ورقة بحثية: حين تخترق الحكومات المعارضين: نظرة إلى الجهات الفاعلة والتكنولوجيا

ورقة بحثية مقدّمة من:

ويليام ر. ماركزاك، *جامعة كاليفورنيا في بيركلي، سيتزن لاب*

جون سكوت رايلتون، *جامعة كاليفورنيا في لوس أنجلوس، سيتزن لاب*

مورغان ماركيز بوار، *سيتزن لاب*

فيرن باكسون، *جامعة كاليفورنيا في بيركلي، معهد الهندسة الكهربائية وعلوم الكمبيوتر* ICSI

ترجمة: مرآة البحرين

ملخص

لطالما راقبت الدول القومية القمعية عالم الاتصالات لرصد المعارضين السياسيين، ويضيف الإنترنت وشبكات التواصل الاجتماعية تحديات تقنية جديدة إلى هذه الممارسة حتى أنها تفتح ميادين جديدة للمراقبة. نحلل في هذه الدراسة مجموعة واسعة النطاق من الملفات المشبوهة والروابط التي استهدفت الناشطين والمعارضين والجمعيات غير الحكومية في الشرق الأوسط على مدى السنوات القليلة الماضية. ونجد أن هذه الأدوات تعكس مساع لمهاجمة الأجهزة الخاصة بالمستهدفين، وذلك لغرض التنصت وسرقة المعلومات وكشف هويّة المستخدمين المجهولين. وسنقوم بوصف حملات الهجوم التي رصدناها في كل من البحرين وسوريا والإمارات العربية المتحدة، وكذلك المهاجمين والأدوات والتكنيكات المستخدمة في التحقيق. وإلى جانب فيروسات حصان طروادة trojan الجاهزة للنفاذ عن بعد واستخدام خدمات طرف ثالث لتعقب بروتوكول الإنترنت IP ، نُعرّف في هذه الدراسة أيضًا برامج التجسس التي تباع حصريًا إلى الحكومات بما فيها برنامج شركة غاما للتجسس FinSpy ونظام التحكم RCS الذي تنتجه شركة Hacking Team. وسنسلط الضوء على استخدامات هذه البرامج في البحرين والإمارات العربية المتحدة، كما سنرسم النطاق الأوسع المحتمل لهذه النشاطات عبر إجراء مسح عالمي لـ"سيرفرات" القيادة والتحكم المطابقة (C&C)

servers، وفي النهاية نؤطّر التبعات الواقعية لهذه الحملات، وذلك عبر دليل ظرفي قوي يربط القرصنة بالاعتقالات والتحقيقات والسجن.

١. المقدمة

تكرس أبحاث أمن الكمبيوتر جهودها لحماية الأفراد من الحملات العشوائية واسعة النطاق مثل تلك التي يشنها مجرمو الإنترنت. ومؤخّرا، استحوذت مشكلة حماية المنشآت من الهجمات الموجّهة التي تشنها الدول (والمعروفة بالتهديدات المستمرة المتقدمة) على اهتمام بحثي كبير. ورغم التداخل بين نطاقي هاتين المشكلتين؛ إلا أن هجمات قرصنة الكمبيوتر الموجهة التي تشنها الدول القومية ضد الأفراد، لم تلق أي اهتمام بحثي منهجي حتى الساعة. وتطرح هذه المشكلة الجديدة تحديات معقدة تقنيًا وذات أهمية كبيرة على مستوى الواقع العالمي في ذات الوقت.

أخذنا على عاتقنا في هذا العمل أن نميّز المشكلة الناشئة لهجمات الإنترنت في الدول القومية ضد الأفراد المرتبطين بحركات مؤيدة للديمقراطية أو بحركات معارضة. وفي الوقت الذي تنقصنا فيه المعلومات من أجل تحقيق هذا العمل بشكل شامل كليّا، نوفّر تفاصيل واسعة من الناحيتين التقنية والتنفيذية كما ظهرت في ثلاث دول. نحن نعرض هذا التوصيف كخطوة أولى أساسية وضرورية للمتابعة العلمية الدقيقة إلى فضاء إشكالية جديدة.

اعتمدنا في دراستنا هذه على نتاج سنوات طويلة من الأبحاث التي أجريناها على حالات من البحرين وسوريا والإمارات العربية المتحدة، فضلًا عن ذلك، وضعنا أطرًا لطبيعة هذه الهجمات والتكنولوجيا والبنى التحتية المستخدمة من أجل هذا الغرض في إطار تأثيراتها على المواطنين. ونأمل أن نشكل من خلال هذه العملية مصدر إلهام لجهود بحثية إضافية تعالج المشكلة الصعبة في كيفية حماية الأفراد بطريقة مناسبة في ظل وجود موارد محدودة في وجه خصوم أقوياء.

وكمثال على هذه الظاهرة نستعرض الحكاية الآتية التي جمعنا تفاصيلها من التقارير العامة وملفات المحكمة.

في فجر ٢٠١٣/١٢/٣ اقتحمت الشرطة منزل "علي الشوفة" ذي السبعة عشر عامًا وصادرت كمبيوتره الشخصي وهاتفه واعتقلته واتهمته بوصم ملك البحرين بالطاغية والساقط على حساب تويتر تحت اسم مستعار هو @alkawarahnews. وبحسب ملفات المحكمة، فإن وحدة مكافحة الجريمة الإلكترونية في

[1] التواريخ الواردة في المستندات مرتبة على الشكل الآتي: الشهر/ اليوم/ السنة

البحرين قد ربطت بين عنوان بروتوكول الإنترنت IP المسجل باسم والده وبين الحساب في ٢٠١٢/٩/١٢. وأرسل مشغّلو حساب alkawarahnews@ بعدها رسالة خاصة مشبوهة إلى أحد المؤسسين. تم استلام هذه الرسالة في ٢٠١٢/٨/١٢ في حساب فيسبوك مرتبط بحساب تويتر نفسه، وتضمنت الرسالة رابطًا عن فيديو احتجاج يزعم أنه أُرسل من قبل شخص مناهض للحكومة. يتم تحويل هذا الرابط إلى iplogger.org، وهي خدمة تسجل عنوان بروتوكول الإنترنت IP لأي شخص يدخل إلى أي رابط بمجرد النقر عليه. وأشارت تحليلات الرابط أنه قد تم الدخول إليه مرة واحدة من داخل البحرين. حكم على علي بالسجن لمدة سنة واحدة في ٢٠١٣/٦/٢٥.

تشكل قضية "علي" مثالًا عن الظاهرة الأكبر التي نحقق فيها: هجمات ضد الناشطين والمعارضين والنقابيين ودعاة حقوق الإنسان والصحافيين وأعضاء من منظمات غير حكومية في الشرق الأوسط (والتي نعرّفها هنا من الآن فصاعدًا بـ "الأهداف"). إن الهجمات التي وثقناها تضمنت غالبًا استخدام روابط خبيثة أو مرفقات ببريد إلكتروني مصممة للحصول على معلومات من جهاز الكمبيوتر. شاهدنا هجمات تستخدم نطاقًا واسعًا من برامج التجسس الجاهزة وخدمات الطرف الثالث المتاحة علنيًا مثل iplogger.org من جهة. ومن جهة أخرى، استخدمت بعض الهجمات ما يسمى بـ "الاعتراض القانوني" باستخدام حصان طروادة وبرامج ذات صلة يبدو أن الشركات، مثل شركة غاما وفريق القرصنة Hacking Team، تبيعها بشكل حصري إلى الحكومات. وتقول شركة "فريق القرصنة" إن الحكومات تحتاج إلى هذه التكنولوجيا "للنظر من خلال عيون أهدافها" أكثر من الاعتماد فقط على "المراقبة السلبية" [١]. وبالإجمال، فإن الهجمات التي نوثقها تعتبر من التقنيات الجديدة والنادرة. وفي الواقع، نظن أنه كان بالإمكان الحد من أكثر الهجمات بشكل كبير عبر الاحترازات الأمنية المعروفة جدا، وإعدادات البرامج وتحديثاتها. ومع هذا، فالهجمات هذه جديرة بالذكر نظرًا لهندستها الاجتماعية الدقيقة وارتباطها بالحكومات وتأثيرها الحقيقي على أرض الواقع في العالم.

لقد حصلنا على معظم ملفاتنا من خلال تشجيع الأفراد المحتمل أن يكون تم استهدافهم من قبل الحكومة ليزودونا بالملفات المشبوهة والروابط غير المرغوب فيها خاصة من مرسلين غير معروفين. ومع أن هذه العملية زودتنا بمجموعة غنية من الملفات لنحللها، إلا أنها لم تسمح لنا بالقول إن مجموعة البيانات التي لدينا تمثيلية.

تربط تحليلاتنا هذه الهجمات بفئة شائعة من الجهات الفاعلة: مهاجمون سلوكهم أو اختيارهم للهدف أو استخدامهم للمعلومات المكتسبة من الهجوم تتلاقى مع مصالح حكومة. وفي بعض القضايا، مثل قضية علي،

يبدو أن المهاجمين هم الحكومات أنفسها وفي قضايا أخرى يظهر أن المهاجمين هم من مناصري الحكومة؛ بعضهم من المواطنين الذين لا ينتمون بالضرورة إلى المتطوعين المهرة، وبعضهم من مرتزقة الإنترنت. هذا وتم تعريف الظاهرة سابقا، كما حصل في ليبيا عندما كشف سقوط نظام القذافي علاقات الحكومة المباشرة بالقرصنة خلال الحرب الأهلية في العام ٢٠١١ [٢].

نحن نقدم المشاركات التالية:

- نحلل التقنية المرتبطة بالهجمات الموجّهة (على سبيل المثال: الروابط الخبيثة وبرامج التجسس) ونتعقّبها حتى الوصول إلى المبرمجين أو المصنعين. وفي حين أن هذه الهجمات غير جديدة - وفي الحقيقة تتضمّن عادة تكنولوجيا مستخدمة في عالم الجريمة الإلكترونية - إلا أنها مهمة لأن لديها تأثير حقيقي وظاهر على أرض الواقع وهي مرتبطة بالحكومات. فضلًا عن ذلك، لطالما وجدنا أخطاء هواة إما في تقنية المهاجم أو عملياته تظهر أن الطاقة المبذولة لمواجهة هذه التهديدات قد تحقق فوائد كبيرة غير أننا لم نخلص إلى القول إن هجمات الدول القومية أو المهاجمين واهنة ونظن أن بعض الهجمات استطاعت تخطّي تحرّياتنا.
- عند الإمكان، نميز تجريبيًا الهجمات والتقنية التي نرصدها. سنرسم خريطة الاستخدام العالمي لأداتي قرصنة تجاريتين تستخدمهما الحكومات عبر البحث في بيانات مسح الإنترنت باستخدام بصمات سيرفرات القيادة والتحكم مستمدة من تحليلاتنا لبرامج التجسس.
- نطور دليلًا قويًا يربط الهجمات بالحكومات المموّلة، والشركات الموردة، يرد على إنكار هذا الارتباط، بطريقة حيّة أحيانًا أو غير مباشرة أحيانًا أخرى، [٣ و٤ و٥ و٦]، في مقابل الإنكارات [٧] أو مزاعم مجلس الرقابة على شركة ما [٨]. وقد احتمل مسحنا استخدام "الاعتراض القانوني" بحصان طروادة Trojan في ١١ دولة أخرى تحكمها "أنظمة مستبدة". ونحن ندرك أن الناشطين والصحافيين في هذه الدول قد يتعرضون لمضايقات أو تهديدات تؤثر على حياتهم أو حريتهم بسبب مراقبة الحكومة.

وأخيرًا، نحن لا نستكشف إمكانيات الدفاع المناسبة لحماية المواطنين المستهدفين في هذا العمل. نحن نؤمن أنه من أجل القيام بذلك بطريقة هادفة مستندة إلى أسس متينة يتطلب الأمر أولًا فهم معرفة المستهدفين بقضايا الأمن، وضعهم فيما يتعلق بكيفة حماية أنفسهم حاليًا والموارد (بما يمكن أن يتضمّن التعليم) التي يمكن

أن يستندوا إليها. للوصول إلى هذا الهدف، نجري الآن (بموافقة مجلس المراجعة المؤسساتي) مقابلات عميقة مع الأهداف المحتملة بالإضافة إلى فحص ممنهج لأجهزة الكمبيوتر الخاصة بهم من أجل فهم هذه الأمور.

٢. أعمال ذات صلة

في العقود الأخيرة تطورت هيئة غنية بالأعمال الأكاديمية لتوثيق وفهم رقابة الحكومة على الإنترنت بما فيها حملات الرقابة القومية مثل الجدار الناري الصيني العظيم Great Firewall of China [٩ و١٠ و١١]. ويشكل البحث حول مراقبة الإنترنت الحكومية والنشاطات الأخرى مثل الاعتراض لتطبيق القانون مساحة صغيرة نسبيًا [١٢]. وتدرس بعض الأعمال الأكاديمية استخدام الأجهزة لتمكين الرقابة مثل القائمة السوداء الرئيسية لمستخدمي برامج الدردشة (المحادثة) الصينيين [١٣] أو برنامج مراقبة مضمون الإنترنت The Green Dam censorware التي كانت ستحمل على الحواسيب الجديدة كلها المباعة في الصين [١٤]. نحن على دراية بأن العمل السابق محدود فيما يتعلق بالبحث في في عوامل التهديدات المتقدمة التي تستهدف الناشطين من خلال القرصنة، حتى إن لم يكن هذا العمل قادرًا دائما على إيجاد دليل حول علاقات الحكومة [١٥].

