

سید الذباب:

تحقیق مفتوح حول
سعود القحطاني

bellingcat

مقدمة.....	1
I - النتائج الرئيسية.....	2
II..... من شاعر إلى منفذ للأوامر	3
III..... تسريب معلومات الاتصال التي يملكها القحطاني	6
حساب القحطاني على تويتر متصل بالبريد الإلكتروني saudq@saud.com ورقم هاتف محمول	6
البريد الإلكتروني للديوان الملكي المستخدم لتوفير رقم الهاتف والبريد الإلكتروني للقحطاني	7
تم ربط جيميل بنفس رقم هاتف القحطاني وبريده الإلكتروني الموجودان على تويتر	8
IV..... النشاط على هاك فورمز	12
خُدع في اليوم الأول.....	13
الراتس (RATs) وشبكات البوت (Botnets) وهجمات حجب الخدمة (DDoS)	14
استهداف استخدام الرات في عملية دولية لإنفاذ القانون	15
حاول توظيف مختص بهجمات حجب الخدمة لإدارة شبكة البوتات	16
استهدف المستخدمين على أحد منصات وسائل الإعلام الاجتماعية الرئيسية، خدمة واتس آب	18
دفع للحصول على قناة يوتيوب، وحذف أكثر من 20 فيديو	18
بحث عن أداة لحظر حساب تويتر	19
امتلك "العديد من حسابات فيسبوك"	20
اختبر أداة لاختراق واتس آب	20
أراد إخراج لاعبين من لعبة على فيسبوك، واشترى عملات للعبة بلياردو	20
نشر آراءه عن الله وأوباما وكشمير	20
نشر بينما كان ثملاً	21
استخدم باي بال، وقدم عنوان بريد على هوتميل	22
دفع 1500 دولار لإختراق حسابات هوتميل	23
حاول اختراق الشبكات اللاسلكية، نشر أول برنامج نصي	23
سعى للحصول على برمجيات تجسس على iOS	24
حاول شراء حركة زائفة لموقع لمتابعي تويتر	25
سعى للحصول على مخدم مخصص في روسيا أو الصين لاستضافة أعمال الاختراق وشبكة البوتات	25
V..... النطاقات	26
سجل أول 13 نطاقاً مع جيميل ورقم الهاتف الخليوي	27
أدرج الاسم الحقيقي في سجلات Whois	29
استعمل nokia2mon2 كنطاق فرعي لمخدم C2	30
نطاقين فعالين متصلين بخدمة بريد إلكتروني مشفر	33
استخدم نطاق Saudq كمخدم برمجيات خبيثة C2	35
سجلات الرسائل النصية المستضافة على نطاقات فرعية مؤرشفة	35

تطبيق بواسطة SaudQ متوفر للتنزيل	37
نطاقان فرعيان استخدمتا لتويتر	38
نطاق فرعي تجريبي مستخدم في إدارة الترجمة	39
النطاق الفرعي تابيتا متضمن في تحليل تويتر للبريد المزعج	39
انتهت صلاحية النطاق مؤخراً	40
VI. حسابات أخرى	41
"باحثٌ عن العقول الفذة" (headhunter) على لينكدان	41
شخصية مؤيدة لمبارك على فيسبوك	41
رقم الهاتف المحمول متصل بسناب شات، واتس آب، وسيجنال	42
استخدم اسم Nokia2mon2 على عدة منتديات	42
VII. الخلاصة	44

مقدمة

قبل قيام سعود القحطاني، المستشار الرفيع المستوى لولي العهد السعودي محمد بن سلمان، بالاتصال عبر سكايب¹ ليشرّف على قتل الصحفي السعودي جمال الخاشقجي وتقطيع أوصاله، عرف القحطاني بإدارته لحسابات وسائل الإعلام الاجتماعي للبلاط الملكي وبلعبه دور المشرف الأول والمنفذ للأليات الدعائية حول محمد بن سلمان. وشملت مهامه أيضاً القرصنة ورصد منتقدي المملكة ومحمد بن سلمان.

في عام 2012 ومرة أخرى في عام 2015، قام شخصٌ عرّف عن نفسه على أنه القحطاني بمحاولة شراء أدوات للمراقبة من² بائعي البرمجيات الخبيثة الإيطاليين المثيرين للجدل هاكنغ تيم (Hacking Team). في 5 تموز/ يوليو 2015 كُشفت هذه المراسلات دون قصد من قبل قرصان يستخدم اسم (Phineas Phisher)، والذي قام بسرقة و نشر ما يقارب 400 غيغابايت من الوثائق الداخلية ورموز الكود المصدرية ورسائل البريد الإلكتروني لهاكنغ تيم.³

ولكن يبدو أن اتصال القحطاني ببائعي البرمجيات الخبيثة لم يلاحظ لسنوات، حتى 29 آب/ أغسطس 2017، عندما تم إنشاء حساب تويتر باللغة العربية وبدأ بنشر مقتطفات من رسائل القحطاني الإلكترونية لهاكنغ تيم.⁴

كما ربط حساب تويتر، الذي استخدم اسم المستخدم @HIAHY وعبارة (تاريخ وذكريات)، عناوين البريد الإلكتروني التي استخدمها القحطاني بعدة حسابات على الإنترنت. حيث أشار حساب تويتر⁵ إلى أن عنوان البريد الإلكتروني المستخدم من قبل الشخص الذي يبدو بأنه القحطاني للتواصل مع هاكنغ تيم - saudq1978@gmail.com - تم استخدامه أيضاً لتسجيل حساب باسم nokia2mon2 على موقع القرصنة المعروف هاك فورمز (Hack Forums)، والذي تعرض بحد ذاته للاختراق في حزيران/ يونيو 2011 من قبل مجموعة النشطاء من القرصنة (LulzSec).⁶

وكشفت تقرير إضافي من مذرورد (Motherboard) في آب/ أغسطس 2018 بأن الرسائل المسربة من هاكنغ تيم تضمنت عناوين إضافيين للبريد الإلكتروني استخدمهما الشخص الذي يزعم بأنه القحطاني: s.qahtani@royalcourt.gov.sa و saudq@saudq.com.⁷

لم يستطيع أي من حساب تويتر @HIAHY ولا مذرورد أن يثبت بشكل قاطع بأن القحطاني هو مالك عناوين البريد الإلكتروني المسربة، على الرغم من أن كليهما يقدمان أدلة ظرفية مقنعة بأن القحطاني هو في الواقع وراء رسائل البريد الإلكتروني إلى هاكنغ تيم وبأنه كان صاحب حساب nokia2mon2 على هاك فورمز.

