتقل مدير الموقع مثلاً، أو فقد الاهتمام، أو إذا كان لا يملك الوقت الكافي، وغيرها من المعوقات. إلى جانب أن حصر كلمة السر في شخص واحد يعيق إمكانيات الفكرة من أساسها، إذ ليس بوسع أي إنسان أن يجاري مجتمعاً الكترونياً قد يبلغ تعداده مئات الآلاف.

كما أن فتح حساب متعدد لأكثر من مدير موقع ليس ممكناً دائماً، فهل سبق لك أن سمعت عن إمكانية التسجيل بأكثر من اسم في حساب «تويتر» نفسه مثلاً؟ بل إنها ليست فكرة جيدة، ونكرر، لأن أي «مدير موقع» يمكنه أن يمحو أو يقصي الآخرين.

أقدم لكم هنا تحايلاً لتفادي الإشكاليات المطروحة في هذا الموضوع، لكني أيضاً أود أن أقترح حلاً فعّالاً.

التحايل للتفادي:

هناك أداة ممتازة باسم Last Pass لإدارة كلمات السر. مع هذه الأداة يمكنك أن تحسن إدارة مسألة كلمات السر، بل ويمكنك أيضاً أن تتشاركها بطريقة مشفرة مع أشخاص آخرين، ومن دون أن يعرفوا هم كلمة السر الخاصة بك. فهم فقط يقبلون أن يتشاركوا معك في كلمة السر التي تقترحها عليهم، ويمكنهم تسجيل دخولهم باستخدام الفأرة على Last Pass. هذه طريقة مفيدة للدوران حول المشكلة الأساسية، لكنها لا تحل مسألة «الملكية» ولا تتضمن عملية تتيح اتخاذ قرار بشأن من يمكنه حيازة حق تسجيل الدخول.

الحل المقترح:

أقترح الحل التالي، والذي يجب البدء بترتيبه من الصفر مع التركيز على الأمور التشاركية:

١) افتح ملفاً تشاركياً

٢) حدد عدد المدراء الذين يحتاجهم الموقع.

٣) حدد نوع التشارك: تشارك كامل، أم تشارك جزئي.

٤) كل من يملك الرابط للملف التشاركي يمكنه أن يرشح و/أو يصوّت لشخص.

٥) يتم الاتصال بأصحاب الأسماء التي تحظى بعدد معين من الأصوات، ويُعطى لهم رابط – وكل شخص يدخل جزءاً من كلمة السر. لا يعرف أي منهم كلمة السر كاملة، ولا يحوز أي منهم لوحده سيطرة مطلقة. وتضمن بهذه الطريقة أيضاً أنه، إذا اعتقل أحدهم، فإن السلطات لن تتمكن من الحصول على كلمة السر وبالتالي لن تدخل الموقع.

٦) باستخدام ملحق من نوع Last Pass – يمكن للأشخاص المذكورين أعلاه تسجيل دخولهم.

يبقى أن نذكّر بأن الأشخاص الذين فازوا بأعلى نسبة تصويت يمكن تغييرهم بشكل أوتوماتيكي، كل فترة (يتم الاتفاق على مدتها)، وبالتالي تضمن هذه العملية تداولاً منصفاً لإدارة الموقع.

للمذيد من المعلومات والتحميل: أنقر هنا

متصفح الويب

متصفح الويب هو برنامج يسمح للمستخدم بإستعراض مواقع وصفحات الإنترنت ومحتويات أخرى مختلفة، هذه المحتويات تكون في الغالب مخزنة في مزودات ويب وتعرض على شكل صفحة في موقع على شبكة الويب أو في شبكة محلية. النصوص والصور في صفحات الموقع يمكن أن تحوي روابط لصفحات أخرى في نفس الموقع أو في مواقع أخرى. متصفح الويب يتيح للمستخدم أن يصل إلى المعلومات الموجودة في المواقع بسهولة وسرعة عن طريق تتبع الروابط.

هناك العديد من متصفحات الويب، ابرزها: مايكروسوفت إنترنت إكسبلورر، موزيلا فايرفوكس، سفاري، جوجل كروم، وأوبرا. وطبعاً كل مستخدم يفضل متصفحاً على آخر ويحاول إقناع معارفه بأن هذا المتصفح هو أفضل من غيره، وهو الأسرع، كأنه يشجع فريق كرة قدم معين! إلا أننا نستطيع القول بأن جميع هذه المتصفحات جيدة ومتقاربة من حيث السرعة والأمان، لكن من المهم جداً إستخدام احدث الإصدارات وتحديثها دوماً.

وتجدر الإشارة بأن معظم برامج التصفح متوافرة باللغة العربية، وتعمل على معظم أنظمة التشغيل مثل لينكس وماك والويندوز.

موزيلا فايرفوكس:

فايرفوكس برنامج مفتوح المصدر. خضعت النسخة الجديدة من فايرفوكس إلى تعديل جذري من ناحية الشكل فهي بسيطة لا تشبه سابقاتها، قابلة للتعديل من قبل المستخدم لتتناسب مع زوقه، كتعديل الالوان والصورة الخلفية. كما أنه مزود بمزايا عديدة لم تكن متوفرة في النسخ السابقة. يتمتع كباقي المتصفحات بنظام حماية متطور، وقد زود بنظام منع التعقب.

يتميز فايرفوكس بالإضافات المتعددة التي يمكن إضافتها أو ما يعرف بال «add-on»، فيما لا تزال إضافات فايرفوكس ٦ قليلة مقارنة مع فايرفوكس ٣ وذلك لأن فايرفوكس ٦ لا يزال جديداً ويتم تطوير الإضافات لتناسبه.

وفايرفوكس يتمتع بمدقق إملائي: حيث أنك أثناء كتابتك داخله، أو بشكل عام أثناء كتابتك في أي مربع نص، فإن المدقق الإملائي يعمل معك بشكل تلقائي، لتجد أنه يضع لك خطوط حمراء تحت الكلمات الخاطئة وبكبس زر الفأرة الأيمن على ذات الكلمة، تظهر لك قائمة بالبدائل.

في حال إغلاقه بشكل غير طبيعي أو فجائي فإن البرنامج يقوم بإستعادة جلسة العمل، وإستعادة الصفحات التي كانت قيد التصفح أو كانت مفتوحة داخله وذلك في أول مرة يعاد بها تشغيله.

انترنت إكسبلورر:

اطلقت شركة مايكروسوفت متصفح انترنت إكسبلورر ٩ وهو متميز عن النسخات السابقة من ناحية الشكل والسرعة وخاصة الأمان، لكنه متوفر فقط للويندوز ٧ وفيستا. يتميز بنظام حماية جيد وحديث جداً، وهو مزود بنظام حماية ضد التعقب والفيروسات. وتمكّنك الحماية من التعقب من تقييد اتصال المتصفح بمواقع ويب معينة للمساعدة في الحفاظ على خصوصية معلوماتك.

الإدارة المحسنة للوظائف الإضافية: يخبرك «مرشد الوظائف الإضافية» عما إذا كانت هناك وظيفة إضافية تعمل على إبطاء أداء المستعرض الخاص بك، كما يسمح لك بتعطيلها أو إزالتها؛ مما يساعدك على ضمان بقاء أداء المتصفح سريعاً على الدوام.

يمكن مشاهدة هذا الفيديو الذي يشرح عن متصفح الويب:
youtube.com/watch

أوبرا ١١:
يتميز اوبرا بسهولة الإستخدام ودعم ذوي الاحتياجات الخاصة مثل الذين لديهم عاهات بصرية أو حركية كما انه متصفح متعدد الوسائط ويقدم الكثير من التفضيلات للمستخدم في الواجهة الرئيسية. تسمح الصفحة بتكبير النصوص والصور والمحتويات الأخرى لمساعدة ضعيفي البصر أو لأسباب أخرى مثل صغر حجم الخط. وهناك إمكانية الاستماع إلى طريقة نطق الكلمات أو الجمل. كل ما عليك فعله هو كبسة على اليمين ونطق speak . ومن الجدير بالذكر وجود مترجم وقاموس وتفقد الأخطاء أثناء الكتابة. ويستطيع المستخدم أيضاً أن يحفظ أوبرا على الذاكرة الومضية «flash memory» لإستعماله على حاسوب آخر.
من الممكن إضافة كلمة سر للمتصفح اوبرا حيث لايمكن لاحد الدخول اليه. وذلك يؤمن حماية لمعلومات المستخدم الشخصية.

اوبرا يونيت Opera Unite:
يسمح للمستخدمين بتشغيل موقع ويب كخادم افتراضي بالإضافة إلى مشاركة ملفات الموسيقى والفيديو والدردشة مع الآخرين. عملية المشاركة تبدأ بإختيارك الملفات التي تريد مشاركتها ثم تحديد خيارات المشاركة: اما عامة للجميع أو خاصة أو محمية بكلمة سر، بعدها يقوم Opera Unite بإنشاء رابط مباشر يمكنك مشاركته مع الاخرين، كما أن المستخدمين الآخرين يمكنهم ان يشاهدوا الملفات المعروضة للمشاركة من اي متصفح متصل بالإنترنت وليس فقط من متصفح لصديق أو جهاز كمبيوتر تعرفه مسبقاً أو تواصلت معه من قبل.

اوبرا توربو Opera Turbo:
ميزة وجدت اساساً لمتصفح اوبرا على الهاتف المحمول. لكن بعد ذلك قامت شركة اوبرا بإضافة هذه الميزة لمتصفح اوبرا على الحاسوب لتعطي اصحاب الإتصالات البطيئة سرعة أكبر. وتعتمد خاصية Opera Turbo على تنفيذ عمليات ضغط الصفحات إلى الثلث أو الربع مما يقلل من حجم البيانات المنقولة إلى ٨٠٪ في بعض الحالات.

اوبرا لينك Opera link:
يتيح لك مزامنة مواقعك المفضلة انشأ حساب مجاني في اوبرا لينك وسيقوم اوبرا بعملية مزامنة اي اخذ نسخة من مفضلتك ووضعها في حسابك في اوبرا لينك لتستطيع الحصول عليها من اي جهاز آخر.

متصفح الويب

جوجل كروم ١٠:

إن جوجل كروم ١٠ يشبه إلى حد كبير النسسخات السابقة مع تعديلات جديدة، كالفكرة المبتكرة في صفحات البدء في المتصفح، فقد استبدلتها جوجل بحيث تظهر على شكل مربعات مصفوفة للمواقع الأكثر زيارة وأيضاً قائمة بالمواقع التي تبحث فيها دائماً، كلها في صفحة واحدة وبترتيب متناغم. وهو سريع بفضل محرك جافاسكريبت جديد، وقد دمجت ال «pdf reader» وال«flash player» في جوجل وذلك يمكّن المستخدم من قراءة ال pdf ومشاهدة الflash فيديو دون الحاجة إلى تحميل برامج لذلك. يتمتع جوجل كروم بنظام تحديث آلي فلا يضطر المستخدم إلى تحديثه .دعمت جوجل متصفحها الجديد بالعديد من ميزات الأمان والسرية التي نفتقدها في متصفحات اليوم. من أهم هذه الميزات إمكانية فتح صفحة جديدة للقراءة فقط. ويقصد بذلك أنه خلال تصفحك لموقع ما فإن كل تفاعلاتك مع الموقع لن تسجل في ذاكرة المتصفح. خاصية ثانية هي تحذيرها من الصفحات الضارة على الشبكة العنكبوتية مثل (Malware and Phishing) وذلك بتوفير بيئة (Sandboxing) تعمل بصلاحيات دنيا بحيث لا يمكّن للموقع الضار من التأثير على جهاز الضحية. وينطبق نفس الكلام على الإضافات (Plugins) للمتصفح. فكل إضافة ستعمل تحت بيئة آمنة بحيث لا يمكن إستغلالها سلباً.

كروم يدير كل صفحة من صفحات المستخدم بشكل مستقل وذلك لأنه في حال إنهارت صفحة من الصفحات، لن تؤثر على باقي الصفحات وبالتالي لن تؤدي إلى إنهيار المتصفح. إن جوجل كروم يتمتع بعدد وافر من الإمدادات وبإمكان المستخدم أن يرى عدد الإمدادات التي تعمل في خلفية المتصفح وإبطال عملها إذا ما أراد. كما بإمكانه إستعمال أسلوب التخفي إذا أراد الحفاظ على خصوصيته.