المنصّات التي تستخدمها الأهداف المحتملة مثل الجي ميل GMail[١٦] وتويتر [١٧] وفيسبوك [١٨] تزداد في جعل تشفير "طبقة النقل" Transport Layer الوضع الافتراضي، مخفية هذه الاتصالات أمام معظم شبكات المراقبة. إن استخدام هذا التشفير، مع الطابع العالمي للعديد من من الحركات الاجتماعية ودور المنفيين، يزيد من القرصنة جاذبية، خاصة بالنسبة للدول غير القادرة على طلب المحتوى من هذه المواقع أو إجبارها على إرساله. في الواقع، إن الاستخدام المتزايد للتشفير والطبيعة العالمية للأهداف ذُكرت من قبل مزودي برامج "الاعتراض القانوني باستخدام فيروس حصان طروادة" في موادهم التسويقية [١،١٩]. وفي قضية بارزة في العام ٢٠٠٩، وزعت شركة "اتصالات" في الإمارات العربية المتحدة تحديث نظام لمستخدمي هاتف البلاك بيري ال١٤٥٠٠٠، يحتوي على برنامج تجسس لقراءة بريد البلاك بيري الإلكتروني المشفر من الجهاز. وقد تم اكتشاف برنامج التجسس عندما تسبب التحديث ببطء كبير في أجهزة المستخدمين [٢٠]. وعلى خلاف التوزيع بحسب نطاق البلد، ينظر عملنا في نوع هذه الرقابة الموالية للحكومة والمرتبطة بالحكومة عبر هجمات موجّهة بشكل عال.

إن مصطلح التهديدات المستمرة المتقدّمة APT يشير إلى مهاجم إنترنت متطوّر يحاول باستمرار استهداف فرد أو جماعة. [٢١] ويقع العمل خارج المجتمع الاكاديمي المتعقّب لهجمات الحكومة الإلكترونية في هذا النطاق. كان يوجد عمل مهم متعلق بالتهديدات المستمرة المتقدّمة APT خارج المجتمع الأكاديمي خاصة بين اختصاصيي الأمن، وشركات تهديدات الاستخبارات، ومجموعات حقوق الإنسان، وقد ركز جزء كبير من هذا العمل على الهجمات الإلكترونية المشبوهة التي تشنها الحكومات على الحكومات الأخرى أو على الشركات [٢٢ و٢٣]. وفي هذه الأثناء، تتعامل هيئة متخصصة في هذا البحث (صغيرة، لكنّها متنامية) مع الهجمات التي تشنها الحكومات ضد المعارضة والجماعات الناشطة التي تعمل داخل وخارج حدود بلدانهم. أكثر الحالات بروزًا هي غوش نت GhoshNet، وهي حملة تجسس واسعة النطاق ضد حركة استقلال التيبت [٢٤ و٢٥]. وهناك أعمال أخرى تتجنب الاستنتاجات حول المهاجمين [٢٦].

البلد	نطاق التاريخ	معدل المستهدفين	رقم النموذج ونوعه	برامج التجسس المميزة وسيرفرات القيادة والتحكم
البحرين	٢٠١٢/٩/٤_ 31/7/2013	≤ ١٢ ناشطًا ومعارضًا ونقابيًا و وأعضاء في جماعات حقوق الإنسان وصحافيين	٨ نماذج من برنامج FinSpy و٧ روابط تجسس على برتوكول الإنترنت IP عبر رسائل خاصة وأكثر من ٢٠٠ رابط تجسس على بروتوكول إنترنت IP رصدت علنًا.	٤ عناوين بروتوكول إنترنت IP مميزة
سوريا	٢٠١١ حتى الآن	١٠-٢٠ فردًا ذوي خلفية تقنية يستقبلون ملفات مشبوهة من معارفهم على الإنترنت	٤٠-٥٠: أغلبهم فيروس بلاك شايد BlackShades, وبرنامج دارك كوميت DarkComet، وبرنامج اكستريم رات Xtreme RAT، وبرنامج ان جي رات njRAT، وبرنامج شادو تيك رات ShadowTech RAT.	١٦٠ عنوان بروتوكول إنترنت IP مميز

الإمارات العربية المتحدة	٢٠١٢/٧/٢٣_ ٢٠١٣/٧/٣١	٧ ناشطين ودعاة حقوق الإنسان وصحافيين	٣١ نموذج برمجيات خبيثة مميزة ولها ٧ أنواع و٥ ثغرات مميزة	١٢ عنوان بروتوكول إنترنت IPمميز

جدول ١: نطاق معلومات الدراسة

البلد	التأثيرات الممكنة	التأثيرات المحتملة
البحرين	١. اعتقال ٣ أفراد حكم عليهم بالسجن من شهر إلى سنة ٢. زعيم نقابي استجوبته الشرطة، وطرد من العمل	١. الحكم على ناشط بالسجن لمدة عام ٢. اقتحام الشرطة لمنزل
سوريا	١. كشف اتصالات المعارضة الحساسة للحكومة ٢. استخدام المواد المسربة لكشف هوية الناشطين واعتقالهم	**١.** أصبح أعضاء المعارضة فاقدي مصداقية بسبب نشر مواد محرجة **٢.** استخدام قوات الأمن للمواد المسربة خلال التحقيقات
الإمارات العربية المتحدة	استهداف المعارف Contacts ببرامج خبيثة	سرقة كلمة المرور وتحميل رسائل البريد الإلكتروني

جدول ٢: تحليل الآثار السلبية المعقولة أو الممكن حدوثها من الهجمات


From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

1 attachment: Rajab.rar 1.4 MB Save

الشكل رقم ١: رسالة بريد إلكتروني تحتوي على ملف تجسس FinSpy

٣. نظرة عامة على البيانات والآثار الناجمة

ترتكز دراستنا على تحليل شامل للملفات الخبيثة والاتصالات المشبوهة المتعلقة بنشاطات المجموعات المستهدفة في البحرين وسوريا والإمارات العربية المتحدة كما ورد في الجدول رقم ١. وقد كان لعدد من الهجمات أثر حقيقي مهم كما ورد في الجدول رقم ٢. وفي حالات كثيرة، أبقينا شرحنا غامضًا بعض الشيء لتجنب التسرب المحتمل للهويات المستدفة.

بدأنا عملنا عندما تواصل معنا أفراد قلقون من أن يكونوا قد استهدفوا من قبل الحكومة بسبب هجمات الإنترنت. وعندما أصبحنا أكثر اطلاعاً على المجتمعات المستهدفة، تواصلنا في بعض الحالات مباشرةً مع هذه المجموعات، وفي أحيانٍ أخرى، تواصلنا مع أفراد ذوي ارتباط مع الجماعات المستهدفة وقد سمحوا لنا بتفحص اتصالاتهم مع الجماعات المستهدفة. وفيما يتعلق بالبحرين وسوريا، شمل العمل ١٠٠٠٠ بريد إلكتروني ورسائل فورية. أما الدراسة التي تتعلق بالإمارات العربية المتحدة، فقد استندت إلى آلاف الاتصالات.

٤. دراسة حالات: ثلاث دول

تحدد الأقسام التالية حملات قرصنة استهدفت مؤخرًا البحرين وسوريا والإمارات العربية المتحدة. ولهذه الحالات ثيمة مشتركة: هجمات على كمبيوترات الأهداف وأجهزتهم من خلال ملفات وروابط خبيثة. في

بعض الحالات، استخدم المهاجمون برامج خبيثة مكلفة وتباع للحكومات حصريا، بينما استخدموا في حالات أخرى، أدوات رخيصة ومتوفرة بسهولة RATs. نستنتج من هذه الحالات أن "الهندسة الاجتماعية" الذكية Social Engineering تلعب غالبًا دورًا مركزيًا، وهو دليل قوي على وجود خصوم مطلعين. كما وأننا، ومع ذلك، نجد كثيرًا من الأخطاء الفنية والتشغيلية يقوم بها المهاجمون، ما أمكننا من ربط الهجمات بالحكومات. وبشكلٍ عام، فالهجمات التي نجدها لا يتم الكشف عنها بشكل جيد من قبل برامج مكافحة الفيروسات anti-virus program .

٤,١ البحرين

قمنا بتحليل حملتي هجوم ضد البحرين، حيث كانت الحكومة تمارس حملة قمع ضد ثورة استلهمت من الربيع العربي منذ ٢٠١١/٢/١٤.

شملت الأولى رسائل بريد إلكتروني خبيثة تحتوي على FinSpy، و هو فيروس حصان طروادة، يستخدم في "الاعتراض القانوني" "trojan" lawful intercept ويباع حصريًا للحكومات. أما الحملة الثانية، فقد شملت روابط تجسس على بروتوكول الإنترنت IP ورسائل إلكترونية "مصنّعة بشكل خاص"، وقد صممت للكشف عن عناوين بروتوكول الإنترنت IP الخاصة بمشغلي حسابات بأسماء مستعارة. بعض الأفراد الذين نقروا على ما يبدو على هذه الروابط ألقي القبض عليهم في وقت لاحق، بمن في ذلك علي (راجع الهامش رقم ١)، الذي تم استخدام نقرته click ضده في المحكمة. وفي حين تشير كلتا الحملتين إلى مسئولية الحكومة، لم نحدد حتى الآن التداخل بينهما، وظهر أن أهداف برنامج التجسس FinSpy مقيمون أساسًا خارج البحرين، في حين أن روابط التجسس على بروتوكول الإنترنت IP استهدفت أساسًا أولئك الموجودين داخل البلاد. سندرس كل حملة على حدة.

حملة FinSpy. بدأت في أبريل/نيسان ٢٠١٢ عندما تلقى المؤسسون ٥ رسائل إلكترونية مشبوهة من نشطاء وصحافيين يسكنون في المملكة المتحدة والولايات المتحدة ويعملون من أجل البحرين. وقد وجدنا أن بعض الملفات المرفقة تضمنت ملف (.exe) مصمم ليظهر كصورة. وحوت أسماء ملفاتهم رمز Unicode

right-to-left override (RLO) دفع نظام التشغيل ويندوز إلى تغيير اسم الملف إلى gpj.1bajaR.exe بدلًا من exe.Rajab1.jpg.

وقد حوت ملفات الضغط rar. الأخرى مستند وورد مع ترميز ASCII مدمج في ملف exe يحتوي شفرة ماكرو مخصصة ضبطت بحيث تعمل تلقائيًا عند فتح الوثيقة. وتحت إعدادات الأمان Security الافتراضية، يعطل برنامج Office كافة وحدات الماكرو غير الموقعة، بحيث يرى المستخدم الذي يفتح المستند رسالة إعلامية تفيد أنه تم تعطيل الماكرو. وبالتالي، تم تصميم هذا الهجوم على ما يبدو مع الاعتقاد أو الأمل في أن المستهدف قام بتخفيض إعدادات الأمان.

تحديده على أنه FinSpy: عبر فحص العينة باستخدام Windows Virtual PC، وجدنا القيمة التالية في الذاكرة و هي: .\y:\lsvn_branches\finspyv4.01\finspyv2 وتشير هذه القيمة إلى FinSpy، وهو منتج من شركة غاما الدولية [٢٧]. استخدمت الملفات التنفيذية exe تشويشًا افتراضياً [٢٨]، بدا أنه مصمم بشكل خاص. و قد قمنا بابتكار بصمة للمشوش وحددنا ملفًا تنفيذيًا مماثلًا في الهيكلية، من خلال البحث في قاعدة بيانات كبيرة للبرمجيات الخبيثة. احتوى الملف التنفيذي قيمة مماثلة، إلا أنه قام بتعريف نفسه ك FinSpy v3.00، وحاول الاتصال ب tiger.gamma-international.de ، وهو نطاق مسجل باسم شركة غاما الدولية.GmbH

تحليل القدرات: وجدنا أن لبرنامج التجسس تصميمًا ذي وحدات، ويمكن أن يقوم بتحميل وحدات إضافية من سيرفرات القيادة والتحكم، بما يشمل صيد كلمة المرور (من أكثر من ٢٠ تطبيقًا)، وتسجيل لقطات الشاشة، ودردشة سكايب، ونقل الملفات، وما يدخل من ميكروفون الكمبيوتر وكاميرته.

لإعادة إرسال البيانات إلى ***سيرفرات القيادة والتحكم***، تقوم وحدة بتشفيرها وكتابتها على القرص في ملف خاص. ويتحقق برنامج التجسس دورياً من هذا الملف بحثًا عن الملفات التي تطابق اصطلاح تسمية معينة، ثم يرسلها إلى سيرفر القيادة والتحكم. بعد ذلك يقوم بالكتابة فوق الملفات وإعادة تسميتها عدة مرات ويحذفها في محاولة لإحباط التحليلات الجنائية.

تحليل التشفير: كون البرامج الخبيثة استخدمت عددًا لا يحصى من التقنيات المعروفة المضادة للتصحيح و التحليل anti-debugging and atnit-analysis، فقد أُحبطت محاولاتنا لأن نربطها بـ debgguer. نظرًا لأنها لم تتضمن شفرة مضادة لـ VM، فقد شغلناها ببرنامج TEMU، وهو محاكي x86 المصمم لتحليل البرامج الخبيثة [٢٩]. ويلتقط TEMU، آثار تنفيذ مستوى التعليمات ويقدم الدعم لتتبع الخلل.

وجدنا أن برنامج FinSpy يشفر البيانات باستخدام تطبيق مخصص من AES-256-CBC. يتم إنشاء مفتاح AES ذي ال٣٢ بايت والـIV ذي ال ١٦ بايت من خلال قراءة ساعة نظام ويندوز ذات الترتيب المنخفض ذي ال٤ بايت، مرارًا وتكرارًا. ويتم تشفير المفتاح والـIV باستخدام المفتاح العام RSA 2048 المضمن فيها، وتخزينه في ذات الملف مثل البيانات. ويفترض أن المفتاح الخاص يقع على سيرفرات القيادة والتحكم. وتقوم مفاتيح الAES الضعيفة بفك تشفير البيانات بشكل مباشر. وقد صمّمنا برنامجًا يستطيع بشكل عام بإيجاد هذه المفاتيح في أقل من ساعة، مستغلًا حقيقة أن الكثير من قراءات ساعة النظام تحدث خلال ساعة التحديث نفسها.