يتوسع هذا التقرير في جهود البحث والتقارير من قبل @HIAHY ومذرورد ويضعها في سبعة أقسام. أولاً، يوجز النتائج الرئيسية للتقرير. ثانياً، يرسم سيرة ذاتية قصيرة لصعود القحطاني إلى السلطة وموجز تورطه في قتل الخاشقجي. ثالثاً، يظهر أن القحطاني يمتلك عناوين البريد الإلكتروني الواردة في ما تم كشفه من هاكنغ تيم بالإضافة إلى رقم هاتف نقال لم يبلغ عنه من قبل — +9750 548 55 966 — والذي يظهر أيضاً في الرسائل المسربة من هاكنغ تيم. رابعاً، يتفحص نشاط القحطاني في هاك فورمز بالتفصيل. خامساً، يحدد ويحلل شبكة بنية تحتية على الإنترنت لم يسبق الكشف عنها استخدمها القحطاني لأغراض خبيثة. سادساً، يستخدم معلومات الاتصال التي ظهر أنها تنتمي إلى القحطاني في القسم الثالث للكشف عن تفاصيل إضافية حول بصمته على الإنترنت، بما في ذلك إنشاء حسابات وهمية على وسائل الإعلام الاجتماعية. ختاماً، تتناول استنتاجات التقرير دور القحطاني غير الواضح في جهود محمد بن سلمان المستمرة لإسكات المنتقدين والمعارضين.

حددت جميع المعلومات الواردة في هذا التقرير من خلال بحوث مفتوحة المصدر فقط.

¹ <https://www.reuters.com/article/us-the-ran-murder-khashoggi-behind-man-the-insight/how-adviser-khashoggi-saudi-https://www.reuters.com/article/us-iduskcn1mw2ha-skype-via-killing>

² [https://citizenlab.ca/tag/hacking](https://citizenlab.ca/tag/hacking-team-https://citizenlab.ca/tag/hacking)

³ <https://web.archive.org/web/20150706031523/https://twitter.com/hackingteam/status/617852091390935040>

⁴ <https://twitter.com/hiahy>

⁵ <https://twitter.com/hiahy/status/902673255395463168>

⁶ <https://haveibeenpwned.com/pwnedwebsites#hackforums>

⁷ [https://motherboard.vice.com/en_us/article/kzjmze/saud](https://motherboard.vice.com/en_us/article/kzjmze/saud-team-hacking-arabia-saudi-gahtani-al-https://motherboard.vice.com/en_us/article/kzjmze/saud)

1 - النتائج الرئيسية

فيما يلي ندرج بعض النتائج الرئيسية التي خلص إليها هذا التقرير:

- يملك سعود القحطاني عناوين البريد الإلكتروني: saudq1978@gmail.com و saud@saudq.com و s.qahtani@royalcourt.gov.sa وكذلك رقم الهاتف المحمول +966 55 548 9750. وهذا يؤكد أن القحطاني هو الشخص الذي تواصل مع هاكنغ تيم لشراء أدوات برمجياتهم الخبيثة في عامي 2012 و 2015.
 - استخدم الشخص الذي عرّف عن نفسه على أنه القحطاني في رسائل البريد الإلكتروني مع هاكنغ تيم في عامي 2012 و 2015 اثنين من عناوين البريد الإلكتروني saudq1978@gmail.com و saud@saudq.com و رقم الهاتف +966 55 548 9750 والتي يمكن ربطها بشكل واضح بالقحطاني من خلال تسرب المعلومات من صفحات استعادة كلمة السر لجوجل و تويتر. واستخدم نفس الشخص أيضاً عنوان البريد الإلكتروني s.qahtani@royalcourt.gov.sa للتواصل مع هاكنغ تيم. مع أنه لم يكن من الممكن الدلالة بما لا يقبل الشك على ملكية القحطاني لعنوان البريد الإلكتروني هذا من خلال تسرب المعلومات على صفحات استعادة كلمة السر، يرى هذا التقرير بدرجة عالية من الثقة بأن s.qahtani@royalcourt.gov.sa هو عنوان البريد الإلكتروني الرسمي الحكومي للقحطاني. ويعزى ذلك جزئياً إلى مراسلات عبر البريد الإلكتروني في شهر حزيران/ يونيو 2015 مع هاكنغ تيم تضمنت استخداماً متواصلًا لعنواني القحطاني s.qahtani@royalcourt.gov.sa و saud@saudq.com في ذات الوقت، بما يثبت وجود صاحب واحدٍ لكلا الحسابين.
- سجل القحطاني ما لا يقل عن 22 نطاقاً منذ عام 2009، استخدم بعضها كمخدمات للقيادة والتحكم في البرمجيات الخبيثة. وأظهر القحطاني ضعفاً شديداً فيما يتعلق بأمنه التشغيلي عند تسجيل معظم هذه النطاقات. إذ تضمنت سجلات التعريف Whois لجميع هذه النطاقات إما بريده الإلكتروني الشخصي saudq1978@gmail.com أو رقم الهاتف المحمول +966 55 548 9750 أو تنويكات مختلفة من اسمه الحقيقي، وذلك باستثناء ثلاثة نطاقات هي (jasmn.info و saudq.com، saudqq.com) ولم يبق من هذه إلا نطاقين فعالين لليوم وهما: saudq.com و jasmn.info.
- ويتأكد أن حساب gmail.com@saudq1978 مملوك من قبل القحطاني يثبت أن الحساب المسجل على هاك فورمز عبر حساب البريد الإلكتروني nokia2mon2 يعود أيضاً إلى القحطاني. وتورد مقالات القحطاني على هاك فورمز من بين ما تورد تفاصيل أدوات وخدمات القرصنة التي اشتراها واستخدمها ومنصات وسائل الإعلام الاجتماعية وتطبيقات المحمول التي استهدفها. كما نشر ثلاث مرات على الأقل وهو ثمل، باعترافه، رأيه في مواضيع لا علاقة لها بالقرصنة مثل دور الدين في السياسة والسياسة تجاه إيران.
- وباستخدام معلومات الاتصال التي يملكها القحطاني، أمكن تحديد معلومات اتصال إضافية له وتحديد عدة حسابات مرتبطة بعناوين البريد الإلكتروني وأرقام الهاتف هذه. لديه حساب بريميميوم على لينكدان تحت اسم "saud a" (اسم القحطاني الأوسط هو عبد الله) ، يصف فيه نفسه بأنه "باحثٌ عن العقول الفذة" (headhunter) في المملكة العربية السعودية. وأنشأ حساباً على فيسبوك تحت شخصية وهمية مؤيدة لمبارك "مواطن مصري في نهاية حياته". ولدى القحطاني أيضاً حسابات على سناب شات، واتس آب وسيفغنال.

II. من شاعر إلى منفذ للأوامر

ولد سعود بن عبد الله القحطاني في 7 تموز/ يوليو 1978 في الرياض، وحصل على درجة البكالوريوس في القانون من جامعة الملك سعود قبل أن ينضم إلى دورة تدريب الضباط في القوات الجوية الملكية السعودية، وذلك بحسب ما ورد في أراب نيوز (Arab News).⁸ وتمت ترقية القحطاني في نهاية المطاف إلى رتبة نقيب، تابع بعدها تعليمه في جامعة نايف العربية للعلوم الأمنية، حيث حصل على درجة الماجستير في العدالة الجنائية.