سفاري ٥:

إن سفاري ٥ متصفح Apple الجديد يتمتع بعدة مزايا فإنه سريع التصفح ويمكنه البحث عن موقع موجود في الـ BookMarks بالعربي، كما إنه يدعم الHTML5 بشكلٍ أفضل ويدعم خاصية الإضافات، التي تسمح بأضافة خاصيات جديدة للمتصفح Plugins كما أضيف إليه خاصية البحث Bing كخيار اضافي وخاصية قرائة المقال دون ازعاج الاعلانات الجانبية، وذلك عن طريق تقريب المقال المراد قرائته في الصفحة ويتمتع بنظام حماية متطور وشكل أنيق. سفاري ٥ متوفر على الماك والويندوز.

إن هذه المتصفحات هي متوفرة مجانياً للتحميل، وهي متشابهة لحدٍ كبير. ومن المستحسن استخدام أجدد نسخة من المتصفح، لأنه في كل نسخة جديدة يتم إصلاح أخطاء برمجية وتطوير نظام الحماية وإضافة مزايا جديدة.

إن جميع برامج تصفح الإنترنت الحديثة مزودة بميزة حماية خاصة، تختلف تسميتها بين متصفح وآخر، «Private Browsing InPrivate, Incognito, Private Window» هذه الميزة تسمح بتصفح الانترنت دون تخزين البيانات عن جلسة التصفح. ويشمل هذا الكوكيز، ملفات الإنترنت المؤقتة، والتاريخ، وغيرها من البيانات. ويتم أيضاً تعطيل أشرطة الأدوات والملحقات الإضافية.

إلا أن هذه الميزة لا تحميك من:

– المواقع التي تقوم بزيارتها من جمع أو تبادل المعلومات عنك.

– إمكانية تتبع الصفحات التي تزورها من مقدمي خدمة الإنترنت أو أرباب العمل.

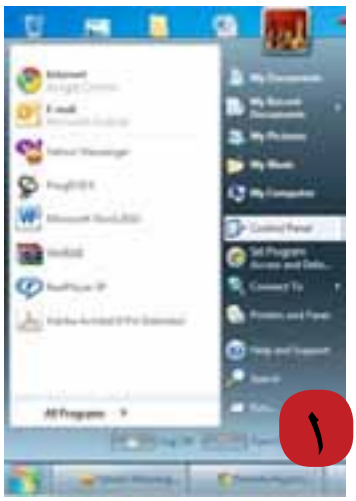
– البرامج الضارة التي تتعقب ضربات المفاتيح الخاصة بك.«Key Logger»

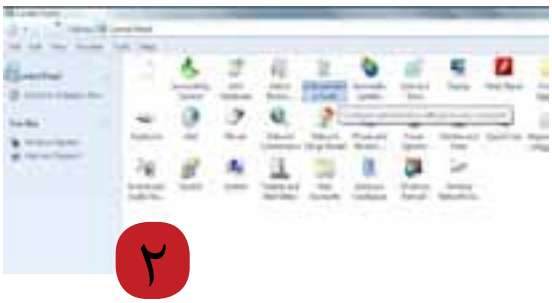
– المراقبة من قبل عملاء سريين.

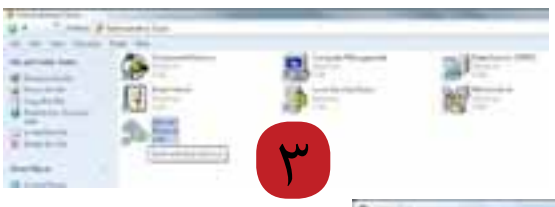
– الناس الذين يقفون وراءك.

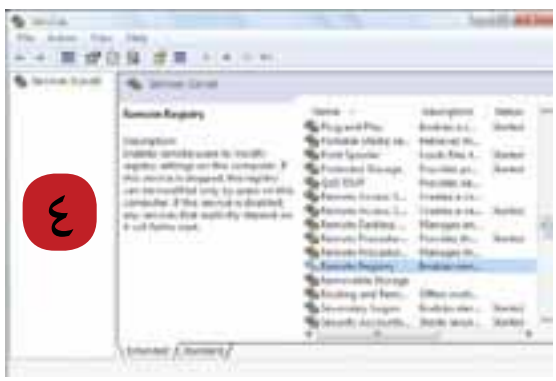
طريقة بسيطة لمنع القراصنة من السيطرة على حاسوبك الشخصي

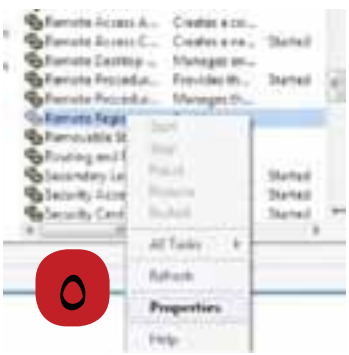
د. رامي البازي

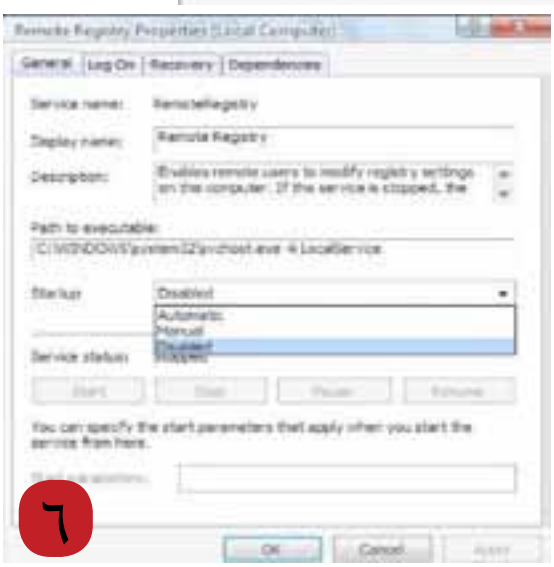












وضعت شركة مايكروسوفت ابتداءً من نسخة Windows XP تطبيق عنصر (Remote Registry) يتيح لرجال الاعمال التواصل مع حاسوباتهم المكتبية وأخذ معلومات منها عن بعد بشرط ان يكون حاسوبك موصولاً بخدمة الإنترنت أو الشبكة المشتركة بين الأشخاص (Network). لكن سرعان ما إستغل هذا التطبيق من قبل القراصنة (Hackers) لسرقة المعلومات الشخصية لأي شخص، لذا يفضل غلق هذا التطبيق لتلافي إختراق حاسوبك، وهنا سنقوم بشرح الطريقة مع الصور:

•في البداية أين تجد عنصر (Remote Registry) ؟

١. إبدأ start

٢. لوحة التحكم control panel

٣. أدوات ادارية administrative tools

٤. خدمات services

٥. ستفتح لك نافذة الخدمات ستجد في الجهة اليمنى من النافذة قائمة طويلة بأسماء الخدمات العاملة في النظام ومرتبة هجائيا – ابحث فيها على (Remote Registry).

*** بعد ان وجد عنصر (Remote Registry) قم بالخطوات التالية:**

١. كليك يمين على العنصر (Remote Registry).

٢. نختار PROPERTIES.

٣. ستفتح لك نافذة الخصائص لهذا العنصر General .

٤. ومن خانة Startup type .

٥. اختار Disabled .

٦. واخيراً OK

٧. حظاً سعيداً لكم، ارجو انكم قد استفدتم من المعلومة، لكن احذروا هذه إحدى الطرق وليست الوحيدة لاختراقك من قبل الاخرين فالعلم يتطور والطرق تكثر، وتسلحك بأحدث المعلومات يجعلك في أمان أكثر

الجيش السوري الإلكتروني - سلاح التحليل

كاردوخ كال.

نزاعات مسلحة بدون دماء، لاتعترف بالرقعة الجغرافية. الأسلحة المستخدمة في تلك النزاعات إفتراضية يقودها شبان ومراهقون لتوجيه الجموع البشرية عبر تقاطعات الشبكة العنكبوتية المتعددة، يستغلون ما يتوفر لهم من أدوات تقنية او جموع بشرية متضامنة مع ارائهم السياسية، أو موظفين في شركات خاصة وحكومية مجبرين على خوض تلك النزاعات لتوجيه ضربات معنوية لأهداف إستراتيجية تختارها قيادة الجيش الإلكتروني.

نظرة عامة:

كان الصينيون من الأوائل المؤسسين لفكرة الجيوش الافتراضية الإلكترونية، واستطاع الجيش الصيني الافتراضي الذي يتقن ٧٠ لغة ويشهد له بالقدرة المتفوقة والعالية في أداء المهام الإلكترونية المتنوعة من إختراقات، أو مراقبة أشخاص معينيين عن طريق تحليل البيانات المبعثرة على الإنترنت أو الولوج إلى وحدات الإتصال المركزية لمزودات الخدمة، في سبيل خدمة النظام السياسي الصيني المشرف على عمل الجيش الإفتراضي. تطورت الجيوش الافتراضية من ناحية الإستغلال، ففي التجربة الإيرانية تشكلت جبهتان إلكترونيتان للنشاط على شبكة الأنترنت، جهة تتبع للنظام السياسي وجهة تعارض التوجه السياسي الحاكم.

الجيش السوري الإلكتروني:

سُمي بالجيش كونه يمتلك قيادة بالإضافة لوحدات مهام متنوعة تعمل إستناداً لأوامر مسؤولين في مستويات عالية وتعتبر عناصر تنفيذ المهام هي الثقل البشري لتحريك تلك الأدوات. ظهر الجيش السوري الإلكتروني المؤيد للسلطة الحاكمة في بداية أحداث ثورة ١٥ آذار وإيماناً من أن الفيس بوك كان منطلقاً للحراك الثوري في سوريا، إتخذ الجيش السوري الإلكتروني المنطلق ذاته – أي الفيس بوك – لتجميع العناصر والبدء برسم إستراتيجية النشاط الإلكتروني الذي تنوع ما بين إختراقات (هاكرز) أو نشاط إعلامي مكثف والقيام بهجمات على صفحات معينة.

وبالرغم من قيام صفحة الفيس بوك بإغلاق صفحة الجيش السوري الإلكتروني معتبرة إياها صفحة تخريبية إلا أن عناصر الجيش الإلكتروني مصرين دائماً على فتح صفحات جديدة وإستكمال العمل بدون إستسلام.

كيفية عمل الجيش السوري الإلكتروني:

السؤال الذي قد يُطرح، كيف تستطيع التكنولوجيا أن تمنح السيطرة على أشخاص يمتلكون نوايا سياسية تجاه قضية معينة وقد يكونوا بالأساس ليسوا من مستخدمي هذه التكنولوجيا بشكل جيد؟

وفرت التكنولوجيا الحديثة أدوات مجانية وسهلة للتواصل مابين العناصر المنضوية تحت فكر ورأي معين. فأغلب الشبكات الاجتماعية تعمل على تحليل توجهات الفرد السياسية وحصرها بداخل الدائرة البشرية التي تتواصل مع اتجاهه الفكري، لذا جمعت الصفحات الخاصة بالجيش السوري الإلكتروني عناصر عديدة مستعدة لتنفيذ المهام التي يُكلفون بها.

هيكلية وحدات الجيش السوري الإلكتروني:

كنوع من المقاربة مابين هيكلية عمل الجيوش الحقيقية يمكننا تقسيمه إلى عناصر أساسية كالتالي:

١- عناصر الاستطلاع.

٢- عناصر التوجيه المعنوي.

٣- عناصر الاستخبارات العسكرية.

٤- الأعمال التكتيكية.

٥- الأعمال الحربية (الكتائب).

لذا وبحسب القوانين والموازين الافتراضية يمكن للجيش الافتراضي القيام بمهام تكتيكية تساعد على تحوير العديد من الحقائق والتأثير عليها على أرض الواقع. سأقوم بتناول العناصر الأساسية للجيش الافتراضي كل على حدا محاولاً أن أضع أساسيات المهام العملية.

الجيش السوري الإلكتروني - سلاح التحليل

عناصر الاستطلاع: بمفهوم الجيش الحقيقي، يقوم عناصر الإستطلاع بمراقبة تحركات الأعداء في وقت السلم لدراسة مدى قابليتهم ولمعرفة أوضاعهم وما لديهم من أسلحة جديدة ووضعية الأسلحة القديمة وأماكن تمركزها، ومن ثم عن طريق تحليل المعطيات تستطيع القيادة العسكرية إنشاء صورة كاملة عن حالة الجيش المعادي هذا أولاً، ثانياً والأهم هي دراسة تحركات العدو وتغير خططه عن كثب أثناء المعارك القتالية.