بالإضافة إلى ذلك، فشل كود FinSpy AES في تشفير المجموعة الأخيرة من البيانات إذا كانت أقل من حجم كتلة AES ذات ال ١٢٨ بت، وترك أثرا لنص عادي. أخيرًا، يستخدم بروتوكول برنامج FinSpy للأسلاك نوع التشفير نفسه من أجل الاتصال بسيرفرات القيادة والتحكم، وبالتالي يخضع لقوة الهجوم نفسها على مفاتيح AES. في حين أننا نشك في أن قصور تشفير FinSpy يعني خللا ما، من الممكن أن نتصور أيضا أن التشفير قد تم إضعافه عمدًا لتسهيل قدرة حكومة واحدة على مراقبة الحكومات الأخرى.

سيرفر القيادة والتحكم: العينات أرسالت خلال الاتصال مع ٧٧,٦٩,١٤٠,١٩٤، والتي تنتمي إلى مشترك من بتلكو، مزود خدمة الإنترنت الرئيسي في البحرين. وقد كشفت عملية تحليل حركة مرور البيانات على الشبكة بين الآلة الافتراضية المصابة وسيرفر القيادة والتحكم أن الملقم استخدم IPID عالمي، الأمر الذي سمح لنا باستنتاج نشاط السيرفر من خلال تقدمه.

وردًا على عملنا التفحّصي، قال مسؤول تنفيذي في شركة غاما للصحافة إن سيرفر FinSpy البحريني كان مجرد سيرفر وسيط Proxy وإن السيرفر الحقيقي يمكن أن يكون في أي مكان، كجزء من ادعاء أن استخدام البحرين ل FinSpy يمكن أن يكون مرتبطًا بحكومة أخرى [٤] . ومع ذلك، فإن السيرفر الوسيط proxy قد يظهر فراغات في IPID عالمي حين يعيد توجيه حركة المرور؛ إلا أن ملاحظتنا الدقيقة والمتتالية لـ IPIDs تناقض هذا البيان.

استغلال البيانات التي تم التقاطها: بما أننا اشتبهنا أنه من المرجح أن يسعى مشغل التجسس لاستغلال معلومات الدخول التي التقطها، لا سيما تلك التي ترتبط مع المنظمات الناشطة البحرينية، عملنا مع بحرين ووتش، وهي منظمة ناشطة داخل البحرين، أنشأت صفحة تسجيل دخول وهمية على موقعها على الإنترنت، وقدمت لنا اسم المستخدم وكلمة المرور. ومن خلال جهاز افتراضي نظيف، تمكنا من الدخول إلى الصفحة

مستخدمين بيانات الاعتماد هذه، مع حفظ كلمة المرور في موزيلا فايرفوكس .Mozilla Firefox بعد ذلك قمنا بإصابة الجهاز الافتراضي بفيروس برنامج FinSpy وسمحنا له بالإتصال بسيرفر القيادة والتحكم في البحرين. وقد كشف ملف السجل في موقع "بحرين ووتش" عن دخول متكرر من 89.148.0.41 (على الصفحة الرئيسية للموقع، بدلًا من صفحة تسجيل الدخول التي أنشأناها)، وقد جاء ذلك بعد فترة وجيزة من إصابة الجهاز الافتراضي. ومع فك تشفير حزمة البيانات الملتقطة من نشاط أداة التجسس، وجدنا أن جهازنا الافتراضي قد أرسل كلمة المرور إلى الخادم قبل دقيقة واحدة بالضبط:

INDEX,URL,USERNAME,PASSWORD,USERNAME FIELD,
PASSWORD FIELD,FILE,HTTP 1,
http://bahrainwatch.org,bhwatch1,watchba7rain,
username,password,signons.sqlite,,
Very Strong,3.5/4.x

لم يتضمن الـ URL الموفر للسيرفر المسارإلى صفحة تسجيل الدخول التي لم يكن يمكن الوصول إليها من الصفحة الرئيسية. ويعكس هذا التجاوز حقيقة أن قاعدة بيانات كلمات المرور في فايرفوكس تخزن أسماء النطاقات فقط، وليس كامل عناوين صفحة تسجيل الدخول، لكل كلمة مرور. وأسفر تكرار التجربة مرة أخرى عن دخول آخر من عنوان بروتوكول الإنترنت IP نفسه في غضون دقيقة. قمنا بتفتيش ملف سجلات بحرين ووتش، والتي لم تظهر أي نشاط لاحق (أو سابق) من هذا العنوان، ولا أي حالات من قيم "المستخدم الوكيل" نفسه.

حملة التجسس على بروتوكول الإنترنت (IP): في هجوم تجسس على عنوان بروتوكول الإنترنت IP، يهدف المهاجم إلى اكتشاف عنوان بروتوكول إنترنت الضحية IP الذي هو عادة مشغل حساب زائف على وسائل التواصل الاجتماعية أو بريد إلكتروني. يرسل المهاجم إلى الحساب الزائف رابطًا إلى صفحة ويب أو رسالة بريد إلكتروني تحتوي على صورة مضمنة عن بعد، وذلك باستخدام واحدة من الخدمات الكثيرة المتاحة[٢]. عندما ينقر الضحية على الرابط أو يفتح البريد الإلكتروني، يظهر عنوان بروتوكول الإنترنت IP للمهاجم. ويكشف المهاجم بعدها هوية الضحية من الشركات المزوّدة لخدمات الإنترنت[٣]. في حالة واحدة، حددنا وثائق قانونية وفرت علاقة ظرفيّة بين رابط تجسس من هذا القبيل، واعتقال مرتبط به لاحقا.

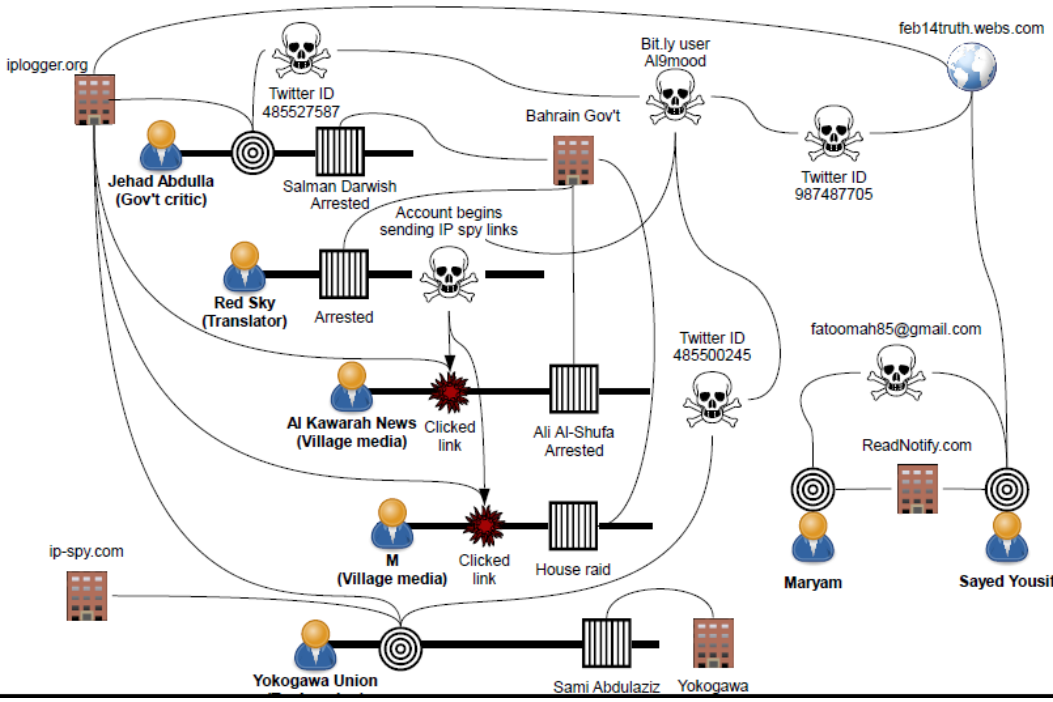
---

[2] e.g., iplogger.org, ip-spy.com, ReadNotify.com

٣ يعمد عدد من مزودي بريد الويب وعملاء البريد الإلكتروني إلى اتخاذ خطوات محدودة لمنع تحميل هذا المحتوى تلقائيًا، ولكن بدا أن بعض رسائل البريد الإلكتروني المنتحلة التي تأتي من مرسل موثوق تتجاوز في بعض الأحيان هذه الدفاعات
.

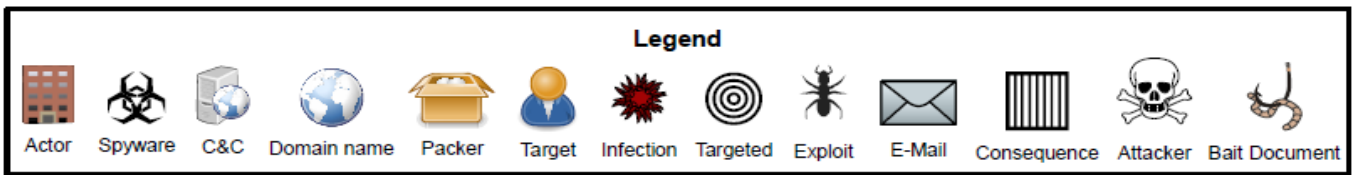
ويوضح الرسم (٢) النظام البيئي الأكبر لهذه الهجمات. يبدو أن المهاجمين يمثلون كيانًا واحدًا، حيث يرتبط كل النشاط مجددًا بالحسابات التي أرسلت روابط "مقصّرة" باستخدام حساب محدد وهو al9mood[٤] (الكتابة بالحروف اللاتينية من الكلمة العربية "صمود") في موقع bit.ly لخدمات تقصير الروابط.

لنتذكّر مجددا علي فيصل الشوفه (ذكر في القسم ١)، الذي اتهم بإرسال تغريدات مهينة من حساب @ alkawarahnews (شبكة الكورة الإعلامية في الرسم ٢). أحد مشغلي الحساب أعطانا رسالة خاصة مشبوهة مرسلة إلى حساب أخبار الكورة على فيسبوك من "Red Sky". ألقي القبض على Red Sky في ٢٠١٢/١٠/١٧ (بحسب مزاعم)، وأدين بإهانة الملك على حساب تويتر التابع له @ RedSky446، وحكم عليه بالسجن لمدة أربعة أشهر[٥]. وعندما أطلق سراحه، وجد أن كلمات المرور لحساب تويتر، والفيسبوك، والبريد الإلكتروني قد تم تغييرها ولم يعرف كيفية استرداد حساباته.



4A Romanization of the Arabic word for “steadfastness.” [4]

[٥] وفقًا للمعلومات التي حصلنا عليها من اثنين من مستخدمي تويتر، إذ ادعى أحدهما أنه التقر ريد سكاي في السجن، في حين كان الآخر مشتركًا معه



الرسم ٢: النظام البيئي Ecosystem لهجمات التجسس على عناوين ال IP في البحرين.

تضمنت الرسالة التي أرسلت من حساب ريد سكاي إلى صفحة أخبار الكورة رابطًا مختصرًا باستخدام خدمة جوجل ggo.gl. وقد استخدمنا goo.gl API للوصول إلى تحليلات الرابط، ووجدنا أنه لم يختصر إلى iplogger.org/25SX وقد أنشئ في ١٢/٨/١٢. وتلقى الرابط نقرة واحدة فقط جاءت من البحرين وكان المرجع www.facebook.com.

احتوت ملفات قضية علي طلبًا من النيابة العامة للحصول على معلومات حول عنوان بروتوكول إنترنت IP كانت قد ربطته بصفحة أخبارة الكورة alkawarahnews بعد حوالى ٢٢ ساعة من إنشاء الرابط. وأشارت وثائق المحكمة إلى أن بيانات ISP ربطت عنوان بروتوكول الإنترنت IP بـ"علي"، وعلى هذا الأساس حكم عليه بالسجن لمدة سنة واحدة .

كما استهدف ريد سكاي M في الرسم ٢. تذكر M نقره على رابط مرسل من ريد سكاي أثناء استخدام الإنترنت من أحد المنازل في قريته. وقد داهمت الشرطة المنزل في يوم ٢٠١٣/١٢/٣، بحثًا عن المشترك المتصل بالإنترنت في المنزل. تمحور استجواب الشرطة حول تغريدات وصفت الملك البحريني بأنه "ملعون". وكان ريد سكاي قد استهدف في وقت سابق مستخدمين آخرين عبر روابط تجسس على الـ IP وقد كانت الروابط مختصرة باستخدام حساب al9mood على bit.ly أيضا.

لم يكن الهجوم على جهاد عبدالله جديرًا بالذكر، لانحياز نشاط الحساب إلى المجتمعات المنتقدة للمعارضة في البحرين. ومع ذلك، فقد وجه الحساب أيضًا انتقادات مباشرة للملك في بعض الأحيان، وقد أشار في حالة واحدة إلى أنه "ضعيف" و "بخيل". وأرسل حساب مرتبط بـal9mood إلى جهاد عبدالله رابط بروتوكول إنترنت للتجسس في ٢٠١٢/١٠/٢ في رسالة علنية. وبتاريخ ٢٠١٢/١٠/١٦، اعتقل سلمان درويش بتهمة إهانة الملك باستخدام حساب جهاد عبد الله وحكم عليه بالسجن لمدة شهر واحد، ويعود ذلك إلى الاعتراف الذي أدلى به. هذا ويدعي والد سلمان أن الشرطة قد حرمت ابنه من الطعام والشراب والرعاية الطبية.