بدأ القحطاني مسيرته في الترويج للأسرة الملكية في أعمدة للصحف السعودية ونشر قصائد قومية تحت الاسم المستعار "الضاري".

في بدايات الألفية الجديدة قام الرئيس السابق للديوان الملكي السعودي خالد التويجري بتوظيف القحطاني لتشغيل جيش إعلامي إلكتروني مكلف بحماية صورة المملكة العربية السعودية بحسب تقارير لرويترز.⁹

انتقل القحطاني بعدها ليشغل عدة أدوار بارزة في الحكومة، بما في ذلك المستشار القانوني للأمانة ومن ثم ولي العهد عبد الله بن عبد العزيز في عام 2003 ومدير الإعلام لنفس الأمانة في عام 2004.

بحلول عام 2008، كان القحطاني قد أصبح مديراً عاماً لمركز الرصد والتحليل الإعلامي بالديوان الملكي. وبعد ذلك بعام، في 2009، انضم إلى هاك فورمز تحت اسم nokia2mon2. في عام 2011 أنشأ حسابه على تويتر @saudq1978.

في عام 2012 تواصل القحطاني مع هاكنغ تيم للمرة الأولى باستخدام عنوان البريد الإلكتروني saudq1978@gmail.com. وأتى عرضه الثاني لهاكنغ تيم في حزيران/ يونيو 2015، حيث استخدم عنوان البريد الإلكتروني الحكومي الرسمي s.qahtani@royalcourt.gov.sa. وكما هو موضح أدناه، على الأغلب لم يكن لدى الديوان الملكي السعودي عناوين بريد إلكتروني رسمية في عام 2012 عندما تواصل القحطاني للمرة الأولى مع هاكنغ تيم.

في ديسمبر/ كانون الأول 2015، أصدر الملك سلمان مرسوماً ملكياً يُرَفِّع فيه القحطاني إلى منصب مستشار ملكي برتبة وزير.¹⁰ قبل ذلك بستة أشهر تقريباً أعلن سلمان تحولاً كبيراً في خط ولاية العهد في المملكة العربية السعودية واضعاً ابنه، محمد بن سلمان، الثاني في ولاية العهد بعد ابن شقيق الملك سلمان، محمد بن نايف.

شغل القحطاني خلال هذه الفترة عدة مناصب رفيعة المستوى في مركز الدراسات والشؤون الإعلامية في الديوان الملكي إلى أن وصل إلى منصب المدير العام في عام 2016. استخدم القحطاني المركز، الذي مارس نشاطاته دون رقابة من قبل أية وزارات أخرى، كقاعدة لعملياته لمساعدة الملك سلمان وابنه محمد في توطيد السلطة فيما كان الأخير يسعى جاهداً لفرض السيطرة مع أفراد آخرين من العائلة المالكة.¹¹ تراوحت هذه المساعي من عمليات فرض التأثير النمذجية، كالتعاقد مع شركات راقية للعلاقات العامة وحشد الرأي، بما في ذلك مجموعة بي جي آر (BGR)،¹² إس جي آر (SGR)،¹³ و سكواير باتون بوجز (Squire Patton Bogg)¹⁴ إلى حملات القمع والترهيب الشاملة بما تتضمنه من اختطاف وتعذيب وقتل.

في ربيع عام 2017، عمل القحطاني والمركز مع "فرقة النمر" أو "مجموعة التدخل السريع" المنشأة حديثاً حينها من أعضاء المخابرات السعودية لتنظيم عمليات خطف المعارضين والنقاد داخل المملكة وخارجها واحتجازهم في مواقع اعتقال سرية.¹⁵ شاركت فرقة النمر في ما لا يقل عن اثنتي عشرة عملية، بما في ذلك قتل الخاشقجي.¹⁶

⁸ [arabia-http://www.arabnews.com/node/1326371/saudi](http://www.arabnews.com/node/1326371/saudi)

⁹ <https://www.reuters.com/article/us-iduskcn1mw2ha-insight-adviser-khashoggi-saudi>

¹⁰ <https://www.spa.gov.sa/1428315>

¹¹ <https://www.washingtonpost.com/opinions/global-about-questions-silence-not-will-anger-rampaging-opinions/mbss>

¹² https://www.washingtonpost.com/opinions/global-f397227b43f0_story.html-b2d2-11e8-d182-khashoggi/2018/10/16/5a0bf43a-jamal

¹³ <https://efile.fara.gov/docs/5430-pdf.53-20160315-ab-exhibit>

¹⁴ <https://efile.fara.gov/docs/6379-pdf.1-20160920-ab-exhibit>

¹⁵ <https://efile.fara.gov/docs/2165-pdf.67-20160920-ab-exhibit>

¹⁶ <https://www.washingtonpost.com/opinions/global-family-saudi-cutthroat-a-in-roots-had-killing-khashoggi-opinions/the>

¹⁶ https://www.washingtonpost.com/opinions/global-68604ed88993_story.html-bc79-11e8-f17b-feud/2018/11/27/6d79880c

¹⁶ <https://www.nytimes.com/2019/03/17/world/middleeast/khashoggi-saudi.html-prince-crown>

في تموز/ يونيو 2017، أصبح محمد بن سلمان ولي العهد بعد أن أصدر الملك سلمان مرسوماً ملكياً يعزل نابف ويعفيه من جميع المناصب الرسمية. ووضع نابف بعد ذلك تحت الإقامة الجبرية. بعد ذلك بخمسة أشهر في تشرين الثاني/ نوفمبر 2017، أسس محمد بن سلمان وترأس "لجنة مكافحة الفساد" التي استخدمت لاعتقال واحتجاز مئات السعوديين الذين شكلوا تهديداً لسلطة محمد بن سلمان، بما في ذلك أمراء ووزراء ورجال أعمال ورجال دين وسياسيين.