افتراضياً فإن مهام عناصر الاستطلاع تقتصر على قراءة وتتبع كافة ما ينشر على صفحات الإنترنت بواسطة أشخاص لديهم الخبرة في تحليل كل كلمة تنشر على الصفحات الإلكترونية وحصر ومراقبة أنشطة أشخاص وجماعات على المنصات الإعلامية الإلكترونية وإنشاء دراسة كاملة عن تحركهم الإعلامي وبياناتهم وتواريخ نشرها. وبحكم كوننا نعيش في صراع افتراضي لكسب الآراء، قامت بعض عناصر الجيش السوري الإلكتروني بخلق شخصيات وهمية لهم أراء قريبة جداً لأراء المعارضين السوريين عبر الشبكات الاجتماعية. وإزداد هذا النشاط بعد ان قامت الحكومة السورية بتقديم الدعم بكافة انواعه لعناصر الجيش الإلكتروني وتدريبهم. وقامت عناصر الجيش بإنشاء صفحات مزورة في سبيل التواصل مع المعارضين من الداخل وكشفهم، كالصفحة المزورة للدكتور عمار القربي والناشطة سهير الأتاسي. ومن جهة أخرى كشفت كافة المعلومات الموجودة في مزودات خدمة الإنترنت لعناصر الجيش الإلكتروني من أجل إكتمال الصورة وكشف الناشطين.

عناصر التوجيه المعنوي: في الجيش الحقيقي، تكون عناصر التوجيه المعنوي وبأدواتها الإعلامية والاتصالية مرتبطة ارتباطاً فعلياً بالمقاتلين لرفع الروح المعنوية وردعهم عن الاستسلام او التخاذل، بالعديد من الطرق، بالإضافة إلى المهمة الأولى وهي تربية المقاتل فكريا.

التوجيه المعنوي الافتراضي: هدفها إيصال الصورة التي يرغب النظام في زرعها في عقول الناس والمتلقين الإلكترونيين الأكثر تفاعلاً مع الأحداث الجارية، مستخدماً أساليب الحقن الفكري. تعتبر الأدوات التي يستخدمها الجيش السوري الإلكتروني كاليوتيوب والمقالات المبعثرة على المواقع الإلكترونية عنصراً رئيساً من اساسيات العمل، إلا انه وبحسب العديد من المراقبين فقد فشل الجيش السوري الإلكتروني من طرح نفسه كطرف إيجابي في هذا النزاع الإلكتروني وأثبت فشله من ناحية «التوجيه المعنوي إعلامياً».

عناصر الإستخبارات العسكرية: في حالة السلم، تعتبر من أهم العناصر المؤلفة للجيش. فهي تراقب أمن الجيش وسلامته من المتسللين والمخربين. وتقوم بالدراسات العديدة عن جميع المقاتلين وميولهم السياسية وحتى الثقافية، لذا تمتلك قاعدة بيانات تحليلية واسعة لمجمل نشاطات واتصالات وحتى الاختراقات العسكرية للجيش.

الاستخبارات الافتراضية: تتألف من عناصر ذات كفاءة عالية في حماية الشبكات والمعروفين بالهاكرز، وهم بدون منازع خبراء في ثغرات الشبكات والأنظمة. مهمتهم الرئيسية وبالتعاون مع الشركات المزودة للإنترنت في سوريا فرض المراقبة الكاملة على شبكات الاتصال وتبادل المعطيات بشكل عام. يضاف إلى ذلك مراقبة المواقع الإلكترونية المعارضة ورصد مواقعها الجغرافية والمشرفين عليها والكشف عن ثغراتها مما سيخول قوات الاستخبارات الافتراضية الولوج إليها وكشف كل من يشترك في نشر حرف واحد على الموقع ومكان تواجده وبل حتى أدق التفاصيل عنه كبريده الإلكتروني. وبواسطة الفريق نفسه من الممكن كسر حماية البريد الإلكتروني وكشف ما بداخله من سجل يحتوي على مراسلات الشخص الذي تدور حوله الشكوك. وقد سجل الجيش السوري الإلكتروني العديد من الإختراقات للبريد الإلكتروني وحسابات الفيس بوك، كحساب السياسي جورج صبره الذي تم إعتقاله بعد اختراق حسابه بيومين.

ومن ناحية أخرى يحاول عناصر الجيش السوري الإلكتروني كشف كافة الإتصالات البيانية مع خارج إطار الدولة إفتراضياً – بالتعاون مع المزودات – والنشاطات الإفتراضية للمعارضة الخارجية ورصدها ومراقبتها ومحاولة خرق حصونها الإفتراضية للحصول على المعلومات التي تخصها. وبذلك إستطاع الجيش السوري الإلكتروني نقل نشاط الإستخبارات الإفتراضية خارج إطار سوريا. وبذلك امتلك الجيش قاعدة بيانات للعناصر المعارضة الخارجية والجهات الداخلية التي تتصل بها.

الأعمال التكتيكية: في المعركة الفعلية، مفهوم الأعمال التكتيكية يعني تلك الخطوات والمهام القتالية التي تحاول قدر المستطاع زعزعة خطة العدو (الدفاعية والهجومية) في المعركة ومحاولة سحبه لكمائن ولمواقع تسهل القضاء عليه بكل سهولة، بالإضافة إلى مهام عديدة كالتمويه، والتخطيط لسير الأعمال القتالية.

الأعمال التكتيكية الافتراضية: هي تلك الخطوات التي يتبعها الجيش الإلكتروني بكل صنوف قواه في الساحات الافتراضية، على سبيل المثال المدونون والمعلقون على الفيس بوك وهم عناصر نشطة جداً في الجيش السوري الإلكتروني تحاول خلق رأي عام، أو إثارة بلبلة معينة بواسطة تدويناته. وتستطيع قوات الاستخبارات والاستطلاع الافتراضي كشف تحركات أناس تفاعلت مع ذالك الطَعم بشكل إيجابي او سلبي مما سيمهد الطريق بشكل واسع للوصول إلى هؤلاء الأشخاص.

تؤمن عناصر التكتيك العديد من الطرق لنشر أعمال عناصر التوجيه المعنوي بكافة الوسائل الممكنة وزرع ألغام إعلامية وثقافية بداخل الساحات الافتراضية المعادية للنظام السوري. ويتم الاستعانة بعناصر تتقن لغات أجنبية متعددة وتنتمي لكتائب مهامها فقط الهجوم بالتدوينات والتعليقات ومركزة على صفحات هامة، كصفحة الرئيس الأمريكي باراك أوباما، او الرئيس الفرنسي ساركوزي، بالاضافة إلى إستهدافهم الدائم لصفحات القنوات الإعلامية كالجزيرة والعربية.

الأعمال الحربية: عسكرياً وفعلياً، العمل الحربي، هو تحرك عسكري للقوات لمهاجمة الأعداء والمتعاونين استناداً على معلومات عناصر الاستطلاع وقوة المقاتل الصديق المعنوية والمادية، ومدى قوة عناصر الدفاع الصديقة ودقة تخطيط الأعمال التكتيكية، عندها وبواسطة التحليل العسكري ستكون النتائج معروفة قبل البدء بالزحف العسكري.

افتراضياً: يعمل العالم الافتراضي ضمن إطار علمي بحت. يضاف إلى ذلك وجود نظام سياسي كامل بكافة بناه التحتية التكنولوجية من مخدمات ومحللين وبيانات مكشوفة عبر المزودات يستطيع عناصر الجيش السوري الإلكتروني جمع ما يملكون من بيانات ومعلومات وتحليلات وأدلة لشن هجوم فعلي على المواقع والعناصر المناهضة للسلطة أو حتى وضع كمائن كما ذكرت سابقاً وبنتيجة نجاح حتمية بنسبة ١٠٠٪. بذلك تم التأسيس لبيئة افتراضية تستطيع التأثير وبشكل كبير جداً على الرأي العام وعلى الحقيقة. فالكثير من الأفلام القصيرة التي تنشر على موقع اليوتيوب على سبيل المثال أو القصص والتدوينات لأبطال مصطنعين تمجد عناصر إفتراضية، تؤثر بشكل كبير على العديد من الشباب التي تتراوح اعمارهم مابين ١٨-٢٩ عاماً، كونهم متلقين إلكترونيين وذوي ثقافة اندفاعية تتأثر بكل كلمة، مشكلين تياراً جديداً في الحياة السياسة يقودها أمراء شبان إفتراضيون.

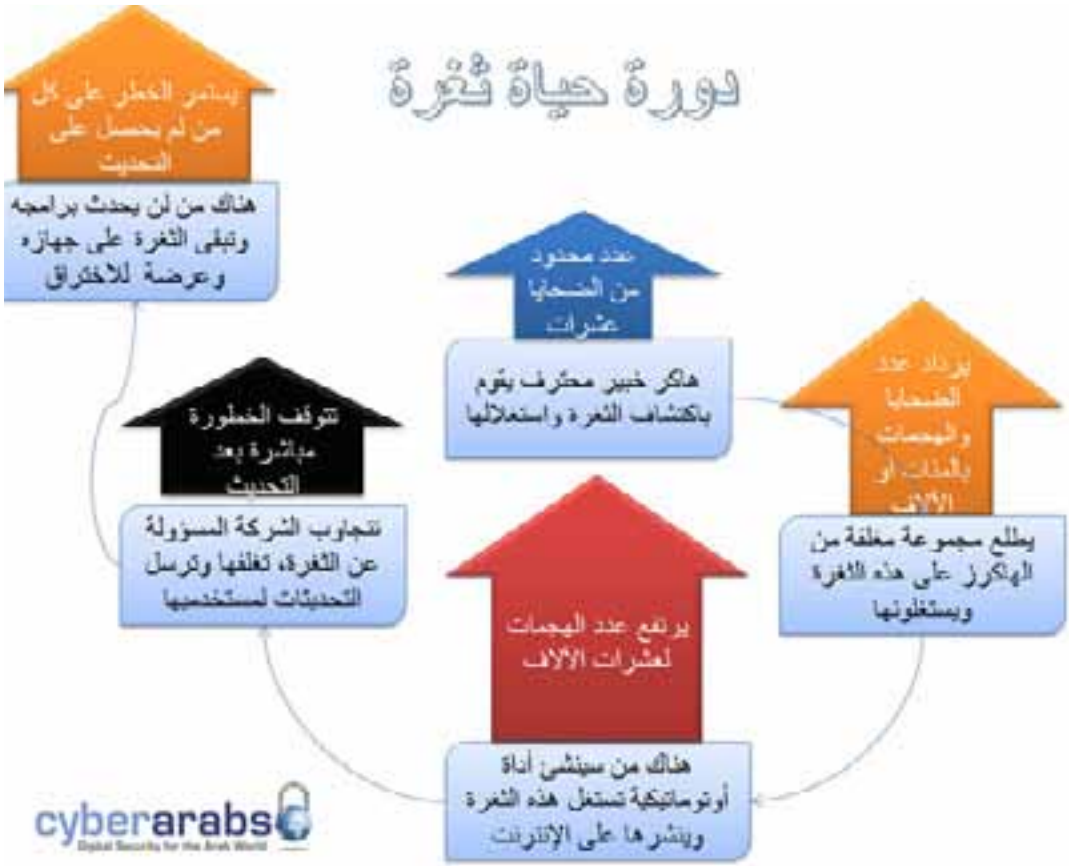
لكون النظام في سوريا لم يولِ الجرائم الإلكترونية أي إهتمام، لم يدرك العديد من الشبان والهاويين ماهية الخطر والإجرام الممكن حدوثه في الإطار الإفتراضي. لذا وبدون أي تردد أو إدراك للعواقب وحقيقة الجريمة الإلكترونية، شارك العديد من الشباب وبزخم كبير في نشاطات الجيش السوري الإلكتروني المتنوعة.

دورة حياة ثغرة

رامي نخلة

لا يمكننا إلا وأن نكون معنيين بهذا الموضوع طالما أننا مستخدمو إنترنت. فوجود ثغرة واحدة على جهازك معناه أن أي هاكر مبتدأ في العالم (وهم يعدون بالآلاف) لديه القدرة على الوصول إلى كل البيانات الخاصة الموجودة على جهازك. فلا يبدأ الموضوع بكلمات السر ولا ينتهي مع حسابك المصرفي مروراً بكل وثائقك السرية والهامة.