استهدف حساب آخر مرتبط بـal9mood حساب @ YLUBH، وهو حساب تويتر يعود إلى اتحاد يوكوجاوا، نقابة عمالية في الفرع البحريني لشركة يابانية. تلقى @ YLUBH على الأقل ثلاثة روابط تجسس على بروتوكول الإنترنت IP في أواخر عام ٢٠١٢، أرسلت عبر رسائل عامة على تويتر. وطردت يوكوجاوا زعيم النقابة سامي عبد العزيز حسن في ٢٠١٣/٣/٢٣ [٣٠] و صرحت لاحقًا أن سامي كان في الواقع المشغل للحساب @ YLUBH، وأن الشرطة قد استدعته للاستجواب فيما يتعلق بتغريداته [٣١].

استخدام الصور المضمنة عن بعد: حددنا عدة أهداف تلقت رسائل إلكترونية بأسماء مستعارة تحتوي على صور مضمنة عن بعد. ويبين الرسم ٢ اثنتين من هذه الحالات، مريم وسيد يوسف. كان المهاجم قد أرسل رسائل البريد الإلكتروني باستخدام ReadNotify.com، والذي يسجل عنوان بروتوكول الإنترنت IP المستخدم حين يحمّل بريده الصورة البعيدة.[٦]

مع العلم أن ReadNotify.com يحظر التحايل في شروط استخدامه، إلا أن لخدمته ثغرة معروفة لدى المهاجمين (وهذا ما أكدناه) والتي تسمح بالتحايل في الـ"Form" من خلال وضع المعطيات المطلوبة مباشرة على استمارة التقديم على موقعهم على الإنترنت. لم نعثر على أدلة تشير إلى أن هذا الخلل معروف علنًا، ولكن يبدو واضحًا أن المهاجم استغل ذلك، على اعتبار أن استمارة التقديم أضافت X-Mai1er: RNwebmail header لم تضف عند الإرسال عبر أساليب ReadNotify.com الأخرى المعتمدة. وقد ظهر العنوان في كل بريد إلكتروني أرسلته إلينا الأهداف.

عند التحايل باستخدام هذه الطريقة، يبظل العنوان الأصلي للمرسل ظاهرا في X-Sender وفي الأجزاء العلوية الأخرى. وفقًا لذلك، فإن كل رسائل البريد الإلكتروني التي تلقتها الأهداف أرسلت من العنوان fatoomah85@gmail.com. وقد وجدت صلة بين الرابط المرسل في إحدى هذه الرسائل الإلكترونية وحساب al9mood على bit.ly

خلال مراقبتنا حسابات متصلة ب al9mood، أحصينا أكثر من ٢٠٠ رابط تجسس على بروتوكول الإنترنت IP في التدوينات العامة على فيسبوك وفي رسائل تويتر. استخدم المهاجمون في كثير من الأحيان (١) حسابات الأفراد البارزين و الموثوق بهم بدلًا من المسجونين مثل "ريد سكاي" (٢) وشخصيات وهمية (على سبيل المثال، النساء الجذابات أو الباحثين الوهميين عن وظيفة عند استهداف نقابة عمالية)، أو (٣) انتحال حسابات قانونية. وفي واحدة من التكتيكات الذكية، استغل المهاجمون الخط الافتراضي في تويتر،

[6] عملاء بريد ياهو والآي فون يحلون تلقائيًا هذه الصور عن بعد خاصةً من البريدات الالكترونية التي تظهر على أنها من مرسلين موثوقين

على سبيل المثال استبدال الحرف "l" الصغير بالحرف "I" الكبير أو تبديل أحرف العلة (على سبيل المثال من "a" إلى "e") لإنشاء أسماء متطابقة عند النظرة الأولى. بالإضافة إلى ذلك، تميل الحسابات الخبيثة إلى حذف تغريدات التجسس على الـ IP المرسلة عبر تعليقات (عامة) بسرعة، وكثيرًا ما تتغير الأسماء المستخدمة في الحسابات profile names.

٤,٢ سوريا

إن استخدام برامج التحكم عن بعد RATs ضد المعارضة كانت ميزة موثقة للحرب الأهلية السورية منذ التقارير الأولى التي نشرت في مطلع العام ٢٠١٢ [٣٦ و٣٩ و٤٠ و٣٢ و٣٤]. الظاهرة منتشرة وبحسب تجربتنا، فإن معظم أعضاء المعارضة يعلمون أن أعمال القرصنة تحدث. وكما لخصنا في الجدول ٣، فإن الهجمات تتضمن غالبًا أدوات أمنية وهمية أو خبيثة؛ فضول أو مضمون إيديولوجي أو يمت للحراك بصلة (مثال: لائحة أسماء الأشخاص المطلوبة). تقترح تقنيات الجذب وملفات الطعم فهمًا جيدًا لحاجات المعارضين وخوفهم وسلوكهم، مقرونًا بتداول برامج التحكم عن بعد الجاهزة. تجري الهجمات في بعض الحالات في نطاق يشير إلى أكثر من علاقة مباشرة مع أحد المتخاصمين: ولاحظت المعارضة السورية بانتظام أن حسابات الموقوفين تبدأ بالتقاط البرامج الخبيثة بعد فترة وجيزة من اعتقال قوات الحكومة لهم [٤١].

هذا وقد سبق للباحثين واختصاصيي الأمان أن جمعوا بعض المعلومات عن الكثير من برامج التحكم عن بعد هذه بما فيها برنامج دارك كوميت DarkComet [٤٢ و٤٣] وبرنامج التحكم عن بعد بلاك شادز Black-shades Remote Controller [٣٨] وبرنامج التحكم عن بعد إكستريم Xtreme RAT [٤٤] وبرنامج التحكم عن بعد إن جي njRAT [٢٦] وشادو تك ShadowTech [٣٦]. بعض هذه البرامج متاحة للشراء من قبل أي شخص بعكس برامج FinSpy و RCS المتوفرة فقط للحكومات. على سبيل المثال، برنامج التحكم عن بعد إكستريم Xtreme RAT يباع بمبلغ ٣٥٠€ وبلاك شادز يباع ب ٤٠€، أما البرامج الأخرى مثل دارك كوميت DarkComet فهي متوفرة مجانًا. وكذلك لاحظنا نسخات ملفات كراك crack من هذه البرامج في منتديات قرصنة عربية حيث يجعلون هذه البرامج متاحة بنسخة قيد التجربة بجهود ضئيلة ومن دون أموال. ومع أن برامج التحكم عن بعد هذه أقل كلفة وتعقيدًا من برامج FinSpy وRCS، إلا أن جميعها لديها الوظيفة نفسها؛ تسجيل اللقطات ورصد لوحة المفاتيح والتحكم البعيد للكاميرات والميكروفونات والتحكم عن بعد ونقل الملفات.

وتعرض الصورة رقم ٣ التسلسل المشترك لأكثر الهجمات حيث يلتقط المهاجم برمجيات خبيثة عبر رسالة دردشة خاصة أو منشورات في مجموعات التواصل الاجتماعي التي تملكها المعارضة أو رسائل إلكترونية. وتحد هذه التقنيات غالبًا الرؤية العالمية للملفات والروابط الخبيثة مبطئين بذلك منتجاتهم السمعية البصرية الشائعة. تتلقى الأهداف إجمالًا أو (١) PE في zip. أو .rar أو (٢) أو رابطًا لتنزيل ملف أو (٣) رابطًا يحرك القرص من خلال التحميل. وتتضمن الرسائل بالعادة نصًا، يكون بالعربية غالبًا ، يحاول أن يقنع الهدف بتنفيذ الملف أو بالضغط على الرابط.

وتعود الهجمات الأولى في الرسم ٣ إلى العام ٢٠١٢ واستخدام ملفات الطعم من خلال تحميل برنامج التحكم عن بعد دارك كوميت DarkComet . تتشارك هذه الهجمات نفس خادم القيادة والتحكم 216.6.0.28، وهو عنوان بروتوكول إنترنت IP تابع إلى شركة الاتصالات السورية والمعرفة علنًا كسيرفر قيادة وتحكم سوري لبرمجية خبيثة منذ فبراير/شباط ٢٠١٢ [٤٥]. يعرض ملف الطعم الأول للضحية نسخةPDF تحتوي على معلومات حول الثورة المخططة في حلب، لكن هذا الملف بالواقع هو شاشة توقف تتنكر بشكل نسخةPDF باستخدام يونيكود من اليمين إلى اليسار تحت اسم ".fdp.scr." يظهر للضحية كـ ".rcs.pdf.". أما ملفات الطعم الأخرى فهي برامج حماية تحتوي على برنامج دارك كوميت DarkComet متخفية ببرنامج تشفير اتصال سكايب مما أدى إلى ارتياب المعارضة بتسلل الحكومة إلى البرمجيات المتعارفة. أما الهجمة الثالثة في الرسم ٣، فقد لوحظت في أكتوبر/تشرين الأول ٢٠١٣ وتظهر الأهداف مع البريد الإلكتروني الذي يزعم احتواؤه على رابط فيديوهات حول الصراع الراهن ويكون بذلك قد أصاب جهاز الهدف ببرنامج اكستريم Xtreme RAT عبر استخدام رابط القيادة والتحكم tn1.linkpc.net.

ومن أجل القبض على الأهداف، يستخدم المهاجمون حسابات مفضوحة (بما فيها حسابات الأفراد المسجونين) أو هويات وهمية تتخفى على أنها مناصرة للمعارضة. يعرض رسمنا بالمصطلحات المجردة استخدام حساب الضحية أ لالتقاط برنامج خبيث (خطة حلب) عبر (ما يسمى) رسائل سكايب إلى الضحايا (ب ن). وفي قضايا العضو المعارض ت والعامل في المنظمة غير الحكومية د (هنا، الضحايا حقيقيين وليسوا وهميين) تم الاستهداف من خلال البريد الاكتروني من مجالات يبدو أنها تعود إلى جماعات معارضة تظهر تسوية محتملة. ويبقى مجال واحد فعال يستضيف موقع جبهة النصرة السلفية [٤٦] بينما يظهر أن المجالات الأخرى غير فعالة. استلم العضو المعارض ت ملفًا خبيثًا مرفقًا مع بريد إلكتروني، في حين أُرسل إلى العامل

د رابط مختصر(url[.]no/Uu5) كي يحمله من دليل[٧] .Mrconstrucciones.[.]net، وهو موقع قد يكون مصابًا. وقد نتج عن هاتين الهجمتين اقتحام برنامج التحكم عن بعد اكستريم Xtreme RAT لهذين الجهازين.

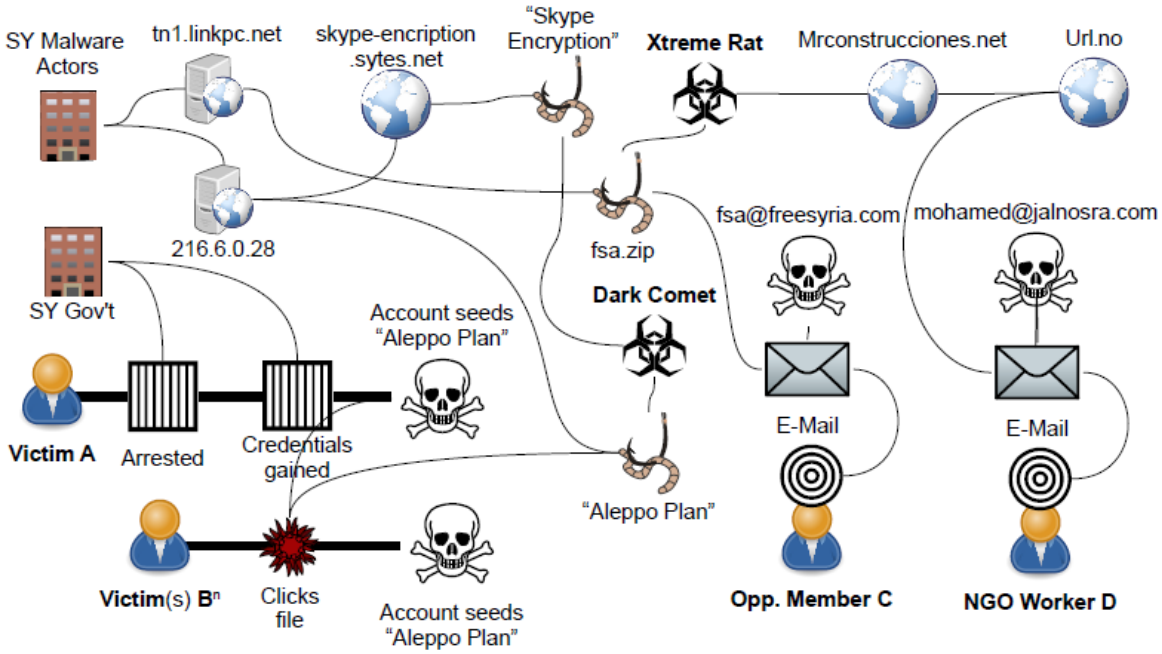
أما في حالة تشفير سكايب الوهمي، فامتدت الخدعة إلى فيديو يوتيوب من "مختبر أمن تكنولوجيا المعلومات" IT Security lab [٤٧] يعرض قدرات البرنامج المزعومة كما يعرض موقعًا يسوق الأداة، skype-ecryption.sytes.net. هذا وأنشأ المهاجمون قاعدة واجهة مستخدم رسومية GUI مغشوشة لتشفير برنامجهم (انظر الرسم ٤). تحتوي واجهة المستخدم الرسومية عددًا من الأزرار غير الفعالة مثل "تشفير" و"فك التشفير" اللذين من شأنهما توليد استجابات وهمية. وفي الوقت الذي يتم فيه تشتيت انتباه الهدف بفعل هذه العملية الفارغة، يتمكن برنامج دارك كوميت Dark Comet من جهازه ٣,٣ [٣٢ و٣٣].