وبعد ذلك بأشهر، في تشرين الثاني/ نوفمبر 2017، تم تكليف القحطاني بترأس التحقيق مع رئيس الوزراء اللبناني سعد الحريري الذي اعتقل في الرياض وتعرض للإهانة اللفظية والضرب وأجبر على الاستقالة.¹⁷

واستمرت حملة القمع السعودية حتى عام 2018، عندما تم اعتقال وتعذيب أبرز الناشطات في مجال حقوق المرأة اللواتي كنّ يناضلن من أجل حق المرأة السعودية في القيادة. حيث أُخبرت إحدى الناشطات، وهي لجين الهذلول، أخاها بأنه تم إغراقها في الماء وصعقها بالكهرباء في قبو أحد السجون بالقرب من جدة. وكان الرجل الذي أشرف على تعذيبها هو القحطاني، بحسب شقيق الهذلول، الذي قال بأن المساعد الشخصي لمحمد بن سلمان حضر التعذيب شخصياً ضاحكاً فيما كان يهددها بالاغتصاب والقتل.¹⁸

كما استخدم القحطاني وسائل الإعلام الاجتماعية لإسكات المعارضة والتعرف على منتقدي النظام وشن حملات على الإنترنت ضد منافسي المملكة العربية السعودية، مثل إيران وقطر. في تغريدة تعود لشهر آب / أغسطس عام 2017 ناشد القحطاني متابعيه على تويتر الذين يزيد عددهم عن المليون باستخدام هاشتاج #القائمة_السوداء (TheBlacklist#) لكشف أسماء وهويات المنشقين والناشطين المتعاطفين مع قطر خلال الأزمة الدبلوماسية بين المملكة العربية السعودية وقطر.¹⁹ أي شخص يضاف إلى القائمة السوداء ستم "متابعته" وفقاً للقحطاني. استخدم القحطاني أيضاً متابعيه على وسائل الإعلام الاجتماعية لمضايقة النقاد على الإنترنت، مما أكسبه لقب "سيد الذباب" — حيث يستخدم مصطلح "الذباب الإلكتروني" من قبل النقاد لوصف بوتات القحطاني وأدواته الجاسوسية على الإنترنت.

وفيما وطد محمد بن سلمان سلطته، استمرت حافظة القحطاني الإلكترونية في النمو. في تشرين الأول/ أكتوبر 2017، أصبح القحطاني رئيساً لمنظمة أنشئت حديثاً تحت رعاية اللجنة الأولمبية السعودية تسمى تحالف البرمجيات والأمن الإلكتروني.²⁰ كان الغرض من المنظمة، التي سميت فيما بعد بالاتحاد السعودي للأمن السيبراني والبرمجة والدرونز (SAFCSP)، هو "بناء قدرات وطنية واحترافية في مجال الأمن السيبراني والبرمجة [...] للوصول بالمملكة العربية السعودية إلى مصاف الدول المتقدمة في صناعة المعرفة التقنية الحديثة" وفقاً لموقع المنظمة على الإنترنت.²¹

في شباط / فبراير 2018 غير القحطاني سيرته الذاتية على تويتر²² لتشير إلى أنه كان رئيس مركز التميز لأمن المعلومات (CoEIA)²³ في جامعة الملك سعود و مركز C4I للنظم المتقدمة²⁴ أيضاً في جامعة الملك سعود (تشير C4I إلى القيادة والسيطرة والاتصالات والكمبيوتر والاستخبارات - Command, Control, Communications, Computers and Intelligence). وكتب أيضاً أنه كان عضواً في عدة مجالس: مؤسسة مسك، ومدارس مسك، والهيئة الملكية لمحافظة العلا، ومؤسسة الدار.

وقعت أول مواجهة بين القحطاني والخاشقجي في أواخر عام 2016، عندما كان الأخير يعمل ككاتب عمود لصحيفة الحياة التي يقع مقرها في لندن. حيث اتصل القحطاني بالخاشقجي لإبلاغه بأنه "لا يسمح له بالتغريد، ولا بالكتابة، ولا بالكلام"، وفقاً لتقارير صحيفة واشنطن بوست.²⁵ "لا يمكنك فعل أي شيء بعد الآن، لقد انتهيت." وبعد أن وقع أمر القحطاني على أذان صماء، غير القحطاني أسلوبه وحاول أن يجتذب الخاشقجي إلى المملكة مجدداً، مؤكداً للصحفي بأن تجاوزه سوف تغفر.

¹⁷ <https://www.reuters.com/article/us-the-ran-murder-khashoggi-behind-man-the-insight/how-adviser-khashoggi-saudi-https://www.reuters.com/article/us-iduskcn1mw2ha-skype-via-killing>

¹⁸ <https://www.bbc.com/news/world-47956124-east-middle>

¹⁹ <https://twitter.com/saudq1978/status/898259368696725504>

²⁰ <http://ara.tv/ntwtv>

²¹ <https://safcsp.org.sa/en.html>

²² <https://spoonbill.io/data/saudq1978>

²³ <https://coeia.ksu.edu.sa/en/about>

²⁴ <https://web.archive.org/web/20150510195222/http://c4icas.ksu.edu.sa>

²⁵ <https://www.washingtonpost.com/world/national-of-shadow-long-the-in-exile-an-months-final-khashoggis-security/jamal-https://www.washingtonpost.com/world/national>

[0aa5c2fcc9e4_story.html-b6a9-11e9-0476-arabia/2018/12/21/d6fc68c2-saudi](https://www.washingtonpost.com/world/national-of-shadow-long-the-in-exile-an-months-final-khashoggis-security/jamal-https://www.washingtonpost.com/world/national-0aa5c2fcc9e4_story.html-b6a9-11e9-0476-arabia/2018/12/21/d6fc68c2-saudi)

في 2 تشرين الثاني/ أكتوبر 2018، تفيد التقارير بأن القحطاني اتصل عبر سكايب عدة مرات للإشراف على قتل وتقطيع الخاشقجي في القنصلية السعودية في اسطنبول.²⁶ حيث بعد أن تبادل الإهانات مع الخاشقجي، أمر أعضاء " فريق النمر " الذي كان قد احتجز الخاشقجي بأن "احضروا لي رأس الكلب." " تقدر وكالة المخابرات المركزية الأمريكية بدرجة ثقة متوسطة إلى عالية أن محمد بن سلمان أمر بقتل الخاشقجي بالاستناد جزئياً إلى 11 رسالة نصية تبادلها ولي العهد مع القحطاني قبل وبعد القتل.²⁷

بعد أن أنكرت وزارة الشؤون الخارجية السعودية أي تورط في مقتل الخاشقجي لمدة 18 يوم، أصدرت الوزارة بياناً في 20 تشرين الأول/ أكتوبر 2018 تقر فيه لأول مرة أن الخاشقجي كان قد قتل على أيدي سعوديين ولكن عن طريق الخطأ نتيجة عراق.²⁸ وفي اليوم نفسه أصدر الملك سلمان مرسوماً بإعفاء القحطاني من منصبه كمستشار في الديوان الملكي.²⁹ استخدم القحطاني تويتر ليعرب عن امتنانه للملك سلمان وابنه محمد لسماحهما له بخدمة بلاده.³⁰ كتب القحطاني: "سأظل خادماً مخلصاً لبلدي إلى الأبد". وأرسل تغريدة لاحقة يشكر فيها زملاءه في المركز والإدارات الأخرى في الديوان الملكي.³¹

تم حظر القحطاني رسمياً من قبل وكالتين أمريكيتين. في تشرين الثاني/ نوفمبر 2018، وافقت وزارة الخزانة الأمريكية على حظر القحطاني و 15 عضواً آخرين من فريق النمر لدورهم في قتل الخاشقجي.³² حيث أفاد البيان الصحفي الصادر عن وزارة الخزانة الأمريكية بأن القحطاني كان "جزءاً من تخطيط وتنفيذ العملية التي أدت إلى مقتل الخاشقجي". والتحقت وزارة الخارجية الأمريكية بزميلتها في نيسان/ أبريل 2019، حيث حددت القحطاني و 15 سعودياً آخرين على أنهم لعبوا دوراً في قتل الخاشقجي.³³ وبذلك تم حظر القحطاني وعائلته المباشرة من دخول الولايات المتحدة الأمريكية.