كلمة ثغرة في كل اللغات تدل على نقطة ضعف معينة في حصن منيع، والشرط الأساسي لأن تكون الثغرة ثغرة، هو معرفة الأعداء فقط الذين يريدون اختراق هذا الحصن بوجودها. فلو عرف بها القائمون على حمايته لأغلقوها في نفس الساعة ولم تعد ثغرة، وما لم يكتشفها الأعداء فهي نقطة ضعف مجهولة للجميع وآمنة إلى حين اكتشافها.



كما في الحصون كذلك في أجهزة الكمبيوتر نقاط الضعف والثغرات موجودة دائماً وكثيرة جداً وهي فقط بانتظار من يكتشفها، وقد يكون شخص هاكر محترف أو شركة أو جهاز أمن أو أي جهة مهتمة لها مصالح في الحصول على معلومات خاصة وسرية موجودة في جهاز شخص أو شركة أو الخ... المهم أنها في جهاز كمبيوتر معين، فستقوم هذه الجهة نفسها أو باستئجار هاكرز محترفين للحصول لها على هذه المعلومات وهنا تبدأ الرحلة.

جرى استخدام «ثغرة» كمصطلح في عالم الكمبيوتر والإنترنت. فكل جهاز كمبيوتر صمم ليكون حصناً منيعاً وجهز بكافة الأدوات والوسائل الدفاعية ليحفظ خصوصية كل ما بداخله، ولا يترك في حصنه إلا المنافذ الشرعية ليدخل كل شيء ويخرج منها بموافقة ورضى القائمين على هذا الحصن أو الجهاز.

كيف تبدأ دورة حياة الثغرة الإلكترونية؟

سيقوم هاكر محترف جداً وخبير بالبدء بدراسة الجهة المستهدفة من كافة النواحي. ما هي أجهزة الكمبيوتر المستخدمة، ما هي البرامج المستخدمة وأنظمة التشغيل التي تعمل عليها وأدوات الحماية التي تمتلكها وما إلى ذلك. بعد التعرف على هذه الخصائص سيبدأ الهاكر

بتجربة كل الثغرات المعروفة والمكتشفة سابقاً من قبل غيره، فلعل القائمين على حماية هذا الجهاز غير مهتمين بأمنهم فلم يسمعوا بها ولم يغلقوها بعد!، وفي حال لم يجد شيئاً سيبدأ العمل الجدي في إكتشاف ثغرة جديدة كلياً أو حتى خلق ثغرة عن طريق استهداف نقطة ضعف معينة.

كيف تتم هذه العملية؟ لا مجال لشرحها هنا لأنها معقدة جداً وإختصاصية وتدخل فيها البرمجة وقراءة الشيفرات والكودات وكتابتها وما إلى هنالك، لكن ما نود معرفته حقاً أنه دائماً ولا يمر أسبوع تقريباً دون أن يتمكن هاكر ما في هذا العالم من اكتشاف ثغرة جديدة وإختراق الجهة المستهدفة بطريقة ما لم يسبقه أحد إليها فيتمكن من الحصول على مراده ويمضي.

إذا هنا ولدت ثغرة جديدة وهناك شخص ما بات يعرفها جيداً ويمكنه تطبيقها في كل يوم بسهولة وإختراق شخص أو جهة أخرى، وهنا يكون مستوى خطورة هذه الثغرة على المجتمع الإلكتروني محدود جداً لأنها بيد شخص واحد وهو من يقوم باستخدامها. فإذا لم يكن لذلك الشخص تحديداً أي مصلحة خاصة بالحصول على معلوماتك أنت بالتحديد فلا خطر عليك من هذه الثغرة.
ولكن إحدى المبادئ أو كما تسمى «الأخلاقيات» الأساسية في مجتمعات الهاكرز هي مشاركة المعلومات فيما بينهم، فلن يلبث هذا الهاكر الذي اكتشف تلك الثغرة حتى يذهب إلى مجتمعه السري المغلق ويشاركهم بهذا الاكتشاف ليحصل على تقديرهم وثنائهم وبالتالي منزلة أرفع في تراتبيتهم الهرمية. وهنا تتسع دائرة الأشخاص الذين يعرفون بأمر هذه الثغرة وأسلوب تطبيقها وتزداد الهجمات والضحايا، لكن أيضاً تبقى هذه الثغرة معروفة من قبل عدد محدود من الأشخاص وهم لديهم خبرة برمجية متقدمة وكافية لتطبيقها وهي محصورة في مجتمعات النخبة، لدى الهاكرز المحترفين.
هنا وفي مرحلة معينة عادة ما نجد أن أحد هؤلاء الهاكرز قام ببرمجة أداة بسيطة تقوم أوتوماتيكياً بإعادة تنفيذ خطوات جلسة الاختراق، مثلاً ما هي السطور البرمجية التي يتوجب على الهاكر كتابتها، وما هي ردة الفعل المحتملة لجهاز الضحية، وما هو رد فعل الهاكر عليها. تقوم الأداة أو البرنامج أتوماتيكياً بالتعامل مع الثغرة دون حاجة المستخدم إلى كتابة أي سطر برمجي والاكتفاء بوضع عنوان الهدف وضغط Attack «هجوم». وستقوم هي بكل العمل لأجله وستدخله إلى جهاز الضحية دون أي معرفة تقنية منه بتفاصيل ما جرى.
وسرعان ما تنتشر هذه الأداة عبر الإنترنت، وسيسارع الهاكرز المبتدئون إلى تحميلها واستخدامها، وهنا يرتفع عدد هذا الهجمات بشكل كبير جداً ويكون لدينا ضحايا بالآلاف يومياً، ويبدأ الخطر الحقيقي لهذه الثغرة يهدد كل مستخدمي الإنترنت.

في الغالب تكون هذه الأداة عبارة عن برنامج يعمل على جهاز الهاكر وحده ويقوم نيابة عنه بكتابة الأوامر البرمجية المعقدة والطويلة. ولكن في بعض الأحيان يكون عبارة عن فايروس أو برنامج خبيث يجب إدخاله إلى جهاز الضحية ليقوم هو بالعمل من الداخل.
وهنا يجب علينا التمييز بين الثغرة الموجودة أصلاً في برمجية معينة لدينا ويتم استغلالها من قبل هاكر وبين الفيروسات والبرامج الخبيثة ذات التصنيفات المتعددة، والتي تأتي في العادة لتفتح ثغرة في حصن أجهزتنا عندما تكون منيعة. وخير مثال على هذا هو حصان طروادة. فكما في الأسطورة كذلك في عالم اليوم هناك أنواع كثيرة من الفيروسات التي تحمل اسم ووظيفة حصان طروادة. لا يتسع المجال هنا لشرح الفوارق بين الفيروس والثغرة، لكننا سنتطرق إليها لاحقا في مقالة مفصلة.

عادة وفي هذه المرحلة تتجاوب الشركة المسؤولة عن إغلاق هذه الثغرة في نظامها عن طريق عمل تحديث update ترسله عبر الإنترنت إلى كل مستخدميها وتدرجه في إصداراتها الجديدة، ويتوقف الخطر مباشرة عند كل من حصل على هذا التحديث
من الأمثلة الشهيرة على هذه الثغرات تلك التي اكتشفت في قارئ الكتب الإلكترونية Adobe Reader عام ٢٠٠٩ وتطورت لتصبح أداة على شكل كتاب إلكتروني. كل من قام بفتحه مّكن القراصنة من التحكم الكامل بجهازه عن بعد، قامت شركة Symantec باكتشاف هذه الثغرة وتواصلت مع أدوبي. وتتطلب الموضوع أسابيع لحل المشكلة. وحتى اليوم كل من يعمل على الإصدارات (٩,٠– ٩,١ – ٩,١,٢) هو معرض للإختراق.
أين يكمن دورنا نحن في الموضوع وكيف نحمي أنفسنا من هذه الثغرات؟ دائماً هناك إحتمال بنسبة معينة أن نكون ضحايا لهذا الإختراق. لكن ما علينا فعله هو أن نخفض هذه النسبة إلى حدودها الدنيا وذلك من خلال حسن إدارتنا لموضوع التحديث المستمر على الجهاز ولذلك ننصح بشدة بالإطلاع على هذا الموضوع
(كيف تتعامل مع التحديثات على جهازك).

رامي نخلة

«أنونيموس» أو «القراصنة الأخيار»:
من هم وما هي قصتهم؟

«أنونيموس» أو «المجهولون» بالعربية، هم مجموعة من القراصنة ظهرت منذ ثلاث سنوات، وهدفها الأساسي هو المناضلة من اجل حرية التعبير، وحرية التجمّع، وحريّة الاتصال، والتشديد على دور الحقوق المدنيّة في بناء مستقبل الشعوب. وهم يُعرفون بكلماتهم التحذيريّة التي تتلخّص ب «لن نسامح، لن ننسى... احذرونا.»

ولكن من هم أعضاء «أنونيموس»، وما هي هويتهم السياسية؟

يستخدم أعضاء «أنونيموس» القناع الشهير المستوحى من فيلم «V for Vendetta». وبطل هذا الفيلم هو شخص فوضوي ومثقّف، يسعى الى تحرير شعبه من القمع عبر بث الوعي في صفوفهم.

يقوم البعض بوصف «أنونيموس» ب»الثوريين الحالمين»، أما البعض الآخر فيطلق عليهم لقب «الفوضويين»، بينما يذهب آخرون الى وصفهم ب»العدميين».. ولكن ما يتّفق عليه الجميع هو أنهم يثيرون قلق وانزعاج حكومات القوى العظمى وإدارات الشركات العالمية، ويُستهدفون من قبل أجهزتها الأمنيّة. أما هذا القلق فبدأ عندما قامت مجموعة «أنونيموس» بأولى عملياتها في العام ٢٠٠٨، وذلك عن طريق استهداف طائفة «السيانتولوجيا» التي تدّعي اصلاح الروح الانسانيّة كذريعة للاحتيال على الناس وسرقة أموالهم.

وقد نسبت مجموعة «أنونيموس» الهجوم المعلوماتي على موقع «PayPal» في كانون الأول الماضي لنفسها، وذلك كرد على منع التبرّع لموقع «ويكيليكس» المسؤول عن كشف وثائق دبلوماسية وأسرار تتعلّق بالسياسة الأمريكيّة. ومن المرجّح أن تكون هذه المجموعة قد هاجمت مواقع أخرى تابعة لشركات الدفع عبر الانترنت، مثل «MasterCard» و «Visa» وغيرها كرد على الحظر الاقتصادي على «ويكيليكس»، خاصة أن الشركات لم تقم باتخاذ الاجراء ذاته مع امبراطوريّة «مردوك» الاعلاميّة بالرغم من اتهامها بالتجسّس.

وقد قامت الشرطة الفيدراليّة الأمريكيّة بالقاء القبض على ١٦ شخصاً في الولايات المتحدة و٥ في بريطانيا وهولندا لتورطهم في هذه العمليات، وقد يسجن هؤلاء لمدة عشر سنوات ويدفعون غرامات تقدّر ب ٢٥٠ ألف دولار. أما السؤال المهم فهو مرتبط بالعلاقة بين العمليات التي قامت بها «أنونيموس» وبين تهديد المسؤولين الأمريكيين لجوليان أسانج، مؤسّس موقع «ويكيليكس»، وقراصنة المعلوماتيّة، مما يقود الى فرضيّة أن هناك أسباب سياسيّة وراء السعي للقبض على أعضاء «أنونيموس». سؤال آخر يطرح نفسه وهو يتعلّق بالأسباب التي تدفع المافيا الروسيّة والمحتالين في أمريكا، وأوروبا، وآسيا، وأفريقيا بالاحتيال المتكرّر من خلال شبكة الانترنت دون التعرّض للملاحقة. وقد قامت «أنونيموس» بشن هجمات ضد المواقع الحكوميّة في تونس ومصر كوسيلة دعم للثوار في البلدين خلال الثورات.

اذا كانت «أنونيموس» تناضل من أجل الحرية وتعبّر عن رأيها، لماذا تتم مطاردتها؟ وهل حقاً «تنتهي حدود حريتي عند حدود حريّة الآخر»؟

Operation Turkey»: «Anonymous» against Censorship»
«عمليّة تركيا»: القراصنة «أنونيموس» ضد الرقابة

مجموعة «أنونيموس»: سياسة الحجب في تركيا هي السبب الرئيسي وراء اختراق الموقع التركي.