النوع	المميزات	أمثلة (برامج التحكم عن بعد RATs)
أدوات الامان	ملفات تنفيذية تظهر كأدوات وغالبًا ما تكون مقرونة بتفسيرات أو جمل عن قيمتها في الجذب المستهدف. على سبيل المثال، على موقع التواصل الاجتماعي وفي موقع التحميل أو في فيديوهات	"تشفير سكايب" (DC)[٣٢و٣٣] و"أمان الفايسبوك" custom [٣٤] ومضاد للقرصنة (DC)[٣٥] و Fake Freegate VPN (ST)[٣٦].
ملفات ذات صلة إيديولوجية أو ذات صلة بالحراك	ملف أو PE كتحميل او مرفق مع تشجيع على فتح الملف الذي يحمل غالبًا اسمًا مستعارًا بنسخة PDF أو برامج الحكومة المسربة بشكل غير إرادي. الاستخدام الدائم لRLO لإخفاء الوصلة الحقيقية (مثل exe. أو scr.)	"أسماء الأفراد المطلوبين من قبل النظام"(DC) و"خطة ثورة حلب"(DC) [٣٧] وفيديوات مهمة(BS)[٣٨] وملف "مجلس متمردي حماة" (DC) [٣٩] وقاعدة بيانات "الأشخاص المطلوبة" (custom) وفيديواهتت تابعة للحراك (برنامج التحكم عن بعد أن

[٧] تجعله غامضًا لتجنب النقرات العرضية على برمجيات URLsالخبيثة الفعالة

		جيnjRAT) وملف عن الجيش السوري الحر (برنامج التحكم عن بعد اكستريم).
أدوات مختلفة	الأدوات التي تزعم أنها تقدم أشياء تابعة للمعاضة، مثل: آداة وهمية تدعي أنها تقدم "تقارير كبيرة" عن صفحات النظام على الفايس بوك.	hack facebook pro v6.9 (DC) [40]

الجدول ٣: الحملات وبرامج التحكم عن بعد المستخدمة في المراقبة السورية.Blackshades BS بلاك شادز/ DarkComet DC، دارك كوميت/ST شادو تك ShadowTech.

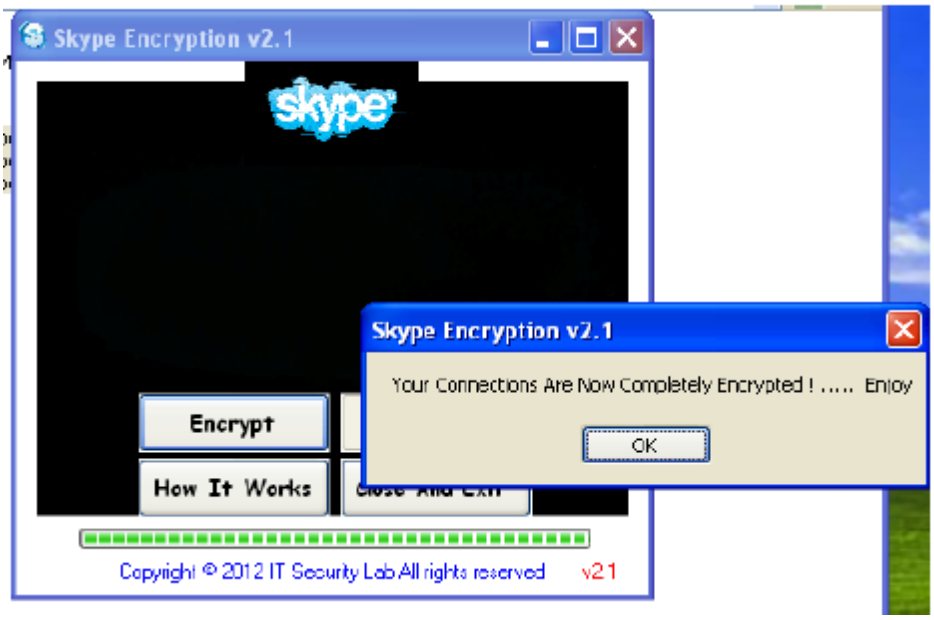


الرسم ٣: نموذج من النظام البيئي Ecosystem لحملات برامج سورية خبيثة

ويبدو أن الحملات تستهدف بشكل أساسي الأحداث في الصراع الجاري، فعلى سبيل المثال، تضاءلت الحملات ومن ثم ازدادت بشكل كبير خلال ساعات بعد إيقاف الإنترنت في سوريا في العام ٢٠١٢ [٤٨].

وكذلك لاحظ المؤسسون أن النشاط تضاءل أيضًا بعد توقعات تدخل الولايات المتحدة العسكري ضد أهداف الحكومة السورية في سبتمبر/أيلول ٢٠١٣. عندما تم إبطال هذا الاحتمال، لاحظنا ارتفاع حجم النماذج الجديدة والحملات مجددًا بما فيها الاستهداف الأخير للعاملين في المنظمات غير الحكومية كما يظهر في الرسم ٣. نحن ندرك رقم حالات المعارضة الضئيل في استخدام برامج تحكم عن بعد RATs مشابهة ضد مناصري الحكومة السورية، على الرغم من أن دليل الهجمة الإلكترونية عبر طرف ثالث موجود.

التبعات الحقيقية: لقد تم اخفاء لوجستيات ونشاطات جماعات المعارضة السورية العديدة عمدًا عن الشعب وذلك لحماية نفوذ الحكومة وأرواح الأفراد المشاركين فيها. مع العلم أن أفراد المعارضة السورية يحيطون علمًا بقصص التسويات الرقمية للشخصيات البارزة التي تتضمن أولئك الموكل إليهم أدوار حساسة فضلًا عن الأعضاء العاديين وتطرح تسوية أمن العمليات تهديدًا موثقًا لحياة كل من ضحايا التسوية الإلكترونية وأفراد العائلات والمؤسسات.



الرسم ٤: برنامج سكايب المزور يشتت انتباه الهدف واعدًا إياه بالاتصالات المشفرة بينما يصيب جهازه ببرنامج دارك كوميت DarkComet.

ويجعل الصراع السوري المستمر عملية جمع أدلة شاملة حول العلاقة بين ممثلي الحكومة وحملات البرمجيات الخبيثة أمرًا صعبًا. فضلًا عن ذلك، تم سجن الكثير من الأشخاص الذين فضحت هوياتهم أو إخفاؤهم، وبذلك أصبحنا عاجزين عن إيجاد علاقة بالأدلة المعروضة عليهم خلال التحقيق. ولكن ما زالت

الأدلة الظرفية القوية تربط استخدام برامج التحكم عن بعد RATs وجرائم الصيد الإلكترونية "فيشينغ" phishing، ونشاط الحكومة الذين نلخصهم بإيجاز هنا: (١) روى الكثير من السوريين للصحافيين والمؤسسين كيف أن المحققين واجهوهم بمواد من كمبيوتراتهم الخاصة. على سبيل المثال:

قال لي الشرطي، "هل تذكر عندما كنت تتحدث إلى رفيقك وأخبرته أن شيئًا ما جرى [منقول] وأنك دفعت مبلغًا كبيرًا من المال؟ في ذلك الوقت كنا نأخذ معلومات من كمبيوترك الشخصي". [٤١]

(٢) لقد زود الناشطون السوريون الصحافيين العالميين بقضايا [٤١] وتبع الاعتقالات كبح سريع لعدد من حسابات الموقوفين على شبكات التواصل الاجتماعية ملتقطين بذلك برامج خبيثة للائحة الأسماء (الرسم ٣). (٣) وعلى الرغم من سوء سمعة حملات الهجوم، بما فيها القيادة والتحكم وبروتوكول الإنترنت C&C IPs في الصحافة العالمية [٤٥]، إلا أن الحكومة السورية لم تدلِ بأي تعليقات رسمية حول هذه الحملات ولم تقوم بأي عمل لإيقاف السيرفر.

إلى جانب هذه التحديات القائمة، كان لحملات البرامج الخبيثة هذه أثر ملموس على المعارضة السورية ولكنها تتوافق بشكل عام مع مصالح حملات دعاية الحكومة السورية. فقضية عبد الرزاق طلاس، وهو قائد في الجيش السوري الحر، هي حالة توضيحية للاستخدامات المحتملة لهذه الحملات، ففي العام ٢٠١٢ ظهرت سلسلة من فيديوهات جنسية لطلاس وهو يؤدي رسائل وأفعال إباحية له أمام كاميرا كمبيوتره [٤٩] ومع أنه نفى هذه الفيديوهات، إلا أن الضرر الذي لحق بسمعته كان كبيرًا وكانت النتيجة أن تم استبداله[٥٠].

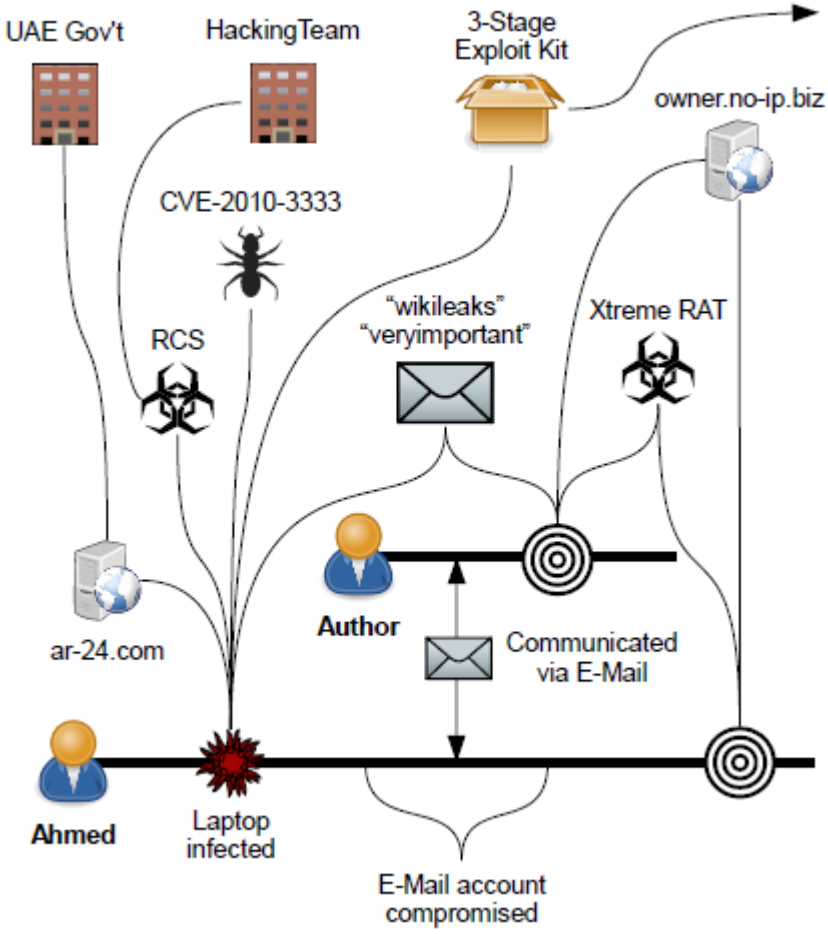
٤,٣ الإمارات العربية المتحدة

في الوقت الذي لم تشهد فيه الإمارات العربية المتحدة أي ثورة أو اضطراب سياسي مؤخرًا، استطاعت أن تقمع معارضتها المتزامنة مع الربيع العربي.

إن أولى الهجمات التي لحظناها في الامارات العربية المتحدة تضمنت "اعتراضًا قانونيًا" حصان طروادة؛ معروف بنظام التحكم عن بعد Remote Control System (RCS) ويباع من فريق قرصنة شركة ايطالية. هذا وأشار سيرفر القيادة والتحكم إلى تورط حكومة الامارات العربية المتحدة المباشر. وتوقفنا مع الوقت عن استلام نماذج نظام التحكم عن بعد RCS من أهداف اماراتية ولاحظنا عوضًا عن ذلك نقلة في استخدام برامج التحكم عن بعد الجاهزة RATs ، واحتمال تدخل مجموعات مرتزقة إلكترونية. إلا أن مهاجمي ضعفاء أمن العمليات سمحوا لنا بإيجاد علاقة بين أكثر الأهداف المشاهدة سويًا.

نظام التحكم عن بعد RCS : تم سجن الناشط الإماراتي محمد منصور (راجع الرسم ٥) من أبريل/نيسان إلى نوفمبر/تشرين الثاني ٢٠١١ بعد توقيعه عريضة مطالبة بالديمقراطية على الإنترنت [٥١] وتلقى بريدًا إلكترونيا يظهر أنه من "ويكيليكس العرب" في يوليو/تموز ٢٠١٠. فتح محمد منصور الملف المرفق الذي كان يحمل اسم "veryimportant.doc" (ملف مهم) ورأى ما وصفه ب"أحرف ملخبطة". وأرسل محمد البريد الإلكتروني إلينا من أجل إجراء التحقيق.

استخدم المرفق CVE-2010-3333، وهو تحليل RTF قابل للسقوط في مايكروسوفت وورد. لم يضم الملف أي طعم في المحتوى وجزء من ملف RTF تالف مما أوضح أن الثغرة الأمنية موجودة في الملف. وقد حملت هذه الثغرة كود القشرة shellcode الذي حمّل من ar-24.com والذي بدوره حمل برنامج تجسس من ar-24.com. نبين هذه التجميعة في3-stage Exploit Kit في الرسم ٥.