²⁶ <https://www.reuters.com/article/us-the-ran-murder-khashoggi-behind-man-the-insight/how-adviser-khashoggi-saudi-https://www.reuters.com/article/us-iduskcn1mw2ha-skype-via-killing>

²⁷ https://www.washingtonpost.com/world/national-to-alleged-aide-with-messages-exchanged-prince-crown-security/saudi-https://www.washingtonpost.com/world/national-e8028a62c722_story.html-9240-11e8-f5c3-killing/2018/12/01/faa43758-khashoggi-overseen-have

²⁸ <https://twitter.com/ksamofaen/status/1053428352164548609//:https>

²⁹ <https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=1830340>

³⁰ <https://twitter.com/saudq1978/status/1053438590095708160>

³¹ <https://twitter.com/saudq1978/status/1053493341147578368>

³² <https://home.treasury.gov/news/press-releases/sm547-https://home.treasury.gov/news/press>

³³ <https://translations.state.gov/2018/11/15/statement//:https-individuals-on-sanctions-magnitsky-global-pompeo-secretary-by-translations.state.gov/2018/11/15/statement//:https-khashoggi-jamal-of-killing-the-in-involved>

III. تسريب معلومات الاتصال التي يملكها القحطاني

استخدم الشخص الذي عرف عن نفسه باسم سعود القحطاني في رسائل البريد الإلكتروني مع هاكنغ تيم ثلاثة عناوين بريد إلكتروني:

- saudq1978@gmail.com في خمس رسائل إلكترونية على الأقل في آذار/ مارس 2012³⁴
- saud@saudq.com في أربع رسائل إلكترونية على الأقل من حزيران/ يونيو 2015 إلى تموز/ يوليو 2015³⁵
- s.qahtani@royalcourt.gov.sa في 14 بريد إلكتروني على الأقل من حزيران/ يونيو 2015 إلى تموز/ يوليو 2015³⁶


أشار نفس الشخص في رسالتين على الأقل تم إرسالهما من s.qahtani@royalcourt.gov.sa و saud@saudq.com أن رقم هاتفه كان +966 9750 548 55³⁷

باستخدام تسرب المعلومات³⁸ على صفحات جوجل وتويتر لاستعادة كلمة السر، فمن الممكن بشكل مؤكد ربط القحطاني مع عناوين البريد الإلكتروني saud@saudq.com و saudq1978@gmail.com و s.qahtani@royalcourt.gov.sa ورقم الهاتف +966 9750 548 55.

حساب القحطاني على تويتر متصل بالبريد الإلكتروني **saudq@saud.com** ورقم هاتف محمول

يرتبط حساب القحطاني المؤكد على تويتر @saudq1978³⁹ برقم الهاتف +966 9750 548 55 والبريد الإلكتروني saud@saudq.com وفقاً لتسرب المعلومات من ميزة استعادة كلمة السر على تويتر:

How do you want to reset your password?



سعود القحطاني
@saudq1978

We found the following information associated with your account.

Text a code to my phone ending in 50

Email a link to sa**@s****.***

[Continue](#)

[I don't have access to any of these](#)

³⁴ <https://wikileaks.org/hackingteam/emails/?q=&mfrom=saudq1978%40gmail.com&mto=&title=¬itle=&date=count=50&sort=1#searchresult&nofrom=&https://wikileaks.org/hackingteam/emails/?q=&mfrom=saud%40saudq.com&mto=&title=¬itle=&date=noto=&count=50&sort=1#searchresult>

³⁵ <https://wikileaks.org/hackingteam/emails/?q=&mfrom=saud%40saudq.com&mto=&title=¬itle=&date=noto=&count=50&sort=1#searchresult>

³⁶ <https://wikileaks.org/hackingteam/emails/?q=&mfrom=s.qahtani%40royalcourt.gov.sa&mto=&title=¬itle=&date=from=¬o=&count=50&sort=1#searchresult>


³⁷ <https://wikileaks.org/hackingteam/emails/emailid/1134945> و <https://wikileaks.org/hackingteam/emails/emailid/1144691>

³⁸ <https://motherboard.vice.com/en/reset-password-us/article/8q8x8a/twitter>

³⁹ <https://twitter.com/saudq1978>

من أجل الوصول إلى صفحة تغيير كلمة السر في لقطة الشاشة أعلاه يجب إدخال عنوان البريد الإلكتروني الصحيح ورقم الهاتف الصحيح. إن تقديم عنوان بريد إلكتروني غير مرتبط بحساب القحطاني يعطي رسالة خطأ:

Verify your personal information



سعود القحطاني
@saudq1978

Enter your email address to continue

Email incorrect. Please try again.

Submit

[I don't have access to this information](#)

وتظهر رسالة خطأ مماثلة عندما يتم تقديم رقم هاتف غير صحيح.

البريد الإلكتروني للديوان الملكي المستخدم لتوفير رقم الهاتف والبريد الإلكتروني للقحطاني

نظراً إلى أن القحطاني هو صاحب رقم الهاتف +966 548 55 9750 وعنوان البريد الإلكتروني saud@saudq.com فمن المحتمل جداً أن عنوان البريد الإلكتروني العائد للحكومة السعودية s.qahtani@royalcourt.gov.sa يعود أيضاً إلى القحطاني.

في 29 حزيران/ يونيو 2015 تلقى مؤسس هاكنغ تيم ورئيسه التنفيذي ديفيد فينشينزيتي رسائل البريد الإلكتروني الأولى المرسلة من s.qahtani@royalcourt.gov.sa إلى هاكنغ تيم. في أحد تلك الرسائل طلب المرسل من فينشينزيتي الاتصال به "على هاتفي الشخصي المحمول +966 548 55 9750" عبر تطبيقات الرسائل المشفرة ثريما (Threema) أو تلغرام (Telegram):⁴⁰

عزيزي ديفيد

نظراً إلى سمعتك الموقرة ومهنتك، نود من مركز الرصد والتحليل الإعلامي في الديوان الملكي السعودي (مكتب الملك) في أن ندخل في تعاون مثمر معك وتطوير شراكة طويلة واستراتيجية.

أطلب منكم التكرم بإرسال قائمة كاملة بالخدمات التي تقدمها شركتكم الموقرة بالإضافة إلى أسعارها، مشروحة بالتفصيل، في أسرع وقت ممكن.

يمكنك الاتصال بي عن طريق تلغرام أو ثريما على هاتفي المحمول الخاص +966 548 55 9750 لترتيب إرسال معلوماتك مشفرة بطريقة مناسبة لك (pgp) أو بأي طريقة أخرى تفضلها.