في ٩ حزيران من هذا العام، قامت مجموعة القراصنة «أنونيموس» باختراق موقع الاتصالات السلكيّة واللاسلكيّة الالكتروني التركي في ما أُطلق عليه»عمليّة تركيا»، وذلك للاحتجاج على حجب مواقع الانترنت.

وقد قامت هذه المجموعة بادلاء التصريح الآتي:
«على مدى السنوات القليلة الماضية، رأينا كيف أن الحكومة التركية شددت قبضتها على الإنترنت، وحجبت آلاف المواقع والمدونات في حين أنّ الإجراءات القانونية التعسّفيّة ضد الصحفيين على الإنترنت لا تزال قائمة. تريد الحكومة الآن فرض نظام فرز جديد من شأنه أن يجعل من الممكن الحفاظ على سجلات نشاطات جميع مستعملي الإنترنت، ورغم أن طريقة تطبيق هذه العملية لا تزال مبهمة... لكن يبدو واضحاً أن الحكومة مصرة على تصعيد عمليات الرقابة للمستوى التالي».

وكرد على هذا التصريح، قامت الرابطة التي تُعنى بمعالجة جرائم المعلوماتيّة، بمناشدة الهيئات الحكوميّة المختصّة على الوقوف في وجه الجرائم الالكترونيّة التي تنتهك «حرمة» البلد. عقب هذا التصريح، وبعد بضعة أيام، ألقت الحكومة التركيّة القبض على ٣٢ شخصاً زعم تورّطهم بالاختراق الذي قامت به المجموعة.

«أنونيموس» أو «القراصنة الأخيار»: من هم وما هي قصتهم؟

Operation Facebook»: «Anonymous» for Privacy»
«عملية فايسبوك»: «أنونيموس» لحماية الخصوصية

مجموعة «أنونيموس»: «اقتل فايسبوك من أجل خصوصيّتك».

قامت مجموعة «أنونيموس» أو «القراصنة المجهولون» الناشطة في مجال الدفاع عن الحريات عامةً، وحريّة التعبير خاصة، بتنزيل فيديوهات باللغات الانجليزيّة، والاسبانيّة، والالمانيّة على «يوتيوب» للاعلان عن خطتهم لتدمير «فايسبوك»، أكبر شبكات التواصل الاجتماعيّة في العالم.

وقد وجّه القراصنة دعوة لكل من تهمّه مسألة الخصوصيّة والحماية من التلاعب بالمعلومات الشخصيّة على شبكة الانترنت للمشاركة في عمليّة «أقتل فايسبوك من أجل خصوصيتك»، وذلك يوم ٥ نوفمبر ٢٠١١. أما اختيار هذا التاريخ المعيّن للعمليّة فمردّه الى «غاي فاوكس»، أو «غويدو فاوكس»، والمعروف بكونه الرأس المدبّر لمؤامرة البارود. ومؤامرة البارود تضمّنت التخطيط لاغتيال الملك جايمس الأوّل بتفجير القصر الملكي باستعمال البارود، وذلك في العام ١٦٠٥. ولاحقاً، وبعد أن فشلت العمليّة وألقي القبض على فاوكس، قامت بريطانيا باعتماد الخامس من نوفمبر يوماً وطنياً للرمز الى فشل الهجوم.

أما الفيديو الذي قامت «أنونيموس» بنشره فيشير الى أنّ «الفايسبوك يقوم ببيع المعلومات للمنظمات الحكومية ويوفّر ولوجاً غير قانوني لبعض الوكالات لتمكينهم من التجسس على الناس حول العالم».

وفي هذا الاطار، تشير مجموعة القراصنة الى أنّ الفايسبوك بخدماته المجانيّة انما هو أداة لبيع معلومات المستخدمين وبياناتهم الشخصيّة، خاصةً أن النظام يقوم بحفظ جميع التغييرات التي يقوم المستخدمون باحداثها وحتى استرجاع الحسابات الملغيّة أو المحذوفة. وبحسب أنونيموس «ما يعلمه الفايسبوك عنك هو أكثر بكثير مما تعلمه عائلتك».

الأخطاء البرمجية والتصحيحات

قامت «غوغل» بتحديثات عديدة لمتصفح «كروم» الخاص بها (Chrome) بهدف معالجة الأخطاء البرمجية العديدة التي كُشِفَ عنها مؤخراً. وعمدت شركة «سكايب» (Skype) إلى تصحيح نقطة ضعف بالغة الخطورة في تطبيق «سكايب ٥» المخصص لـ«ماكنتوش» (Skype ٥ for Mac) والذي قد يمكّن أي معتدٍ على دراية كافية من استغلاله للتحكم بنظام الحاسوب لديكم.

تصحيحات «غوغل كروم» (Google Chrome)

تتولى التصحيحات التي تمت مؤخراً في «غوغل كروم» تصويب مجموعة من الأخطاء البرمجية. ومن أصل ١٣ تصحيحاً، ثلاثة فقط صنّفوا في درجة عالية الخطورة وأضيف إليها اثنين في خانة الخطير. وتخطط «غوغل» لإبقاء التفاصيل بشأن عدد هذه التصحيحات سري إلى حين يقوم العدد الأكبر من مستخدمي متصفح «كروم» بتحديث النسخة الأخيرة منه.

وكشفت شركة أمنية مؤخراً عن خطأ برمجي من شأنه أن يسمح للمعتدين بتخطي آلية العزل (sandbox) في متصفح «غوغل كروم» وتشغيل برمجة خطيرة على أنظمة الحاسوب لديكم. وتفيد «غوغل» أنه بما أن الخطأ البرمجي يتطلب إستخدام مشغل الوسائط «فلاش» (Flash)، فلا شكّ أن هذا الخطأ البرمجي مرتبط بـ«أدوبي» (adobe)، وليس بـ«غوغل». وعالج التحديث الذي قامت به «غوغل مؤخراً» المشكلة من خلال تنصيب نسخة محدَّثة من «أدوبي فلاش بلاير» النسخة ١٠,٢.

ويعمد متصفح «كروم» إلى التحديث تلقائياً عند اكتشافه أن نسخة جديدة من المتصفح قد أصبحت متوفرة. إنما إذا لم يقم المتصفح في نظامكم بتطبيق التحديثات لأي سبب من الأسباب، قم بالنقر على رمز مفتاح الربط في شريط الأدوات واختر «تحديث غوغل كروم» (Update Google Chrome) من القائمة الظاهرة.

تحديثات خاصة بمستخدمي نظام «ماكنتوش» (Mac)

من شأن نقطة ضعف اكتشِفَت مؤخراً في تطبيق «سكايب ٥» المخصص لـ«ماكنتوش» أن تتسبب بتوقف «سكايب» في حال أرسل المعتدي رسالة مُرَكَّبة خصيصاً.

وقد تسمح نقطة الضعف هذه له بالتحكم عن بعد بأي غلاف نظام (shell)، وهو كناية عن خاصية ضمن واجهة المستخدم لإحدى التطبيقات (وفي هذه الحالة يتمثل بواجهة المستخدم الرسومية [graphical user interface] لتطبيق «سكايب»). وتفيد «سكايب» أن هذا الخطأ البرمجي لا يتم استغلاله في الوقت الحالي. إلا أن الشركة تحث المستخدمين على التحديث للحصول على النسخة الأحدث من تطبيق «سكايب ٥» المخصص لـ«ماكنتوش» (النسخة ٥,١,٠,٩٢٢ أو تلك التي تليها) لصدّ أي اعتداءات محتملة. وأصدرت «سكايب» بالإضافة إلى ذلك تحديثين منفصلين، أحدهما لمستخدمي «ماكنتوش» (Mac) والآخر لمستخدمي «ويندوز» (Windows)، وذلك، بعد أن حال أحد الأخطاء البرمجية دون تسجيل دخول.

وعلى مستخدمي «ماكنتوش» تنصيب التحديث الأمني ٢٠١١-٠٠٣ لمستخدمي نظام «ماك أو إس إكس سنو ليوبارد» (Security Update 2011-003 for Mac OS X Snow Leopard). يعدّل هذا التصحيح نظام عزل الملفات السيئة (quarantine system) في نظام «ماك أو إس إكس» للبحث يومياً عن أي تحديثات لتحديد البرمجيات الخبيثة بهدف التعرّف على البرامج المضرّة في «ماك» مثل برنامج «Mac Defender» المضاد للفيروسات المزيف. قوموا بتحديث البرمجيات في نظام «ماك» الخاص بكم لضمان أنكم تواكبون دائماً التحديثات.

بنات و شباب «الدوار» يفخرون باسم العائلة الجديد!

لا نشعر بالعار لوصمنا بشباب وبنات الدوار بل نفخر بذلك، وان اضطررنا إلى حماية أنفسنا وتورية اسمائنا، سوف نستخدم الدوار كاسم مستعار

لا تتوانى مواقع التواصل الإجتماعي «دينامو الثورات العربية» أن تخدم الثوار في نقل المعلومة والصورة وأن تستخدم للإتصالات الخاصة والجماهيرية. لكنها أيضاً تعجز عن صد الأنظمة القمعية عن ترصّد ثوار الطراز الجديد. ذلك أن هذه المواقع التي تتهم حيناً بتقديم خصوصيات المستخدمين «المستباحة» للأجهزة الاستخباراتية وسماسرة المعلومات، وبخدمة الربيع العربي حيناً آخر، هي في الحقيقة تقدم خدماتها «بتساوٍ مفرط» إن صح التعبير. مصيرها ميدانياً يكر ويفر فيه العرب الذين قرروا التناحر مع أنظمتهم السلطوية المترهلة منذ مطلع هذا العام.

بعد أن انتصر البحرينيون لثورتهم في «فيسبوك» على نحو خاص، نظير توفيره نشر الصوت والصورة بشأن أكثر فعالية قياساً بـ «تويتر» مثلاً لا حصراً، إنتصر «فيسبوك» عليهم بعد أن إشتغلت الآلة القمعية على أقصاها، لأنه يوفر معلومات مفصلة عن المستخدمين من خلال ملفاتهم الشخصية. إشتغل «فيسبوك» كأداة تعقب مستخدميه في البحرين بعد أن «تثقف» الجهاز الأمني البحريني على إستخدامه وزرع فيه «جواسيس إلكترونيين» أولى أولوياتهم رصد ناشطي العالم الإفتراضي الذين لم يعودوا أقل شأناً من ناشطي الميدان أو الأروقة السياسية.

استدرك الناشطون الأمر بطريقة تجذب الإنتباه، وتدل إلى حد ما على مزاج الثوار، إذ أبقوا على أسمائهم الأولية وغيروا أسماء عائلاتهم إلى «الدوار» في إشارة إلى تقاطع – دوار اللؤلؤة الذي تغير توصيفه إلى «ميدان» فور نصب الخيام فيه عشية الرابع عشر من فبراير، طبعاً مع حذف كل المعلومات الشخصية التفصيلية على أشكالها.

ولوضع الفكرة وراء هذا الاسلوب في التورية ضمن سياقه الصحيح، يجدر التنويه أن الاعلام الرسمي وضمن حربه النفسية-الإعلامية وصف الثوار ببنات وشباب «الدوار» على غرار بنات وشباب «الشوارع» وما حال الوازع الاخلاقي دون اتهامهم جزافاً بالأخلاقيات المنحلة وممارسة الشنائع. ولذا أوصل الثوار «الإلكترونيون» عبر فيسبوك رسالة واضحة، ليست عبر مشاركة الصور أو الملفات، ولا عبر كتابة «نوت» أو «ستيتس» بل بطريقة ابداعية تمثلت باستخدام اسم عائلة موحد، تفيد بأننا «لا نشعر بالعار لوصمنا بشباب وبنات الدوار بل نفخر بذلك، وان اضطررنا إلى حماية أنفسنا وتورية اسمائنا، سوف نستخدم الدوار كاسم مستعار".

الحق، أن كثيراً من المعلومات والصور فقدت بعد أن أضطر اصحابها إلى حذفها، وأن عدداً من الناس حذفوا الكثير من على قائمة أصدقائهم من معارف لاشتباههم أن يكونوا مخبرين أو موالين متطرفين للنظام. ويبقى أن ما فقد في عملية إعادة التموضع يجري تعويضه تحت الأسماء المستعارة، وأن الناشطين ردوا على الحرب النفسية بحرب مضادة على نظام بات يقشعر من شأن ما يذّكره بنصب «اللؤلؤة» الذي حطمه بمعية كادر عسكري سعودي في ختام مراسيم «تطهير» الدوار وفق أدبياتهم.