الرسم ٥: جزء من النظام البيئي Ecosystem لحملات مراقبة هجمات الإمارات العربية المتحدة.

وكذلك عمل سيرفر القيادة والتحكم C&C server على ar-24.com. عندما حصلنا على النموذج في يوليو/تموز ٢٠١٢، حلل ar-24.com على أنه يعود إلى عنوان بروتوكول إنترنت Linode وهو مزود استضافة. وبعد ثلاثة أشهر، حلل على أنه يعود إلى عنوان إماراتي تابع للفريق الملكي [٥٢] وهو منظمة تابعة للحكومة الإماراتية العربية المتحدة برئاسة الشيخ طحنون بن زايد آل نهيان، وهو عضو في الأسرة الحاكمة في الإمارات العربية المتحدة وابن مؤسسها.

تحديده على أنه نظام للتحكم عن بعد: لقد عرّفنا مقاطع من الذاكرة تطابقت مع تحليل دلالي [٥٣] لبرنامج التحكم عن بعد RCS (المعروف أيضًا بدافنشي أو كرايسس DaVinci or Crisis)، وهو منتج من فريق القرصنة من الشركة الإيطالية [٥٤]. هذا واستطعنا تحديد موقع ملف وورد مشابه تركيبيًا عبر فايروس توتال VirusTotal. استخدم الملف الثغرة نفسها وحاول تحميل مرحلة ثانية من rcs-demo.hackingteam.it الذي كان غير متوفر عند وقت الفحص.

تحليل القدرات: لبرنامج التحكم عن بعد RCS مجموعة من الوظائف المشابهة عمليًا لبرنامج FinSpy، إلا أن هناك اختلافًا في الموجهات المستخدمة لتحميل برنامج التجسس. وحددنا نماذج إضافية (راجع §٥) التي كان معظمها في ملف jar. والذي يحمل نسخة نظام تشغيل مناسبة لنظام التحكم عن بعد (ويندوز أو أو. إس. اكس) الذي يستخدم الثغرات اختياريًا. اذا تم تضمينه كبرنامج صغير ولم يكن هناك وجود للثغرات، ويعرض الجافا تحذيرًا أمنيًا ويسأل المستخدم إن كان يوافق على هذا التنزيل. ورأينا أمثلة عن3Stage Exploit Kit حيث تضمنت المرحلة الأولى استغلال الفلاش وفي بعض الحالات استطعنا تحصيل المراحل كلها والتأكيد أنها حملت برنامج للتحكم عن بعدRCS . واستطعنا أن نجمع بعض النماذج بواسطةMPress Packer[٥٥] وجُعلت بعض نماذج ويندوز مبهمة لتبدو كعميل Putty SSH.

ويوجد فرق آخر مهم، على سبيل المثال، نموذج نظام التحكم عن بعدRCS . الذي أرسل إلى أحمد يضيف تشغيل مفتاح التسجيل، بينما نماذج FinSpy المستخدمة في البحرين تكتب فوق القرص الصلب لتعديل قطاع إقلاع؛ يتم تحميل برنامج التجسس قبل نظام التشغيل ويدخل نفسه إلى عمليات نظام التشغيل بمجرد بدئها. وكان لنماذج برامج التحكم عن بعد القدرة على الانتقال أيضًا إلى أجهزة أخرى حتى تلك غير النشطة منها في أم وير VMWare الحقيقية عبر تعديل صورة القرص على محرك أقراصUSB وهواتف ويندوز المحمولة. وكانت النتيجة أننا لم نجد قدرات متشابهة في نماذجFinSpy التي اختبرناها.

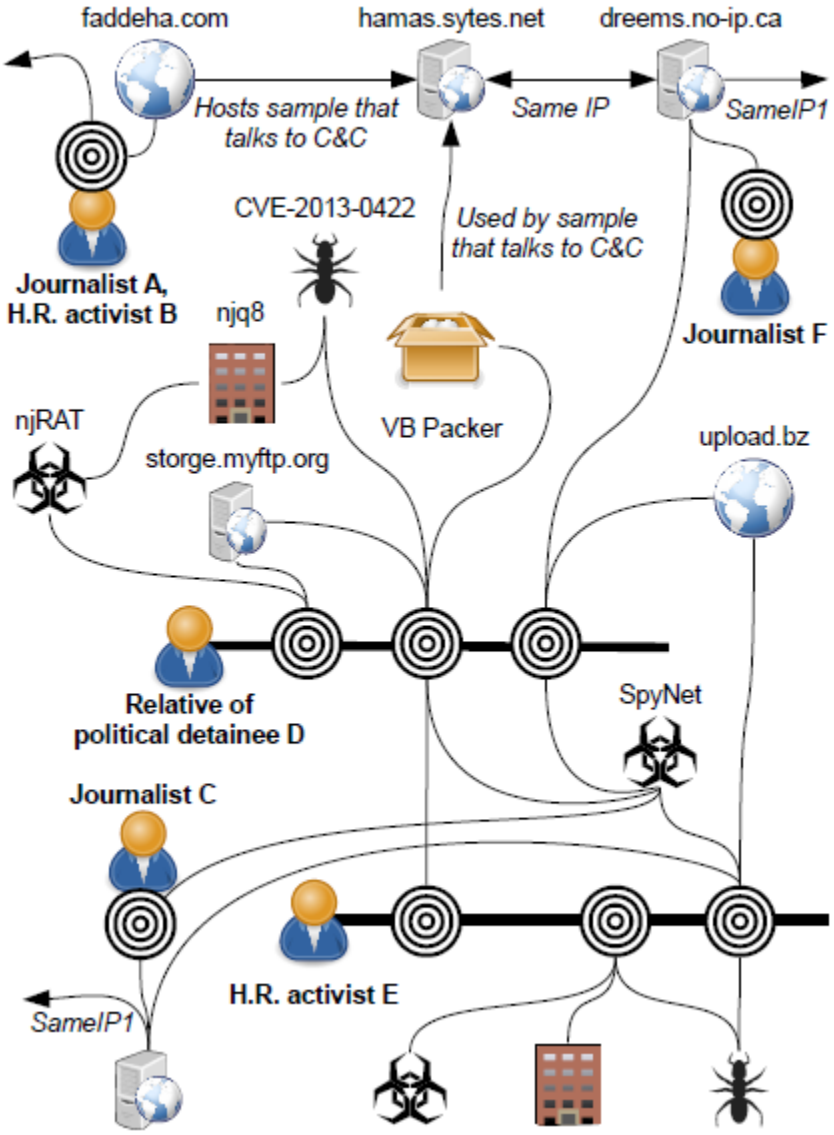
استغلال البيانات المجموعة: عندما استلم أحمد ملف نظام للتحكم عن بعدRCS ، فتحه وتضرر جهاز الكمبيوتر الخاص به (الرسم ٥) وبعد ذلك انتبه أحمد إلى الدخول المشبوه عدة مرات إلى حساب Gmail الخاص به عبر نظام الوصول لرسائل الإنترنت. واستمر هذا الدخول حتى بعد أن غير أحمد كلمة المرور. وعند التواصل مع أحمد على حسابه، اكتشف أحد كتاب هذا البحث أن المهاجم قد حمل تطبيق كلمة المرور الخاصة application specific password في حساب أحمد وهذا التطبيق هو عبارة عن كلمة سر ثانوية يبدو أن المهاجمين استخدموها للوصول إلى الحساب حتى عندما غير أحمد كلمة المرور الأساسية. وتوقف هذا الدخول المشبوه بعد حذف تطبيق كلمة المرور الخاصة.

بعد أسبوعين من التواصل مع أحمد، تلقى أحدنا (واضع الرسم ٥) بريدًا إلكترونيا مستهدفًا يحتوي على رابط ملف استضافة على ملفات جوجل وفيه إعلان عن نظام التحكم عن بعد الجاهز RAT ونظام اكستريم للتحكم عن بعد Xtreme RAT . تم إرسال البريد الإلكتروني من منطقة الإمارات العربية المتحدة الزمنية (كما في حال البلدان الأخرى) وكان يضم مصطلحات "هام جدًا" و "ويكيليكس"، تمامًا مثل البريد الإلكتروني الذي أرسل إلى أحمد.

استخدم نظام التحكم عن بعد المرسل إلى المؤلف owner.no-ip.biz لسيرفر القيادة والتحكم وهو أحد المجالات التي ذكرت في التقرير الذي نشره نورمان حول حملة الهجمات الإلكترونية التي دامت سنة على الأهداف الإسرائيلية والفلسطينية التي شنتها المجموعة والتي لم يستطع نورمان تحديدها [٥٧]. وبعد ثلاثة أشهر على استهداف المؤلف، تلقى أحمد بريدًا إلكترونيا يحمل مرفقًا مع برنامج اكستريم للتحكم عن بعد Xtreme RAT الذي تواصل مع سيرفر القيادة والتحكم نفسه (الرسم ٥) مقترحًا أن المهاجمين الذين أصابوا كمبيوتر أحمد بنظام التحكم عن بعد RAT جهزوا لائحة عناوين إلكترونية مثيرة للاهتمام لمجموعة أخرى من أجل استهداف أكبر.

النتائج المحتملة: يقول أحمد إنه تعرض بعد فترة وجيزة من استهدافه لاعتداء بدني مرتين على يد مهاجم استطاع أن يتعقب موقعه [٥٨]. ويذكر أحمد أيضًا أنه قد تمت سرقة سيارته واختفى مبلغ كبير من حسابه في المصرف وتمت مصادرة جواز سفره [٥٩]. ويظن أحمد أن هذه النتائج هي جزء من حملة تخويف الحكومة ضده، لكننا لم نستطع إيجاد روابط مباشرة بين هذه الحوادث والإصابة. (أرسلت برامج تجسس تباعًا إلى الآخرين الذين استخدموا محتوى طعم عن أحمد).

هجمات أخرى: في أكتوبر/تشرين الأول أرسل إلينا صحافي أ وناشط حقوقي ب إماراتيين (الرسم ٦) رسائل إلكترونية مشبوهة وصلتهم وكانت تحتوي على ملف وورد يعود إلى المرحلة الأولى ل 3-stage Exploit Kit (الرسم ٥). واحتوى الملف المرفق على ملف فلاش مضمن استغل الثغرة الموجودة في أدوب فلاش Adobe Flash 11.4 محملًا بكود القشرة لتنزيل المرحلة الثانية من Faddeha.com، إلا أننا لم نتمكن من الوصول إلى المرحلة الثانية أو التنزيلات الأخيرة لأن الموقع لم يكن متوفرًا أثناء فترة الاختبار. هذا وتظهر exploit kit على أنها مؤشر لتورط فريق القرصنة، فقد لحظنا في صفحة Faddeha.com في ذاكرة تخزين جوجل المؤقتة وجود jar. مع فئة البرنامج الصغير نفسه (WebEnhancer) كتلك التي وجدت في ملفات jar. التي اكتشفنا أنها تحتوي على برنامج للتحكم عن بعد.



الرسم ٦: جزء آخر من النظام البيئي لحملات مراقبة هجمات الإمارات العربية المتحدة.

برامج التحكم عن بعد الجاهزة RATs: وجدنا ملفًا حمله فيروس توتال VirusTotalمن Faddeha.com الذي هو من أدوات الوصول البعيد المعروف ك SpyNet يمكن للجميع الحصول عليه بمبلغ ٥٠ يورو [٦٠]. ويتواصل نموذج |SpyNet مع قيادة وتحكم hamas.sytes.net.

تخزين برنامج SpyNet : وجدنا مثالًا آخر عن المرحلة الأولى من 3-Stage Exploit Kit على فيروس توتال. وقد حملت الثغرة المرحلة الثانية التي بدورها حملت نموذج SpyNet من maile-s.com. تواصل هذا النموذج مع سيرفر القيادة والتحكم نفسه hamas.sytes.net وخزن باستخدام ASProtect[٦١]. عندما يشغل هذا النموذج يقوم بفك ضغط بيانات مشروع تحويل برمجي مترجم بطريقةRunPE [٦٢]، وهو ملف تنفيذي يخزن مع UPX [٦٣]. وأخيرًا يفك هذا التنفيذ ضغط بيانات SpyNet. تقدم واجهات المستخدم الرسومية خيار واحد فقط للتخزين مع UPX مقترحين أن المهاجمين أضافوا طبقات التخزين الاخرى. في بعض الحالات يحمل مشروع التحويل البرمجي اسم NoWayTech الذي يبدو أنه أداة RunPE سرية، بينما تسمى المشاريع الأخرى SpyVisual والتي لم نتمكن من إيجاد صلة بينها وبين أي أداة سرية عامة. وعليه، قد يعكس الأمر تخصيصًا من قبل المهاجم. تحتوي مشاريع SpyVisual على السلسلة c:\Users\Zain\AppData\Local\Temp\OLE1EmbedStrm.wav التي تستخدم كبصمة VB Packer في الرسم ٦.

هجوم Cedar Key: استخدم ال VB Packer نفسه في الهجوم على المعتقل السياسي د والناشط الحقوقي ه في الرسم ٦ حيث تلقى هذان الشخصان رسائل إلكترونية فيها رابط لصفحة ويب على cedarkeyrv.com متخفية باسم يو تيوب وبمجرد فتح الهدف الرابط، ظهرت صفحة عبارة "Video loading please wait..." "تحميل الفيديو، الرجاء انتظر..." وأعيد توجيه الصفحة إلى يوتيوب بعد عدة ثوان وذلك بعد أن نزلت ثغرة جافا [٦٤]- عدم حصانة معروفة من دون رقعة patch حول وقت إرسال الرسائل الإلكترونية. أطلقت شركة أوراكل رقعة patch بعد ١٢ الساعة من بدء الناشطين بتلقي هذه الروابط.