مع أطيب التحيات

سعادة سعود القحطاني
مستشار في الديوان الملكي
المدير العام لمركز الرصد والتحليل الإعلامي

[ملاحظة، لا يتحدث القحطاني الانكليزية بطلاقة. وجميع أخطاء التهجئة والنصوص والقواعد الواردة في النص الإنكليزي من هذا التقرير منقولة حرفياً من الأصل. تم تفادي هذه الأخطاء وتصحيح المعنى قدر الإمكان في الترجمة العربية]

بعد مواجهة الكثير من الصعوبات لربط مفتاح pgp بشكل صحيح، أرسل الشخص وراء s.qahtani@royalcourt.gov.sa بريداً إلكترونياً إلى ممثل حساب هاكنغ تيم، عماد شحاتة، في 30 حزيران/ يونيو 2015 يذكر فيه عنوان البريد الإلكتروني saud@saudq.com على أنه عنوان بريده الإلكتروني الخاص:⁴¹

أرسلته إليك الآن من بريدي الإلكتروني الخاص
saud@saudq.com
بما أن هناك مشكلة في إرفاقه في هذا البريد الإلكتروني
أمل أن يعمل هذه المرة
تحياتي

قبل دقيقتين من ذلك، أرسل القحطاني بريداً إلكترونياً إلى شحاتة من saud@saudq.com بموضوع "مفتاحي".⁴² وكتب القحطاني: "تجده مرفقاً، أمل أن يعمل الآن". هذا البريد الإلكتروني إلى شحاتة كان أول بريد إلكتروني إلى هاكنغ تيم باستخدام بريد القحطاني الإلكتروني saud@saudq.com.

رد شحاتة بعد دقائق إلى القحطاني عبر saud@saudq.com بأنه تلقى المفتاح. في الساعة التاسعة صباحاً بتوقيت غرينتش، رد القحطاني عبر saud@saudq.com "عظيم؛ أنا بانتظارها لأوقعها كي نستطيع الذهاب إلى الخطوة التالية. أنا متأكد من أن اتفاقية السرية الخاصة بك ستكون جيدة جداً وسوف تحمي خصوصيتنا."⁴³ في الساعة التاسعة وسبع دقائق صباحاً بتوقيت غرينتش، رد qahtani@royalcourt.gov.sa على رسالة من شحاتة تحمل موضوع "اتفاقية السرية (NDA)" كاتباً: "حسناً، حصلت عليها، سأوقعها لاحقاً اليوم وأرسلها لك مرة أخرى".⁴⁴

إن مراسلات شحاتة المتواصلة مع عنواني البريد الإلكتروني s.qahtani@royalcourt.gov.sa و saud@saudq.com في ذات الوقت، فيما يتعلق بنفس الموضوع، يزيد احتمالات كون القحطاني هو صاحب عنوان البريد الإلكتروني التابع للديوان الملكي.

تم ربط جيميل بنفس رقم هاتف القحطاني وبريده الإلكتروني الموجودان على تويتر


يملك القحطاني أيضاً عنوان البريد الإلكتروني saudq1978@gmail.com استناداً إلى تسرب المعلومات من ميزة استعادة كلمة السر لدى جوجل، مما يدل على أن حساب جيميل متصل برقم هاتف القحطاني: +966 55 548 9750:

<https://wikileaks.org/hackingteam/emails/emailid/1134964> ⁴¹

[1134947/https://wikileaks.org/hackingteam/emails/emailid](https://wikileaks.org/hackingteam/emails/emailid/1134947) ⁴²

<https://wikileaks.org/hackingteam/emails/emailid/1134955> ⁴³

<https://wikileaks.org/hackingteam/emails/emailid/1134951> ⁴⁴


Account recovery
This helps show that this account really belongs to
you

saudq1978@gmail.com ▾


A text message with a 6-digit verification code was just sent to 055 548 9750

Enter the code


G-

[I don't have my phone](#) [Next](#)

كما هو الحال مع ميزة استعادة كلمة السر في تويتر، فإن تقديم رقم هاتف غير مرتبط بحساب القحطاني يعطي رسالة خطأ:


Account recovery
This helps show that this account really belongs to
you

saudq1978@gmail.com ▾




Get a verification code

To get a verification code, first confirm the phone number you added to your account50. *Standard rates apply*

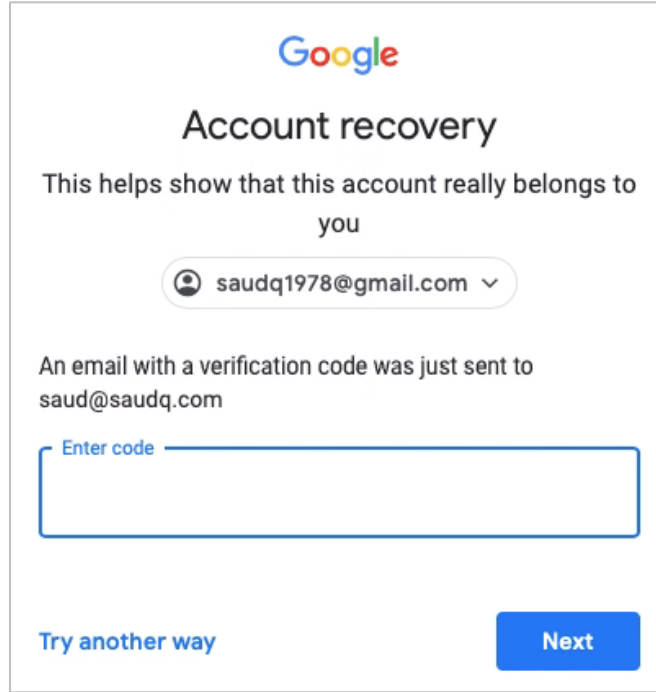
Phone number

+966 555489050|

 This number doesn't match the one you provided. Try again.

[I don't have my phone](#) [Send](#)

وتظهر نفس التقنية أن البريد الإلكتروني للقحطاني saud@saudq.com متصل أيضاً بالعنوان :saudq1978@gmail.com



ينتج تقديم عنوان بريد إلكتروني غير صحيح رسالة خطأ مشابهة لرسالة خطأ رقم الهاتف أعلاه.

تم إرسال أول بريد إلكتروني إلى هاكنغ تيم من القحطاني عبر saudq1978@gmail.com في 18 آذار/ مارس، 2012 وطلب فيه من هاكنغ تيم السفر إلى المملكة العربية السعودية لشرح ما يمكن للشركة أن تقدمه وتوفير التدريب:⁴⁵

سيدي العزيز:
نحن بحاجة إلى أشخاص لزيارتنا باستضافة الحكومة السعودية بحيث يجب أن يملكو معرفة تقنية ممتازة وسلطة عالية من أجل تقديم عرض متكامل وشرح الحلول التي تقدمونها وتوفير التدريب والتكاليف. سوف نتحمل كل تكاليف الرحلة من البداية للنهاية. من فضلك أرسل لي كل المعلومات التي تحتاجها للقيام بذلك.