تجدر الاشارة، أن ناشطي البحرين إستخدموا الفيسبوك في انشاء مجموعات لحصر المعلومات وأخرى لتوزيعها. وتملك أهم الجمعيات السياسية حسابات على فيسبوك وغيره من مواقع التواصل الإجتماعي وتقوم من خلالها ببث وقائع فعالياتها مباشرةً مثل المؤتمرات الصحفية، والمظاهرات. كما مكّن فيسبوك المتعاطفين مع البحرينيين من التعبير عن هذا التعاطف والمساهمة لصالح قضيتهم مثلما فعل إدرايوا مجموعة «أنا البحرين» التي أسسها ويديرها طاقم غير بحريني. وشأن ثورة اللؤلؤة شأن بقية ثورات الربيع العربي إنطلقت شرارتها من مجموعة على الموقع ذاته تعلن يوم الرابع عشر من فبراير موعداً للتظاهر.

عوداً على بدء، تستلزم المواجهة الإلكترونية الذكاء وسعة الحيلة شأنها شأن المواجهة الميدانية، ولزم على مستخدمي شبكات التواصل الاجتماعي تحري الدقة والإلمام بتفاصيل التطبيقات التي يستخدموها بغية سد الثغرات التي قد يستغلها رجال الأمن في تعقبهم. وثبت حسب التجربة أنه يمكن تحويل القصور في هذه الوسائط إلى فرص يمكن من خلالها تعزيز المقاومة المدنية بكفاءة وفعالية.

Heart Al-Dawar
4 mutual friends

+1 Add Friend

Lola Al-Dawar

+1 Add Friend

Montaha Al-Dawar
2 mutual friends

+1 Add Friend

Laila Al-dawar
1 mutual friend

+1 Add Friend

Zainab Al-Dawar (Zainab Al-hujairi)
1 mutual friend

+1 Add Friend

Fatima Al-Dawar

+1 Add Friend

ZoZo Al-Dawar

Zizo Mohd Al-Dawar
5 mutual friends

+1 Add Friend

Mujtaba Al-Dawar
1 mutual friend

+1 Add Friend

Hamod Al-Dawar (Hamod Al-Dawar)

+1 Add Friend

محمد عبدالله

البحرين بعد مشروع الإصلاح والديمقراطية
النظام: تكلم افتراضياً تعاقب واقعياً وكله «وفق القانون»

البحرين ليس استثناءً عن عدد من الدول العربية التي جل مصاب حكامها حساسية مفرطة تجاه الرأي الآخر. فعند الأمراء العرب هناك لسان واحد هو لسان الشيخ الأمير، أو جلالة الملك، أو فخامة الرئيس، أي حصراً أصحاب السيادة والسمو. وكما كانت الكنيسة في عصور الظلام التي تجاوزتها المجتمعات الغربية ودخلت في عصور التنوير وأخيراً إلى الدولة المدنية الحديثة تعاقب كل من تسول له نفسه الخروج عن رأي الرهبان، البحرين أيضاً تعاقب من يزعجها بموقعه أو بتعليقه في الفضاء الإلكتروني الذي يصل صداه إلى أبعد مدى.

ما يلي بعض حالات الإعتقال بحق الناشطين الإلكترونيين في ثورة الرابع عشر من شباط/فبراير.

علي عبد الإمام ، صاحب الموقع الإلكتروني الأشهر في البحرين من مجهول السجن إلى مجهول الهروب من الدولة

مدوّن، ومشارك في موقع «جلوبال فويس» ومؤسس المنتدى الحواري الأبرز في البحرين «ملتقى البحرين» عام ١٩٩٩. كان قد اعتقل ٢٠٠٥ لمدة خمسة عشر يوماً مع زميليه إدرايي الموقع حسين يوسف وعلي الموسوي وأطلق سراحه لاحقاً، ليعاود جهاز الأمن الوطني الاتصال به مجدداً وأمره بالحضور إلى مركز التحقيقات عشية الخامس عشر من سبتمبر/أيلول ٢٠١٠ ضمن حملة أمنية موسعة شنتها الدولة آنذاك على معظم الناشطين السياسيين. وكان عبد الإمام والدكتور سعيد السهلاوي هما الوحيدين ضمن جملة المعتقلين الذين ينشطان في مجال الإعلام الإلكتروني.

وفور ورود الإتصال من الجهات الأمنية، ترك عبد الإمام رسالة على صفحته على «فيسبوك» تقول أنه تم استدعاؤه إلى قسم التحقيقات. وتشير المصادر إلى أن الأجهزة الأمنية إعتقلته في مطار البحرين الدولي وهو يحاول الهروب من البحرين إلى دولة قطر. وما إن وصل خبر الإعتقال إلى أصدقائه المدونين والناشطين حول العالم حتى شكلوا حملة إلكترونية قوية تطالب بالإفراج الفوري عن المعتقل علي عبد الإمام. مشاركته في العديد من المؤتمرات وورش العمل وعلاقاته بمنظمات حول العالم ساهمت في تشكيل فريق عمل للتضامن معه، شاركت فيه لاحقاً منظمات مهمة مثل فرونت لاين، مراسلون بلا حدود، وهيومان رايتس وتش.
شكل ضغط الإعلام الغربي والمنظمات الحقوقية عائقاً أمام السلطة في البحرين لاتهام عبد الإمام بالانتساب إلى الخلية الإرهابية لقلب نظام الحكم التي اتهمت بها جل المعتقلين واكتفت بمحاكمته مفرداً بالتحريض على كراهية النظام وبث أخبار كاذبة عبر موقعه الإلكتروني.

وماطلت السلطة في المحاكمة وأبقته في السجن حتى تم الإفراج عنه مع بقية المعتقلين في فبراير/شباط ٢٠١١ في عفو عام أصدره الملك لإحتواء الثورة البحرينية التي انطلقت من قلب العاصمة البحرينية. بعد تبدل الأحوال من صالح المعارضة إلى صالح السلطة بعد أن دخلت السعودية بعسكرها وما استطاعت جمعه من عسكر دول الخليج قامت السلطة بإعادة سجن المعتقلين سابقاً، التي كانت قد أفرجت عنهم وبتطوير سيناريو الخلية الإرهابية عبر إدخال جهات خارجية مثل حزب الله اللبناني وإيران في الموضوع. غير أن هذه المرة لم يكن علي عبد الإمام ضمن المعتقلين وذلك ليس كرامة من الدولة! بل لأنه صار مثل فص الملح الذي ذاب. نجح علي عبد الإمام في الهروب هذه المرة وتوارى عن الأنظار حتى ساعة كتابة هذا التقرير.

وبالرغم من اختفاء صاحب الموقع، ظل ملتقى البحرين يعمل بأقصى طاقته ولعب ولازال دوراً جوهرياً في ثورة الرابع عشر من فبراير البحرينية. ولم تتمكن السلطة من إغلاقه سوى لأيام قليلة بعد أن تمكنت حسب التقديرات من أخذ كلمة المرور من علي عبد

الإمام قسراً باستخدام التعذيب وقامت بوضع صورة لجامع الفاتح الذي كان موقعاً لتجمع موالي الحكومة مرتين إبان الثورة على الصفحة الرئيسية. غير أن جهات يتحفظ عن ذكرها تمكنت من الوصول إلى حساب الموقع مجدداً وإعادته مع كل محتوياته.

ويبقى علي عبد الإمام مفصولاً من عمله في شركة طيران الخليج منذ إعتقاله العام الماضي مجهول المصير ومبعداً قسراً عن زوجته وأطفاله الثلاثة. وحتى في حال انفرجت الأزمة وعادت الأمور إلى نصابها، هل سيأمن علي عبد الإمام من اعتقال ثالث إذا ما تفجرت أزمة سياسية أو أمنية جديدة؟

مراجع

١- ملتقى البحرين: www.bahrainonline.org

٢- مدونة حملة الدفاع عن علي عبد الإمام:
http://freeabdulemam.wordpress.com

محمد المسقطي، مجرم لإتقانه الإنجليزية

لم يكن محمد المسقطي المدون الوحيد الذي استخدم تويتر لإيصال الصوت البحريني إلى العالم في ثورة الرابع عشر من فبراير/ شباط. الكثير من الأفراد إستخدموا «صانع الثورات العربية» حسب تعبير الصانداي تايمز لتدعيم ثورتهم وتصديرها للرأي العام. بل على العكس لم يكن المسقطي منضوياً تماماً تحت حزب سياسي مؤيد للملكية الدستورية أو لإسقاط النظام، على الأقل لم يبين ذلك خلال «تغريده». إذ كان يحرص أن يكون موضوعياً ومتزناً فيما يطرحه. غير أن مصداقية الطرح كانت تتعارض مع التستر عن العنف المفرط الذي واجهت به الدولة المسيرات وسقوط عشرات القتلى، حينها تضطر حتى الموضوعية والحيادية نقل مثل هذه المعلومات التي – بالطبع – تزعج الدولة رغم أن مداخلات المسقطي عملياً كانت في المجمل معلومات تستند إلى مصادر ونادراً ما كانت آراء خالصة.

مع دخول قوات درع الجزيرة المشتركة، قامت السلطة البحرينية برعاية سعودية بتصفية الحسابات مع من كانوا يشكلون مصدر إزعاج لها في عنفوان الثورة، وكان محمد المسقطي ضمن هؤلاء. ما يعرفون محلياً بـ«زوار الليل» وهم عناصر بملابس مدنية أو أمنية أو عسكرية تدخل المنزل منتصف الليل دون قرع الباب في الغالب وتقوم بإعتقال من تريد وتفتيش المنزل دون إبراز أي إذن خطي أو إشعار مسبق وتأخذ المعتقل لجهة غير معلومة، قاموا بإعتقال المسقطي لعدة أيام حتى أفرج عنه وعاد إلى منزله. كتب عبر تويتر ما يشبه الإعتذار وقال أنه يريد قضاء الوقت مع عائلته الآن وانخفض نشاطه إلى الحد الأدنى، شأنه شأن العديد ممن كانوا يكتبون بأسمائهم الصريحة وكان ذلك أقل ما عليهم أن يفعلوه ليحموا أنفسهم من شر قوات عسكرية لا تبقي ولا تذر.

تشير التقديرات إلى أن السبب الرئيس لإعتقال المسقطي هو إستخدامه اللغة الإنجليزية فضلاً عن أسلوب مقنع بحياديته ومصداقيته إجمالاً. لم يكن الرأي العام العربي مهتماً، إذ فوق ما كانت تملك السلطة من آليات تجيره لصالحها، هو أساساً صاحب موقف سلبي تجاه الأغلبية الشيعية في البحرين، ولكن الخوف كان من الرأي العام الغربي والدولي الذي كان آخذاً بالتشكل آنذاك. فكانت الرسائل ذات النمط الغربي التي حمل معنى مباشراً واضحاً، أقرب إلى العلمية من الرأي الشخصي هو قطرات المطر التي يمكن أن تشكل السيل والذي وجد النظام أنه قد يجرفه ما لم يجفف منابعه.

مراجع :

١) مدونة محمد المسقطي: http://emoodz.com

٢) محمد المسقطي تويتر : http://twitter.com/emoodz

محمود اليوسف «عميد المدونين البحرينين» إلى المحاكمة والاعتقال رغم علاقاته الواسعة

قد تعود أهمية وشهرة الناشط الإلكتروني والسياسي محمود اليوسف إلى كونه أحد التجار المعروفين في مجال تقنية المعلومات فضلاً عن أنه خريج الولايات المتحدة في هندسة وقيادة الطيران. شخصية ناجحة وذات خلفية علمية وتجارية مثل هذه لن يكون ظلها الإلكتروني بسيطاً، جانب مهم ربما يفسر لقب «عميد المدونين البحرينين» الذي استحقه اليوسف وهو نشاطه في إدارة مواقع وحملات إلكترونية يذكر منها حملة «بس بحريني» التي حاربت النزعة الطائفية الشيعية والسنية على حد سواء وروجت لمجتمع مدني يحمل «البحرين» هوية ومرجعية.