إن مجال cedarkeyrv.com مرتبط ب RV park في Cedar Key. هذا وأطلعتنا شركة استضافة الموقع أن الأخير قد اختبر تسويةً وأن الشركة لا تمتلك تفاصيل اضافية حول الموضوع.

يبدو أن الثغرة التي استخدمت في الهجوم قد نشرت من قبل مستخدم كويتي njq8 على موقع تبادل ثغرات عربي اللغة [٦٥]. تواصلنا مع المستخدم njq8 الذي أخبرنا أنه قد حصل على الثغرة من موقع عام وأنه قد

عدلها قبل نشرها. حمّل الهجوم فيروس SpyNet من isteeler.com (الذي أظهر فحصنا له أنه لا يحتوي على محتوى مشروع) الذي استخدم قيادة وتحكم Storge.myftp.org. واستخدم سيرفر القيادة والتحكم نفسه في هجوم آخر (الرسم ٦) استهدف قريبًا للمعتقل السياسي د، في هذه الحالة كان انتقال الفيروس عبر برنامج للتحكم عن بعد RAT متاحًا مجانًا ومعروف بنجرات (njRAT) مكتوبة من قبل المستخدم نفسهnjq8 كملصق الثغرات التي تم شرحها أعلاه. غير أننا لم نجد أي دليل اضافي يثبت تورط المستخدم njq8 في كلتي الهجمتين.

هجماتSpyNet أخرى: إن مجال hamas.sytes.net الذي سبق أن رأينا استخدامه عبر نموذجي SpyNet حلل ونسب إلى67.205.79.177 وقد سبق أن نسب dreems.no-ip.ca إلى هذا العنوان أيضًا. واستخدم كذلك فيروس غير معرف سيرفر القيادة والتحكم هذا لاستهداف الصحافي وهو السيرفر نفسه الذي استخدم في الهجوم على قريب المعتقل السياسي د. في الحالة الأخيرة، وصل النموذج عبر بريد إلكتروني في مرفق rar. التي احتوت على ملف وورد متخفٍ scr. ملف ال scr. كان أرشيفًا مستخرجًا ذاتيًا فك الضغط وشغّل الملف الطعم والفيروس.وكان مصدر بروتوكول إرسال البريد البسيط .webmail.upload.bz

أبين Appin: في أوائل العام ٢٠١٣، حول الناشط الحقوقي ه عدة ملفات تضمنت ثغرة معينة CVE-2010-0158 لمايكروسفت وورد. واحتوى مجموع هذه الملفات على ١٧ تشفير مميز hashes وعشرة تشفيرات مميزة لفيروساتhashes of payloads (بعض الملفات التي اختلفت في تهشيرها حملت الفيروس نفسه). وقد حملت الثغرات أولًا فيروسات SpyNet من upload.bz والتي تواصلت بأغلب قسمها مع سيرفر القيادة والتحكم على sn.all-google.com والذي بدوره استخدم سيرفر القيادة والتحكم في هجمات أخرى بما فيها الهجوم على الصحافي ج.

فضلًا عن ذلك، حملت ثغرتان من ثغرات CVE-2012-0158 دارك كوميت DarkComet من موقعي www.getmedia.us و www.technopenta.com بعد نشر نظام معلومات على random123.site11.com. توافقت المواقع الثلاث هذه مع تلك التي استخدمت من قبل مجموعة مرتزقة هندية يقال إنها مرتبطة بمجموعة أمن آبين[٦٦]. استضاف المجالان السابقان محتوى غير برامج التجسس (قد يكونوا أقاموا تسويةً). غيرنا مالكwww.getmedia.us الذي أزال الفيروسات.

٥. الوصف التجريبي

أتاحت لنا النماذج التي حصلنا عليها الفرصة لنمثل تجريبيًا استخدام برنامج FinFisher وفريق القرصنة حول العالم ممكنة إيانا من تقييم انتشارها وتعريف حالات الدول الأخرى التي تأذن لنا بالتحقيق في المستقبل. حللنا النماذج وسلوك سيرفرات القيادة والتحكمC&C لنتوصل إلى مؤشرات (بصمات إلكترونية fingerprints)) ليكيفية استجابة السيرفرات لبعض أنماط الطلبات، ومسحنا بعدها مساحة مسافة الإصدار الرابع من بروتوكول الإنترنت IPv4 كلها ("٠/") مع نتائج الفحص التي حصلنا عليها من المسح الأخير.وفي الكثير من الحالات لم نعطِ تفاصيل كاملة عن بصماتنا وذلك تجنبًا لتسوية ما قد تكون تحقيقات مشروعة.

FinSpy ٥،١

تحليل السيرفرات والربط بينها: توصلنا إلى عدد من البصمات الإلكترونية fingerprints لتحديد سيرفرات FinSpy باستخدام ميثاق نقل النص الفائق المرتكز على الفحص ومخصص FinSpy ذات البروتوكول المبني على TLV. واستغلينا ميزات مثل عدم التوافق المحدد مع طلب تعليقات ٢٦١٦ واستجابات لأنواع معينة من البيانات غير الصالحة ووجود تأشيرات مثل "Hallo Steffi" غير المألوفة التي حددها غوارنيري Guarnieri من سيرفرات القيادة والتحكم الخاصة ببرنامج FinSpy في البحرين [٦٧ و٦٨]. راجع الفهرس أ من اجل التفاصيل. وبعد ذلك مسحنا بشكل عام الإنترنت باحثين عن بصمات إلكترونية مشابهة.

وتعلن توثيقات غاما Gamma أنه يمكن لمشغل FinSpy جعل مكان وجود سيرفر القيادة والتحكم غامضًا (يسمى الرئيسي "ذا ماستر"the master)) عبر بناء بوابة وسيطة proxy يعرف ببديل relay . ولاحظنا في ربيع ٢٠١٢ أن سيرفرات FinSpy تصدر الآن 302 Redirects إلى google.com. إلا أننا لمسنا عيوبًا: على سبيل المثال، كانت الخوادم في الهند تعيد التوجيه إلى إصدار لاتيفي latvian لجوجل google.lv. نحن نتوقع أن يكون السيرفر في الهند بديلًا للتحويل للرئيسي master الموجود في لاتفيا latvia ولأن الأخير ;كان قد شكل بوابة فرعية لجوجل استطعنا أن نكشف بروتوكول الإنترنت الخاص به باستخدام ميزات جوجل التي تطبع عنوان بروتوكول إنترنت المستخدم بناء على طلب "عنوان بروتوكول الإنترنت" "IP address". بالإضافة إلى ذلك، أوجدنا بصمة إلكترونية إضافية مرتكزة على سلوك المخدم

الفرعي وأصدرت طلبات GET/search?q=ip+address&nord+1 إلى السيرفرات، فلاحظنا بعض المواقع الرئيسية المثيرة للإهتمام في الجدول ٤.

مواقع السيرفرات: توافقت بصماتنا الإلكترونية fingerprints بالإجمال مع ٩٢ عنوان بوتوكول إنترنت IP مميز في ٣٥ بلدًا مختلفًا وبعد أن حللناها في ٢٠١٣/٨/٨ ظهر في النتيجة أن ٢٢ عنوانًا مميزًا ما زالوا يستجيبون: البحرين وبنغلادش والبوسنة والهرسك واستونيا وأثيوبيا وألمانيا وهونغ كونغ واندونيسيا ومقدونيا والمكسيك ورومانيا وصربيا وتركمانستان والولايات المتحدة. ووجدنا خوادم تستجيب لعدد من بصماتنا مقترحين تباطؤ بعص السيرفرات في تحديثاتها أو جهودًا متضافرة لتغيير سلوك سيرفرات FinSpy لجعل اكتشافها أصعب.

وجدنا: (١) ثلاثة عناوين نطاقات بروتوكول إنترنت IP مسجلة في غاما. (٢) سيرفرات في ثلاثة عناوين نطاقات بروتوكول إنترنت IP مسجلة علنًا لوكالات حكومية: وزارة اتصالات تركمانستان ومكتب الشؤون الأمنية في قطر ومجلس الوزراء البلغاري. (٣) ثلاثة عناوين بروتوكول إنترنت IP إضافية في البحرين جميعها في بتلكو. (٤) خوادم في ٧ بلادان مع حكومات صنفتها مجلة ذا إيكونومست "كأنظمة استبدادية"[٦٩]: البحرين وأثيوبيا ونيجيريا وقطر وتركمانستان والإمارات العربية المتحدة وفيتنام.

نماذج FinSpy اضافية: بالتوازي مع مسحنا، حصلنا على تسعة نماذج من FinSpy عبر كتابة قواعد YARA[٧٠] لميزة "صيد البرامج الخبيثة" لاستخبارات فيروس توتال. ترسل إلينا هذه الميزة كل النماذج الجديدة المقدمة التي تتوافق مع بصماتن الإلكترونية. حددنا موقع إصدار ل FinSpy لا يستخدم اقامة اتصال FinSpy العادي إنما يستخدم بدلاً منه بروتوكولًا مبنيًا على طلبات HTTP POST للتواصل مع سيرفر القيادة والتحكم. لم يظهر ما إن كان هذا إصدارًا أقدم ل لبروتوكول أو أجدد مقترح أن نتائج مسحنا قد لا تعكس النطاق الكامل لخوادم تحكم وقيادة FinSpy. وربما تم إرسال بروتوكولHTTP POST إلى عميل غاما محدد لتلبية مطلب.

بروتوكول الإنترنت البديل	Block Assignment البديل	البلد البديل	بروتوكول الإنترنت الرئيسي	Block Assignment الرئيسي	البلد الرئيسي
5.199.xxx.xxx	SynWebHost	ليتوانيا	188.219.xxx.xxx	فودافون	إيطاليا
46.26.xxx.xxx	UK2VPS.net	المملكة المتحدة	78.10.xxx.xxx	مبنى أمن الدولة	قطر

119.18.xxx.xxx	HostGator	الهند	81.198.xxx.xxx	Statoil DSL	لاتفيا
180.235.xxx.xxx	Asia Web Services	هونغ كونغ	80.95.xxx.xxx	أنظمة تقنية المعلومات	الجمهورية التشيكية
182.54.xxx.xxx	GPLHost	أستراليا	180.250.xxx.xxx	شركة اتصالات PT	اندونيسيا
206.190.xxx.xxx	WestHost	الولايات المتحدة الأمريكية	112.78.xxx.xxx	Biznet ISP	اندونيسيا
206.190.xxx.xxx	Softlayer	الولايات المتحدة الأمريكية	197.156.xxx.xxx	شركة اتصالات اثيوبيا	أثيوبيا
209.59.xxx.xxx	Endurance International	الولايات المتحدة الأمريكية	59.167.xxx.xxx	Internode	أستراليا
209.59.xxx.xxx	Endurance International	الولايات المتحدة الأمريكية	212.166.xxx.xxx	فودافون	اسبانيا

الجدول ٤: تقطيع مخدمات FinSpyالفرعية (اقتران نماذج عنواين خوادم القيادة والتحكم الأولية إلى تلك الرئيسية التي يرسلون إليها)

٥,٢ نظام التحكم عن بعد RCS: بدأنا بتحليل نموذج التحكم عن بعد الخاص بالإمارات العربية المتحدة UAE RCSمن أحمد وحصلنا على ستة نماذج من فيروس توتال VirusTotalعبر البحث عن نتائج AV التي تحتوي على سلسلتي "دا فينشي" DaVinci"و"نظام التحكم عن بعد"RCS.". في ذلك الوقت، أضاف عدد كبير من بائعي AV نظامًا يكتشف نظام التحكم عن بعد RCS وفقًا لنموذج حلله د.ويب Dr. Web [٧١] و نموذج التحكم عن بعد التابع للإمارات العربية المتحدة المرسل من أحمد. وكذلك حصلنا على FSBSpy وحللناه [٧٢]، وهو برنامج خبيث يمكنه إرسال نظام معلومات وتحميل لقطات الشاشة وسحب برمجيات خبيثة أخرى وبرمجتها. ابتكرنا بناء على هذه النماذج تأشيرة YARA التي ولدت ٢٣ نموذجًا اضافيًا من البرمجيات الخبيثة المشابهة تركيبيًا.

البصمات الإلكترونية fingerprints: حللنا سيرفرات القيادة والتحكم الخاصة بنظام التحكم عن بعد ونماذج FSBSap ووجدنا أنها استجابت بطريقة مميزة لطلبات ميثاق نقل النص الفائق وأعادت شهادات SSL مميزة.

وبحثنا في نماذج بما فيها Shodan وتحاليل Internet Census services 5 [٧٣] وCritical. مسح البيانات الداخلة [٦٨] عن سلوك HTTP المميز الذي رصدناه. بحثنا كذلك عن مسوحات شهادات SSL في تحاليل Internet Census Services 2 من ZMap [٧٤] وتواصلنا مع فريق TU ميونيخ [٧٥] الذي طبق بصماتنا الإلكترونية fingerprints على بيانات مسح SSL التابع لهم. حصلنا على ٣١٣٤٥ مؤشر نقرات من جميع هذه الموارد تعكس ٥٥٥ عنوان بروتوكول إنترنت IP في ٤٨ بلدًا.

عادت شهادة SSL بنتيجة ١٧٥ سيرفرًا صادرة من "/CN=RCS Certification Authority/ O=HT srl" تشير على ما يبدو إلى اسم برنامج التجسس والشركة.(بما فيها سيرفرات ل ٥ من نماذجنا FSBSpy واثنين من نماذج نظام التحكم عن بعد RCS الخاصة بنا) استجابت لهذا النوع من الشهادة.