تحياتي

سعود

طلب مدير الحساب لدى هاكنغ تيم، مصطفى مئاع، من القحطاني استخدام عنوان بريد إلكتروني رسمي نظراً لأن "سياستنا تحصر التعامل بالوكالات الحكومية فقط." رد القحطاني بأن الديوان الملكي ليس لديه عناوين بريد إلكتروني رسمية:⁴⁶

سيدي العزيز، أنا مخول من حكومتي أن أتصل بكم. نحن من البلاط الملكي للمملكة العربية السعودية، مكتب الملك. ليس لدينا عناوين بريد إلكتروني رسمية ونستخدم فاكس مؤمن فقط، الرقم هو: +96612926120. إن كنت ترغب يمكننا تأكيد ذلك معك عبر الفاكس.
أو: أرسل لي الاسم والرقم والبلد للشخص الذي ستتصل به سفارتنا. سيأكدون رسمياً أننا سمحنا له بالاتصال بشركتك. لن يخول لهم مناقشة أي شيء معك، لكنهم سيؤكدون فقط - تبعاً لطلبك -
بأن هذه صفقة حكومية وستكون مؤمنة وبأن رقم الفاكس هو رقمنا الرسمي وبأننا

⁴⁵ <https://wikileaks.org/hackingteam/emails/emailid/578260>

⁴⁶ (المرجع نفسه)

مخولون بالكلام والتعامل باسم الديوان الملكي في المملكة العربية السعودية. بعد ذلك يمكننا المضي في الخطوة التالية. أتمنى أن يكون هذا مناسباً لك.

تحياتي، سعود عبد الله

وفقاً لسجلات Whois فإن النطاق royalcourt.gov.sa الذي سيستخدمه القحطاني لاحقاً للتواصل مع هاكنغ تيم في عام 2015، لم ينشأ حتى حزيران/يونيو 2013:

```
% SaudiNIC Whois server.
% Rights restricted by copyright.
% http://nic.sa/en/view/whois-cmd-copyright

Domain Name: royalcourt.gov.sa

Registrant:
الديوان الملكي
Address: قصر اليمامة
الرياض
المملكة العربية السعودية

Administrative Contact:
فيصل الشيبلي
Address: الرياض قصر اليمامة
الرياض 1137
Saudi Arabia

Technical Contact:
يزيد بن فهد المقرن
Address: الرياض قصر اليمامة
الرياض 1137
المملكة العربية السعودية

Name Servers:
ns2.elm.com.sa
ns2.dnspark.net
ns5.dnspark.net
ns1.elm.com.sa

Created on: 2013-06-30
Last Updated on: 2016-07-07
```

IV. النشاط على هاك فورمز

استخدم القحطاني saudq1978@gmail.com لمجموعة واسعة من الأنشطة عبر الإنترنت، بما في ذلك تسجيل حسابات على المنتديات ومواقع التواصل الاجتماعي. ذكر كل من حساب تويتر @HIAHY ومذر بورد أن saudq1978@gmail.com استخدم لتسجيل حساب على موقع القرصنة هاك فورمز تحت اسم المستخدم nokia2mon2.nokia2mon2.

في الواقع، ربطت البيانات الناتجة عن اختراق الموقع في حزيران/ يونيو 2011، والذي يتمتع بشعبية لدى القرصنة ومرتكبي الجرائم الإلكترونية ذوي المهارات المنخفضة، saudq1978@gmail.com مع اسم المستخدم nokia2mon2 وعنوان بروتوكول الإنترنت IP- 153.120.62.248 [.] - والذي يشير تحديد موقعه الجغرافي إلى أنه في الرياض ويشكل حالياً جزءاً من شبكة فرعية مخصصة لشركة الاتصالات السعودية (اتحاد اتصالات).

كان القحطاني عضواً نشطاً في هاك فورمز، حيث نشر أكثر من 500 مرة⁴⁷ وساهم بأكثر من عشر آلاف دولار في الموقع بين تموز/ يوليو 2009 وأيلول/ سبتمبر 2016. وقد حذف ما لا يقل عن 98 من تدويناته، حيث تشير بياناته الشخصية كعضو إلى أنه نشر 441 مرة، في حين تظهر لقطة شاشة نشرت على @HIAHY أنه نشر على الأقل 539 مرة.

لم يكشف القحطاني أبداً عن هويته في المنتدى، لكنه شارك معلومات عن سيرته الذاتية في تدوينه، وكشف عن اسم القحطاني الأول مستخدم آخر للمنتدى في سلسلة من التدوينات تشرح تفاصيل صفقة بين هذا المستخدم والقحطاني.

في تشرين الأول/ أكتوبر 2010، كتب القحطاني تدوينة عن نفسه رداً على نقاش يتضمن توظيف أعضاء لمجموعة تطلق على نفسها اسم ذا راتس كرو (The RATS Crew) (RAT)، أو ما يعرف بـ "remote access trojan"، هو نوع من البرمجيات الخبيثة التي تسمح للقرصنة بالوصول إلى والسيطرة على جهاز الكمبيوتر المصاب عن بعد).⁴⁸ كتب القحطاني أنه كان يبلغ من العمر 33 عاماً وأنه استخدم الـ راتس (RATs) منذ عام 2000. في الواقع، كان القحطاني يبلغ من العمر 32 عاماً في ذلك الوقت إذ أنه مولود في 7 تموز/ يوليو 1978، بحسب وزارة الخزانة الأمريكية.⁴⁹ وكتب بأنه كان من المملكة العربية السعودية، وأنه توقف عن استخدام الـ راتس بحلول عام 2002 "لأنني أعمل على مستقبلي (:". كما ذكر أعلاه، تم تعيين القحطاني من قبل الرئيس السابق للديوان الملكي السعودي، التويجري، لتشغيل جيش إعلامي إلكتروني مكلف بحماية صورة المملكة العربية السعودية في بدايات الألفية.

في تشرين الأول/ أكتوبر الذي سبق، بدأ مستخدم يسمى ReIvIotelVlod سلسلة من التدوينات في المنتدى الموازي "سوق البائعين الثانوي" (Secondary Sellers Market) ذكر فيه اسم القحطاني الأول، سعود، في عنوان التدوينة: "صفقتي أنا وسعود لشراء مخدم افتراضي خاص" (me & saud vps deal).⁵⁰ تبدو الصفقة التي وصفها ReIvIotelVlod وكأنها عملية احتيال: إذ دفع القحطاني لهذا المستخدم 250 دولار لبوتات على شبكة البوتات الخاصة "بصديق" ReIvIotelVlod. لكن صديق ReIvIotelVlod قام بحظره، بحسب ما ذكره ReIvIotelVlod، لذا طلب من القحطاني مبلغ 20 دولار إضافية لإنشاء مخدم (IRC) لشبكة بوتات.