بسبب كتاباته السياسية، واجه اليوسف دعوى قضائية من وزير البلديات والزراعة السابق منصور بن رجب في العام ٢٠٠٦ إثر تدوينة انتقد فيها فشل الوزارة في مواجهة الأمطار الغزيرة التي هطلت على البلاد في تلك السنة. واحتجز اليوسف وقتها ثلاث ساعات قبل أن يتم إطلاق سراحه بكفالة وباتفاق تسوية يقضي بإعادة صياغة التدوينة مقابل إسقاط الدعوى، وبالرغم من إجراء التعديلات رفض الوزير بعد ذلك إسقاط الدعوى ما اضطر اليوسف للمثول أمام المحكمة.

مع موجة التظاهرات في فبراير ٢٠١١ تزامناً مع ربيع الثورات العربية، إعتقل محمود اليوسف في ٣٠ مارس/آذار، وأطلق سراحه في اليوم التالي. وليس بسراً القول إن إطلاق سراح محمود اليوسف جاء بسبب ثقله الإجتماعي وعلاقاته المحلية والخارجية التي ترتبطه مع موطن دراسته الولايات المتحدة الأمريكية. غير أن ذلك لم يمنع ملاحقة زملائه الناشطين في حملة «بس بحريني» الذي إعتقل بعضهم في نقاط تفتيش قوات درع الجزيرة المشتركة ذات الغالبية السعودية التي دخلت البحرين لقمع التظاهرات.

ويمكن تفسير توقيف اليوسف السريع في سياق حملة الترهيب التي تم خلالها توقيف عدد غير معلوم من الناشطين الإلكترونيين لفترات متباينة وتوقيع بعضهم تعهدات على

عدم كتابة ما يمس بالسلطة وتهديدهم بأن أياً منهم قد يكون في المستقبل عرضة لتوقيفات أطول قد تضمنها وجبات تعذيب ولن تكون سهلة كما كانت الأولى.

مراجع :

١) صفحة محمود اليوسف على الويكيبيدا :
http://en.wikipedia.org/wiki/Mahmood_Al-Yousif
٢) مدونة محمود اليوسف : http://mahmood.tv
٣) حملة بس بحريني : http://justbahraini.org
٤) محمود اليوسف على غلوبال فويز : http://advocacy.globalvoicesonline.org

الحالة الأخطر:
«زكريا العشيري» من المنزل إلى السجن إلى النعش

سموه بـ «شهيد الحرية والقلم» كانت صوره على المغتسل وهو مسجى وآثار التعذيب بادية على جسده أبلغ من شهادة الوفاة التي أوعزت سبب الموت إلى «مرض السكري».

إعتقل شأنه شأن المئات الآخرين الذين سيقوا زرافات إلى السجن بسبب المطالبة جهراً بحريات أوسع وبنظام سياسي أكثر ديمقراطية وعدلاً بعد أن تغلغل الفساد في حكومة تديرها العائلة الحاكمة وتتحكم من خلالها بكل موارد الدولة.

كتب مقاله الأخير تحت عنوان «أنا إنسان قبل أن أكون شيعياً» وسأل فيه صراحةً كيف تكون الثورة في مصر جهاد وحرية وثورة بينما تكون في البحرين عدم ولاء وخيانة للوطن! لامس الجرح ولاشك، غير أن جروحه لم تسعفه أن يواجه الجلاد بقوة كقوة كلماته التي كانت سبباً في تصفيته. أسس منتدى حوارياً لقريته «الدير» وصار يهتم بنقل نقاش مشاكله ووصل رجالاً وشباباً ومؤسسات القرية بعضهم البعض، موقع مدني ووطني بإمتياز يرتقي بالقرية ويعزز من ارتباط أوصالها، في نموذج دأب الشباب الإعلاميون والتقنيون البحرينيون على تعميمه على سائر القرى أهلياً وإجتماعياً في حركة تكافلية ضخمة، كان من المفترض أن يحصل على اهتمام الدولة أو تقديرها في الحد الأدنى لا القبض على أرواح روادها.

وشأنه شأن كثيرين لم يكن نشاطه عبثياً. إشتغل العشيري على نفسه قبل أي شخص آخر، وأتم دورات في القانون الدولي والإتصال السياسي والتنسيق الإعلامي وفن الخطابة وكتابة الأخبار والتقارير الصحفية، وكانت كلها إضافة إلى دراسته ومهنته في النقل البحري والشحن والميكانيك. كان الهدف من هذه المهارات التي إكتسبها كإضافة على مهنته الأصلية صقل المجتمع وتطويره. غير انه للأسف انتهت هذه الطاقة بطرفة عين ربما من قبل شخص لا يفقه شيئاً غير التلذذ بسادية مطلقة في تعذيب مساجين عاجزين غللت أجسادهم بالحديد بعد أن عجزت كل الطرق الأخرى في تكميم أفواههم.

ربما رحل العشيري، ولكن يبقى فعله وعمله خالداً وتشهد قريته قبل أي شخص آخر على أنه أدى واجبه على أكمل وجه، ولم يكن الشخص المعني بنفسه فقط بل كان من كافأ العرفان بالعرفان وخدم البلد الذي ولد فيه وظل طوال عمره ينتمي

محمد عبدالله

القرار رقم ١

محمد عبدالله

وُصِف بالقرار رقم واحد! وانتهى الأمر. قرار واحد، كلمة واحدة غيرت الحريات الالكترونية في البحرين. في الأول من يناير/كانون الثاني من العام ٢٠٠٩ أصدرت وزيرة الثقافة والاعلام آنذاك الشيخة مي بنت محمد آل خليفة ما سمي بـ «قرار رقم ١ للعام ٢٠٠٩ الخاص بتنظيم حجب وغلق المواقع في مملكة البحرين».

تضمن القرار ست مواد وزعت على مزودي خدمة الإنترنت في البحرين تلزمهم بحظر المواقع التي يأمر الوزير بحظرها وفق تقنيات موحدة بالإضافة إلى حظر أي منفذ – مثل البروكسيات – أو أية وسيلة أخرى يمكن تجاوز الحظر من خلالها. وحصرت كل صلاحيات رفع الحظر بتوقيع واحد هو توقيع الوزير، الذي سربت بعض المصادر أنها هي نفسها لا تملكه! ومن خلاله – أي القرار رقم ١ – دخلت السلطة في البحرين مستنقع القمع الإفتراضي، القمع الذي لا تكف الحكومات عن ممارسته بأعلى التكلفات والتقنيات، وتقوم الشعوب في مقابلها بتخطيه بخطوات بسيطة.

تفرض البحرين على أصحاب المواقع تسجيل مواقعهم رسمياً، وإستخراج رقم الترخيص الذي يخولهم بفتح مواقع بحرينية أو معنية بالبحرين، ما يعني تثبيت اسم وعنوان ومعلومات صاحب الموقع عند الدولة. وإقرار بما سوف يتضمنه الموقع والذي – بطبيعة الحال– لن يُرخّص اذا ما كان إتجاهه معارضاً للحكومة.

تصنف الحكومة البحرينية المواقع المحظورة بصنفين هما: المواقع الإباحية، والمواقع الطائفية. الأولى لم تكن أبداً مشكلة في بلد يستثمر في السياحة الجنسية من تحت الطاولة. أما «الطائفية» فهي الصفة التي تلصقها الحكومة بكل موقع معارض أو يحمل توجهات ومواقف تنتقد السلطة السياسية. فتكاد تكون معظم الشبكات الإلكترونية الخاصة بالقرى، والتي يتم التواصل الاجتماعي خلالها وتنشر فيها مواضيع على نسق إعلانات الزواج أو الوفاة ومجالس الضيافة وما شابه ذلك «طائفية ومحظورة» وكل المواقع السياسية المعارضة «طائفية ومحظورة» وكل المواقع غير البحرينية المتعلقة بالشأن السياسي البحريني «طائفية ومحظورة». وعلى الأغلب لقصور تقني تجد موقعي «غوغل للترجمة» و«أرشيف الإنترنت» ضمن المواقع المحظورة أيضاً.

على الطرف الآخر هناك مواقع معظمها «منتديات حوارية» يتم فيها التكفير والشتم والتخوين، لم تتعرض لأي مس من قبل الحكومة ويعود السبب إلى أنها تدار من قبل الديوان الملكي البحريني وفق أجندة خاصة لتغيير التركيبة الديموغرافية في البحرين حسب ما أشار تقرير البندر الذي كشف في عام ٢٠٠٦ عن خطة حكومية موسعة تتعلق بهذا الخصوص وأشار فيها إلى موقع «منتديات مملكة البحرين».

بعد دخول الحظر حيز التنفيذ تحرك بعض النشطاء السياسيين والالكترونيين لمواجهة القرار رقم ١. أقيمت ندوتان على الأقل إحداهما برعاية سياسية وأخرى برعاية إعلامية، تمثلت في جريدة الوسط البحرينية. وتبنت الموضوع أيضاً جريدة الوقت (التي توقفت عن الصدور لاحقاً لأسباب مالية بعد تمنع الدولة عن الإعلان فيها كما في سائر الصحف) وكانت تنشر مقالاً شهرياً على الأقل تحت عنوان «X شهور مرت على حجب المواقع» حيث «X» تعني عدد الشهور التي مرت منذ حجب أول موقع الكتروني لأول مرة في تاريخ البحرين. وكان يوجز الأخبار والتطورات التي حصلت في هذا الشهر فيما يخص شأن حظر المواقع. كما دُشنت عريضة إلكترونية وقّع عليها ألف شخص كانت ضمن خطة عمل متكاملة وضعت في جلسة عمل سرية لمجموعة كانت تعمل لأجل مكافحة القرار غير أنه ولأسباب غير معروفة كانت هذه العريضة الأمر الوحيد الذي أنجز من الخطة.

تشير التقديرات أن الدفعة الأولى من المواقع المحجوبة تفوق ١٠٠٠ موقع محلي. وفي مايو/أيار من ذات العام أصدرت منظمة فريدوم هاوس تقريراً عن حرية الصحافة، نالت فيه البحرين المرتبة ١٥٦ من أصل ١٩٥ دولة. ولم تزل الحكومة البحرينية حتى اليوم لا توفر جهداً في حظر المواقع المعارضة التي كان آخرها موقع مرآة البحرين الذي أُنشئ كصحيفة الكترونية بعد أحداث «ثورة الرابع عشر من فبراير» التي حصلت على غرار ثورات الربيع العربي. غير أن حظر المواقع بعد الثورة صار تحصيل حاصل وما يخشى منه اليوم هو مراقبة الإتصالات الخليوية وإستخدام الإنترنت. وقد سجلت عدة حوادث إختراق لمواقع معارضة وصفحات على الفيسبوك كان بعضها عن طريق إعتقال المسؤول عنها أو مصادرة اجهزته الإلكترونية. كما سجلت حالة تفتيش في مطار البحرين الدولي أجبر فيها المفتشون أحد المسافرين على أن يفتح كافة حساباته البريدية وحسابه في فيسبوك وتويتر والمواقع الالكترونية المختلفة وأخذ المفتشون نسخة عن كل هذه المراسلات.

اجمالاً يمكن القول أن وضع الانترنت في البحرين في أسوء أحواله منذ دخوله لأول مرة، إذ تجاوز الأمر حظر المواقع الإلكترونية وصار لزاماً على المستخدمين أخذ كافة الاحتياطات وشتى سبل التمويه لإتقاء شر المراقبة، ومن ثم الملاحقة والإعتقال.

كيفية تجنب الخدع على «فيسبوك»

إن أي من محاولات خدع «فيسبوك» التي تتنوع مثلاً بين الضغط على زر «لم يعجبني» (dislike button) و«متقفي المتعقب» (stalker tracker) (الذي يزعم أنه يدلكم على من يزور صفحتكم الخاصة) و«شاهد هذا الفيديو» (watch this video) لا تعتَبَر جديدة. وقد تعتقدون أن الأشخاص لن يستمروا بالوقوع في فخها. على العكس، بالطبع يقعون في فخها. فمقاومة الحاجة الملحة والفضول لنقر الزر يمكن أن تكون صعبة، ومنفذو الخدع يدركون ذلك. هم يستغلون فضول المستخدم وثقته من جهة، وقدرتهم على تصوير الخدع على أنها عمليات ترويج قانونية عبر الإنترنت من جهة أخرى. ولحسن الحظ، تتوفر بعض المؤشرات يمكن التنبه لها.