أعادت بعض هذه السيرفرات هذه الشهادات في سلاسل تضمنت شهادات مميزة أخرى ووجدنا أن ١٧٥ عنوان بروتوكول إنترنت مميز (بما فيها خادم القيادة والتحكم ل٥ من نماذج FSBSpy التابعة لنا واثنين من نماذج نظام التحكم عن بعد) استجابوا بهذا النوع الثاني من الشهادة.

ابتكرنا مؤشرين آخرين: الأول توافق مع ١٢٥ عنوان بروتوكول إنترنت IP ويتضمن ٧ نماذج FSBSpy وسيرفر التحكم والقيادة والثاني توافق مع عنوانين بريد الكتروني في ايطاليا وكازخستان.

مواقع الخوادم: حللنا في ١٣/٤/١١ جميع عنوانين بروتوكول الإنترنت التي جمعناها ووجدنا ١٦٦ عنوان ناشط يتوافق مع بصماتنا في ٢٩ بلدًا مختلفًا. نلخص أبرز المزودات والبلدان في الجدول ٥.

البلد	بروتوكول الإنترنت
الولايات المتحدة	٦١
المملكة المتحدة	١٨
ايطاليا	١٦
اليابان	١٠

المغرب	٧

الجدول ٥: أبرز البلدان والمزودين المستضيفين لسيرفرات نظام التحكم عن بعد النشطة في ١٣/٤/١١

المزود	بروتوكول الإنترنت
Linode	٤٢
NOC4Hosts	١٦
Telecom Italia	٩
Maroc Telecom	٧
InfoLink	٦

تنتشر السيرفرات النشطة إما في الولايات المتحدة الأمريكية أو تستضاف من قبل Linode[٨] ويبدو أنها تشير إلى استخدام نافذ لموقع خارج البلاد وخدمات VPS.

فضلًا عن ذلك وجدنا: (١) ثلاثة عناوين بروتوكول إنترنت على أ/٢٨ يسمى HT Public Subnet مسجلًا في CFO لفريق القرصنة [٧٦]. ويحلل نطاق hackinhteam.it إلى عنوان في هذا المعدل. (٢) عنوان يعود إلى عمانتل وهي شركة اتصالات في عمان تملك الدولة معظمها، وتمكنا من الوصول إلى العنوان عندما قمنا بتحليله؛ أرشدنا باحث إلى نموذج FSBSpy يحتوي على ملف طعم باللغة العربية حول شاعر عماني، إلا أن هذا الملف تواصل مع سيرفر القيادة والتحكم في المملكة المتحدة. (٣) سبعة عناوين بروتوكول إنترنت تعود إلى اتصالات المغرب وتم استهداف صحافي مغربي على Mamfakinch.com عبر نظام تحكم عن بعد في العام ٢٠١٢[٧٧]. (٤) الخوادم التي وجدت في ثماني بلدان كانت تعود إلى حكومات ذات أنظمة استبدادية [٦٩]: أذربيجان وكازخستان ونيجيريا وعمان والسعودية والسودان والامارات العربية المتحدة وأوزبكستان.

إيجاد رابط بينها وبين فريق القرصنة: استجابت جميع السيرفرات النشطة التي توافقت مع إحدى تأشيراتنا بطريقة غريبة عندما استخدمت معطلبات HTTP سيئة التشكيل، وكانت الاستجابة HTTP1/1 400 Bad Request (بدلًا من أن تكون HTTP/1.1 ومن Detected error: HTTP code 400. عند البحث عن هذه الاستجابة، كانت النتيجة مشروع GitHub em-http-server [٧٨] وهو خادم ويب مبني على Ruby وورد اسم البيرتو اورناغي كمؤسس لهذا الويب؛ ألبيرتو هو مهندس برامج في فريق القرصنة. نتوقع أن يتضمن سيرفر قيادة وتحكم فريق القرصنة رمزًا من هذا المشروع.

[٨] تستضيف الولايات المتحدة الامريكية ١٩ خادم Linode من أصل ٤٢ لذلك فإن أنماط الانتشار ممبزة

العلاقة بين السيرفرات: كشفنا عدة حالات حيث تمت استضافة السيرفر من قبل مزودين مختلفين وفي بلدان مختلفة وأعادوا شهادات SSL مماثلة ومطابقة لبصماتنا. وكذلك شاهدنا ٣٠ سيرفرًا نشطًا استخدموا IPID عالمي، إلا أن خادمًا واحدًا فقط لم يمتلك IPID عالميًا ولا شهادة SSL مطابقة لبصماتنا الإلكترونية fingerprints. وقيّمنا ما إن كانت السيرفرات التي تعيد شهادات SSL تعيد الإرسال إلى سيرفرات مع IPIDs عالمية عبر اندفاع حركة مرور للسابق ومراقبة IPID اللاحق. وجدنا أن ل١١ سيرفر نشاط متعلق باتصالات ترسل إلى سيرفرات أخرى وقسمناها وفقًا لشهادات SSL التي أعادوها ووجدنا أن كل مجموعة أعادت الإرسال إلى سيرفر واحد فقط باستثناء حالة واحدة حيث أرسلت المجموعة إلى بروتوكولي إنترنت مختلفين (كلاهما في المغرب). وكذلك وجدنا مجموعتين أرسلتا إلى العنوان نفسه. كان هناك تخطيط ١:١ بين العناوين الثمانية الباقية والمجموعات. كشفنا هنا مجموعة سيرفرات قد تكون مرتبطة بالضحايا أو المشغلات في بلد معين، ويمهد بعض هذه الاكتشافات لتحقيقات أخرى محتملة:

تركيا: حددنا مجموعة تتضمن ٢٠ سيرفرًا في ٩ مناطق. نظامين تحكم عن بعد و ٥ نماذج FSBSpy من فيروس توتال تواصلت مع عدة خوادم في المجموعة. وتواصلت نماذج التحكم عن بعد مع نطاقات ذات تسجيلات منقضية، لذا سجلناها لمراقبة المستخدمين الواردين. تلقينا حصريًا دخول نظام تحكم عن بعد من عناوين بروتوكول تركية. (يمكن تحديد دخول نظام التحكم عن بعد استنادًا إلى عميل مستخدم مميز و URLفي طلبات POST). يبدو أن نموذج FSBSpy قد ثبت ثغرة على سيرفر تركي تواصل مع أحد السيرفرات في هذه المجموعة. [٧٩]

بالإضافة إلى ذلك وجدنا مجموعة سيرفرات تحتوي على سيرفرات في أوزبكستان وكازاخستان ووجدنا كذلك نماذج FSBSpy في فيروس توتال حمل من هذه البلدان التي تواصلت مع خوادم في هذه المجموعات.

في الحالات أعلاه، صنفنا تركيا بين الدول ذات النظام الاستبدادي والتي من المحتمل أن تكون استخدمت منتوجات فريق القرصنة ضد أنواع الأهداف التي ذكرناها في هذا البحث. تظهر إشارات في حالة تركيا على توجيه الأداة ضد المعارضين.

٦. خلاصة

إن المراقبة المستهدفة للأفراد التي أجرتها الدول القومية تطرح مشكلة أمنية صعبة استثنائية وهي عدم توازن الموارد والخبرة بين الضحايا والمهاجمين. لقد قمنا برسم طبيعة نطاق المشكلة كما نقلها إلينا الافراد المستهدفون في ثلاث دول في الشرق الاوسط. تتضمن الهجمة برنامج تجسس للمراقبة المستمرة واستخدام روابط "جاسوس بروتوكول الإنترنت" لتعريف المعارضين.

ومع أن الهجمات تتضمن في بعض الأحيان هندسة اجتماعية فعالة، فهي تفتقر بشكل عام إلى عناصر تقنية جديدة لأنها وظفت بدلًا من ذلك أدوات سابقة التحضير طورها الباعة أو حصلوا عليها من أسرار الجريمة السيبرانية. تعاني هذه التكنولوجيا أحيانًا من مشاكل رديئة تواجهنا (أخطاء خطيرة في تنفيذ التشفير ورسائل بروتوكول معطوبة) كما يوظفها المهاجمون (تحديد المعلومات المتضمنة في الثنائيات وخوادم القيادة والتحكم التي يمكن اكتشافها عبر المسح أو "قرصنة جوجل" وتجمع الحسابات المرتبطة عبر نشاط مشترك). ساهمت بعض هذه الأخطاء في الجهود التي نبذلها لجمع الأدلة التفصيلية ذات المصادر الحكومية. فضلًا عن ذلك، قمنا بوضع خريطة الاستخدام العالمي لمجموعتي قرصنة دولية تضمنت تحديد ١١ حالة مستخدمة في دول ذات "أنظمة استبدادية".

نهدف من خلال هذا العمل أن نشكل مصدر إلهام لزيادة الجهود لاجراء بحوث تحاكي المشكلة الصعبة لكيفية حماية الأفراد بطريقة مناسبة في ظل وجود موارد محدودة في وجه خصوم أقوياء. تتضمن الأسئلة المفتوحة كشفًا عمليًا قويًا للهجمات المستهدفة التي صممت لاختراق بيانات حاسوب الضحية واكتشاف توجهات المهاجم الجديدة ومقاومتها مثل العبث باتصالات النترنت لادخال برمجيات خبيثة.

تفرض هذه المهمة تحديًا كبيرًا إلا أن مناصريها المحتملين كثر أيضًا. رجَّح عضو معارض، حول قرصنة الدولة في ليبيا سبب تشغيل بعض الستخدمين للملفات حتى بعد معرفتهم أنها خبيثة[٢]: "لم نكن لنهتم حتى لو كنا أكثر عرضةً كنا نحاول جاهدًا أن نطلق أصواتنا، كانت مسألة حياة أو موت، وكان من الضروري أن تخرج هذه المعلومات إلى العلن".

شكر

دعمت مؤسسة العمل الوطنية هذا العمل من خلال الهبات ١٢٢٣٧١٤٧ و١٢٣٧٢٦٥ وعضوية سيتيزن لاب. إن أي آراء ونتائج وخلاصات وتوصيات معروضة في هذه المادة تمثل الكاتبين ولا تعكس بالضرورة وجهات نظر المتبنين.

يود الكاتب أن يشكر هؤلاء الافراد لمساعدتهم في مختلف جوانب تحليلنا: برنارد عمان وكولين د. أندرسون وبراندون ديكسون وذاكر دورومیریك و إيفا جالبيرين وكلاوديو غوارنييري ودرو هنتز ورالف هولز وشين هنتلي وأندرو ليونز ومارك شلوسر ونيكولاس ويفر.

ملحق: بصمات FinSpy

بعد إجرائه لأبحاث سابقة وجد غوارنييري بعد مسح سيرفرات FinSpy أن الاستجابة لطلب مثل /GET يعيد سيرفر القيادة والتحكم البحريني استجابة بسلسلةHallo Steffi [٦٧]. بحث غوارنييري في قاعدة بيانات لمثل هذه الاستجابات التي تصنف ثم تجمع بواسطة Critical مشروع مسح إنترنت IO [٦٨] محددًا موقع ١١ سيرفرًا إضافيًا في ١٠ بلدان [٦٧]. نشير إلى البصمة بـ α1، وبالتزامن مع هذه الجهود ابتكرنا بصمتنا الخاصة β1 التي فحصت ثلاثة جوانب من الاتصال بين متضرر من FinSpy وسيرفر قيادة وتحكم FinSpy الذي يتبع مخصص بروتوكول مبني على TLV ويعمل على منفذات مثل ٢٢ و٥٣ و٨٠ و٤٤٣. أجرينا مسحًا مستهدفًا لعدة بلدان باستخدام β1 وأكدنا نتائج غوارنييري التي وجدت أن الوصول ممكن إلى هذه السيرفرات بعد أن نشرها.

لاحظنا مسار: تغيرات في استجابة HTTP عبر FinFisher بعد نشر النتائج عن البرامج. في يوليو/تموز ٢٠١٢، على سبيل المثال، بعد منشور عن نماذج FinSpy بحرينية [٨١] أغلقت السيرفرات اتصال TPC استجابة لطلب /GET أو /HEAD (على الرغم من أن السيرفرات تابعت التصرف بالتوافق مع β1. تبعت تغيرات أخرى في العام ٢٠١٢ تضمنت استجابة جديدة لطلبات /GET التي تضمنت نسخة فاسدة عن استجابة سيرفر Apache HTTP (استخدمت ترويسة التاريخ UTC بدلًا من GMT). وثقنا هذا الخطأ كـ α٢ ووثقنا بعدها تصرفًا مميزًا في العام ٢٠١٢ استجابة ل /GET الطلبات كـ α 3 .

حددت مسوحات /٠ اللاحقة ل α 2 وα 3 خمس تحقيقات في Internet Census لـ α 2 من خلال α 3، مواقع عدد من السيرفرات الإضافية. وفي فبراير/ شباط عام ٢٠١٣، عرفنا استجابة HTTP جديدة ووثقناها مع α 4 وعدلنا β1 لننتج β٢ التي تختبر فقط اثنين من مظاهر اتصالات FinSpy (لقد تم تعطيل الاختبار الثالث لـ β1 بعد أن تم تعديل سيرفرات FinSpy لتقبل أنواع البيانات غير الموجودة لديها والتي تم رفضها سابقًا).

ابتداءً من ١٣/١٣/٣ تطابقت جميع سيرفرات α1 مع بصمات β٢.

* قدّمت الورقة البحثية في مؤتمر USENIX Security في ٢٢ أغسطس/آب ٢٠١٤

* الترجمة الكاملة في ملف PDF

* رابط الورقة البحثية باللغة الإنجليزية:

http://www.icir.org/vern/papers/govhack.usesec14.pdf