الأصدقاء المزيّفون

تتمثل إحدى الحيَل التي يستخدمها منفذو الخدع في «فيسبوك» بتشجيع الأشخاص على النقر على عنوان إنترنت (URL). وإذا بهم بدلاً من رؤية الموقع المرجو، يقومون عن غير قصد بإرسال رسائل غير مرغوب بها (Spam) إلى الأصدقاء مع روابط إلى عنوان الإنترنت نفسه. ويمكن لبعض الرسائل أن تكون مقنعة لدرجة أن ضحايا الخدع قد يفصحون عن معلومات شخصية مثل البطاقة الائتمانية أو أرقام الهاتف التي بإمكان منفذ الخدع استغلالها لاحقاً للقيام بعمليات تسديد أموال غير مسموح بها. والعنصر الأساسي في أي عملية خداع ناجحة يكمن في قدرتها على استغلال ثقة الضحية. ويُشار في هذا الصدد إلى أن العديد من الخدع تظهر على شكل روابط ضمن رسالات ينشرها أشخاص أنت على معرفة بهم. وعنصر النجاح يتمثل بأن هذه الخدع مصدرها أشخاص على شبكتنا الخاصة، وبالتالي فإن درجة تيقظنا تكون متدنية أصلاً، وذلك أمر يصعب جداً مكافحته.

وإذا قام صديق بنشر رابط على حائط الصفحة الخاصة بكم يبدو أنه تسجيل فيديو يرافقه تعليق «هل هذا الشخص أنت؟ lol»، قد تقوم على الأرجح بالنقر عليه. إلا أن الأمر قد يكون كناية عن خدعة أو رابط يذهب بكم إلى موقع مضرّ قام محتال بنشره مستخدماً حساب «فيسبوك» مسروق.

وفي ما يلي إشارتين بالغتي الأهمية لا بدّ من الانتباه لهما لدى النقر على أي رابط:

الأولى تتمثل بعدم ولوجك لدى النقر على الرابط إلى الصفحة المرجوة؛ أو أن التحميل يستغرق وقتاً أطول مما تتوقع. ويُشار هنا إلى أن أي تحميل متأخر قد يعني أنه يتم تناقلكم بين خوادم بروكسي (proxy server) لتغطية موقع المتسلل، وذلك، بدلاً من توجيهك فوراً إلى الصفحة المرجوة. والثانية تتمثل بضرورة التنبه للصفحات التي تطلب منكم فجأة الإفصاح عن معلومات تسجيل الدخول إلى «فيسبوك». ومتى تمكن منفذو الخدع من الوصول إلى تفاصيل الحساب الخاص بك، بإمكانهم استخدامه لبعث رسائل غير مرغوب بها إلى أصدقائك. وإذا حصل ذلك، أو إذا شككت بأي لعبة خداع مهما كان نوعها، قم بتغيير كلمة السر فوراً.

وبإمكان عنوانين مختصرة لمواقع إنترنت أن تشكل مخاطرة بما أن المستخدمين لا يمكنهم التمييز ما إذا كان عنوان الموقع صحيح عبر قراءته. وبالتالي، إذا قام أحدهم بنشر رابط مختصر على الحائط الخاص بصفحتكم أو عبر استخدام رسالة «فيسبوك» أو «دردشة» (Chat)، استأنف ما تقوم به بحذر. وفي نهاية الأمر، معظم الخدع مصممة لحصول منفذي الخدع على الأرباح من خلال برامج الدفع عند النقر (pay–per–click) أو عبر النفاذ إلى معلومات ممكن أن تسهل عملية تسديد أموال غير مسموح بها بواسطة البطاقات الائتمانية أو أرصدة الهاتف.

facebook

ما يمكنك أن تقوم به إذا وقعت ضحية إحدى الخدع

إذا اتضح لك أنه تم خداعك، قم أولاً بإلغاء التطبيق المضرّ (إذهب إلى زر «موقع» [Account] يليه «إعدادات الخصوصية» [privacy settings] ثم زر «تعديل إعدادات الخصوصية» [Edit your settings] الذي يقع أدنى «apps» و«websites» و«تعديل الإعدادات» [Edit Settings] الذي يقع أدنى «apps you use» وقم بالنقر على علامة X بالقرب من التطبيق الذي تريد إلغاءه). ثم قم بإلغاء أي رسالات منشورة قام التطبيق بها نيابةً عنك، وأنذر أصدقاؤك بما حصل وقم بتغيير كلمة السر الخاصة بحساب «فيسبوك».

يكمن عدم التعرض للخداع في التيقظ. تنبه إلى إعدادات خصوصيتك وقم بحصر ما يمكن أن تقوم به التطبيقات بالمعلومات الخاصة عنك أو بصفحة «فيسبوك» الخاصة بك. ولتعديل هذه الإعدادات، سجل دخولك إلى «فيسبوك» وأنقر على زر «حساب» في أعلى الصفحة إلى اليمين، ثم اختر «إعدادات الخصوصية» [privacy settings] ضمن «apps» و«Websites» في أسفل الصفحة إلى الشمال. أنقر على زر «تعديل الإعدادات» (Edit Settings) بالقرب من عبارة «How people bring your info to apps they use». الشكّ السليم هو نهاية الأمر عامل حاسم أيضاً.

نصائح إضافية:

تأكد من اسم واضع التطبيق. أنقر على اسم واضع التطبيق وتتبّعه إلى الصفحة الرئيسية الخاصة بالتطبيق. وابحث عن أي مؤشر قد يبدو غريباً أو غير مهني. قم ببحث عبر «غوغل» بشأن اسم التطبيق وواضعه.

استعلم عن تجربة مستخدم آخر. إن أي عملية بحث بسيطة من شأنها أن تثمر عن نتائج تبرز ما هو قانوني وما هو غير قانوني. لا تفصح عن معلومات شخصية (من ضمنها اسم تسجيل الدخول الذي تستخدمه في «فيسبوك» وكلمة السر) إلى أي شخص إلا في حال كنت واثقاً من الوضع القانوني للمتلقي ومدى أمن قنوات التوزيع.

لا بدّ لك من التنبه إلى أن أمنك في شبكات التواصل الاجتماعي يعتمد جزئياً على مدى أخذ الآخرين الذين ينتمون إلى شبكتك مسألة الأمن بعين الاعتبار. قد لا يكون الأمر معقداً، إلا أن خبراء الأمن يعتبرون أن الحماية الأفضل لكم تكمن في أن «تحذروا مما تنقرون عليه».

كيف أغير أو أحمي عنواني على الإنترنت

عادة ما يرغب الناشطون على الإنترنت بتشفير الإتصال وحماية بياناتهم المرسلة عبر الإنترنت، كذلك الأمر بالنسبة للعديد من الشركات والمنظمات. كما ان بعض الإجراءات في هذا السياق قد تمنع السلطات أو الهاكرز من تتبع تصفحهم وعنوانهم على الإنترنت.

أحد البرامج الأكثر إستعمالاً حول العالم في هذا السياق هو «هوت سبوت شيلد» ليس لكونه يوفر حماية فحسب بل طريقة عمله تجنب الحجب وتمكن الإطلاع على المواقع والمدونات المحجوبة.

ويتميز هذا البرنامج بالصفات التالية:

– يؤمن اتصال بشبكة الإنترنت مع تشفير HTTPS، كما يوفر إستعمال آمن للتسوق عبر الإنترنت ونقل البيانات والمعلومات الشخصية وحماية نفسك من سرقة الهوية على الإنترنت.

– إخفاء عنوان بروتوكول الإنترنت (IP) الخاص بك.

– الوصول إلى كافة محتويات الإنترنت دون رقابة وإمكانية تخطي جدران الحماية الالتفافية.

– حماية نفسك من المتلصصين على شبكة «واي فاي» والفنادق والمطارات ومكاتب الشركات.

– يعمل على كافة الانظمة ويندوز وماك، بما في ذلك أنظمة التشغيل الجديدة (ويندوز ٧، وسنو ليوبارد، وليون).

نحن نقّدر شبكة الإنترنت بسبب الحرية التي توفرها للإستكشاف والتنظيم والتواصل. «هوت سبوت شيلد» يمكننا من الوصول إلى جميع المعلومات على الانترنت وتوفير حرية الوصول إلى جميع محتويات الويب بحرية وأمان. وهو يؤمن السريّة والأمان ويحافظ على خصوصيتك على الانترنت. إن برامج مكافحة الفيروسات تحمي جهاز الكمبيوتر الخاص بك، ولكن ليس نشاطك على الإنترنت.

كيف يعمل الهوت سبوت شيلد؟

يقوم هوت سبوت شيلد بإنشاء شبكة افتراضية خاصة (VPN) بين حاسوبك وبوابة الإنترنت خالية من العوائق. حيث تم إنشاؤه أساساً لتمكين المستخدمين من الوصول إلى الإنترنت عن طريق خادم وسيط، مما يمكّنهم من الإفلات من آليات حجب وفلترة محتوى الإنترنت وبالتالي تجنب الرقابة، وذلك للحصول على السرية للمعلومات بين كمبيوتر المستخدم وخوادم هوت سبوت شيلد، وضمان إخفاء الهوية عند الوصول لمصادر الإنترنت.

هذه الشبكة لا يمكن إختراقها من قبل المتلصصين، والمتسللين، ومقدمي خدمات الانترنت، ولذلك لن يستطيع أحد إستعراض أي شيء من نشاطك على الإنترنت مثل: الرسائل الفورية، والتنزيلات، ومعلومات بطاقة الإئتمان أو أي شيء آخر ترسله عبر الشبكة. «هوت سبوت شيلد» هو برنامج مجاني، ويستخدم أحدث تقنيات الشبكات الخاصة الإفتراضية، وسهل التركيب والإستخدام.

إن شركة AnchorFree هي المالكة ل«هوت سبوت شيلد» وتؤمن ارباحها ومدخولها من الدعايات التي تظهر في المتصفح خلال إستعمال البرنامج.

يمكن تنزيل وإستعمال هوت سبوت شيلد بالنقر هنا.

ما هو برنامج KeePass؟

إن برنامج KeePass هو برنامج مجاني وموثوق يعمل على جميع أنظمة ويندوز وماكنتوش، ويوجد منه نسخ خاصة للهاتف iphone, ipad, Android, BlackBerry. وظيفته الأساسيّة هي حفظ وتخزين كلمات المرور (Passwords) الخاصة بالمستخدم بطريقة سهلة وآمنة.
كل ما يتوجب على المستخدم فعله من خلال هذا البرنامج هو حفظ كلمة سر واحدة آمنة، وخلق قاعدة بيانات بكلمات المرور، والبرنامج سيتذكر جميع كلمات المرور ويحفظها في مكان مشفّر.
كل شخص لديه عدد من كلمات المرور التي يستعملها لتسجيل الدخول الى بريده الالكتروني أو حساباته في مواقع متعدّدة على الانترنت، وكلمات المرور تزيد بعدد حسابات المستخدم. ويُفضّل استعمال كلمة مرور مختلفة لكل حساب، بالاضافة الى تغيير كلمة المرور كل شهرين لكي يحمي المستخدم بياناته. وبما أنه سيصبح لدينا كلمات مرور عديدة وليس من السهل تذكّرها جميعها، وقد يصادف وجود شخص جالس بقربنا ويشاهد ماذا نطبع على لوحة المفاتيح، فإنّ برنامج KeePass يحل لنا جميع هذه المشاكل.
يعمل ال KeePass على تخزين جميع كلمات المرور الخاصة بالمستخدم في قاعدة بيانات مشفّرة تحت مفتاح رئيسي (ملف مفتاح) يحمله المستخدم معه على وسيلة تخزين مثل CD أو USB ومحمي بكلمة مرور واحدة، طويلة، وآمنة، ولا يعرفها سوى المستخدم نفسه. بالاضافة الى هذا، يستطيع المستخدم اضافة أو حذف أو تغيير كلمات السر بشكل متكرّر. وهنا يقوم KeePass باقتراح كلمات مرور قويّة. كما انه من الممكن أيضاً أن يقوم المستخدم بتخزين جميع كلمات المرور التي يستعملها في مجموعة واحدة أو تصنيفها في مجموعات متعدّدة. وهنا لا بد من ذكر أن قاعدة البيانات والحقول المتعلّقة بكلمة المرور بالاضافة الى اسم المستخدم، الخ.... كلها مرمّزة ومشفّرة بطريقة آمنة جداً.
KeePass هو برنامج مفتوح المصدر، وهو يمكّن المستخدم من القاء نظرة على الكود الخاصة بالبرنامج، وتجميع الشيفرة بنفسه. أخيراً، إن برنامج KeePass متوفر بثلاثين لغة.

يمكن تحميل برنامج KeePass من هنا.

إضغط هنا للمشاهدة على يوتيوب