يعرض هذا القسم بالتفصيل نشاط القحطاني في المنتدى، بما في ذلك ما يلي:

- الحيلة التي وقع ضحية لها
- أدوات وخدمات القرصنة التي اشتراها واستخدمها
- منصات التواصل الاجتماعي وتطبيقات المحمول التي استهدفها
- آراءه بشأن الرب والدين والرئيس أوباما وكشمير
- اعترافه بأنه ثمل
- طرق الدفع التي اتبعها واستخدامه لعنوان بريد إلكتروني إضافي
- محاولاته لاختراق الشبكات اللاسلكية

⁴⁷ <https://twitter.com/hiahy/status/902979053417848833/photo/1>

⁴⁸ [https://hackforums.net/showthread.php?tid=151065&pid=7031243&highlight=becuse + making+my + future # pid ?https://hackforums.net/showthread.php](https://hackforums.net/showthread.php?tid=151065&pid=7031243&highlight=becuse+making+my+future+pid?https://hackforums.net/showthread.php?tid=166087&pid=1565133&highlight=saud+vps+deal#pid1565133)

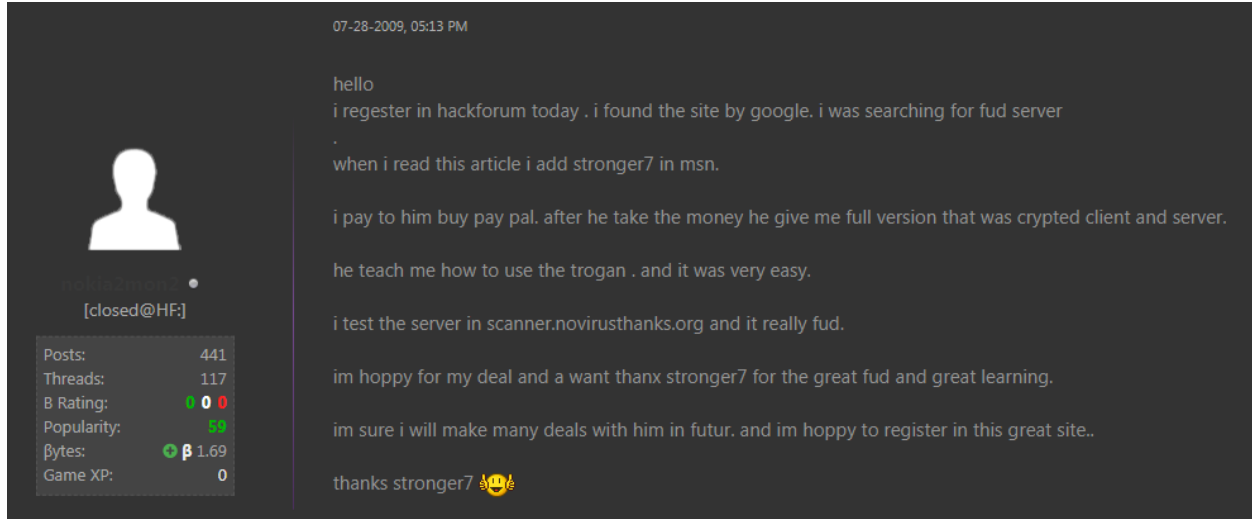
7031243

⁴⁹ <https://www.treasury.gov/resource>

⁵⁰ [https://hackforums.net/showthread.php?tid=166087&pid=1565133&highlight=saud + vps + deal#pid1565133](https://hackforums.net/showthread.php?tid=166087&pid=1565133&highlight=saud+vps+deal#pid1565133)

خُدع في اليوم الأول

كانت بداية القحطاني في هاك فورمز مشؤومة، حيث يعد الاحتيال شائعاً. سجل القحطاني حساب nokia2mon2 في 28 تموز/ يوليو 2009، وفقاً لملفه الشخصي.⁵¹ ونشر تدوينته الأولى في نفس اليوم، حيث قال فيها أنه وجد هاك فورمز بعد البحث عن "خادم فد" (fudserver) (يعني الاختصار FUD "غير قابل للكشف إطلاقاً" (fully undetectable) ويشير إلى البرمجيات الخبيثة التي لا يمكن كشفها إطلاقاً بواسطة البرمجيات المضادة للفيروسات). وكتب أنه اشترى برمجية طروادة⁵² من مستخدم يدعى سترونغر7 (stronger7)، والذي علمه كيفية استخدام البرنامج الذي لم يذكر اسمه:



وعلق مستخدمون آخرون على الموضوع على أن تلك البرمجية التي باعها سترونغر7 تبدو وكأنها نسخة معدلة من رات يدعى سيربيروس (Cerberus). بعد ذلك بأيام، في 2 آب/ أغسطس 2009، كتب القحطاني أن حاسبه الشخصي كان مصاباً بفيروس وأنه كان عليه إصلاحه.⁵³ ربط المستخدمون على الفور مشكلة حاسوب القحطاني مع سترونغر7: "على الأرجح أن حاسوبك أصيب بالهراء التجسسي الذي باعه سترونغر7. أنت اشتريت ذلك أليس كذلك؟" رد القحطاني: "نعم اشتريته!! هل هو ضار؟؟ [...] لا أعتقد أن سترونغر7 قد يفعل ذلك بي. أعتقد أنه رجل جيد جداً ويبدو محل ثقة!!!!" علق مستخدم آخر: "ضحية مسكينة أخرى!" تم حظر سترونغر7 لاحقاً من قبل مدراء هاك فورمز.

سقط القحطاني ضحية لحيلتين أخريين على الأقل فيما كان يمارس نشاطه على هاك فورمز، وتم اختراق حسابه أيضاً.

في أيلول/ سبتمبر 2010، بعد عام من إصابته بفيروس سترونغر7، قال أنه تعرض للاحتيال بمبلغ 150 دولار بعد أن دفع لمستخدم يدعى موبريز (MoBreeze) عن طريق ويسترن يونيون ليعطيني كلمة مروري المخترقة لبريد هوميل.⁵⁴

بعد خمس سنوات، في نيسان/ أبريل 2015، كتب أنه تم خداعه بمبلغ 3000 دولار في بيتكوين من قبل مستخدم يدعى "أونك" (Unk).⁵⁵ ولم يشر القحطاني إلى ما كان يحاول شراؤه. لم يتم تحديد عنوان محفظة البيتكوين الخاصة بالقحطاني في سياق هذا التحقيق.

في كانون الأول/ ديسمبر 2015، تم اختراق حساب القحطاني. حيث نشر شخصٌ ما باستخدام حسابه تدوينة تطلب تبديل 8000 دولار إلى بيتكوين.⁵⁶ بعد ثلاث صفحات من النقاشات التي تكفل nokia2mon2 وتعبير المستخدمين عن دهشتهم لكبر المبلغ، بدأ بعض أعضاء المنتدى بتخمين أن حساب nokia2mon2 قد تم اختراقه بعد أن لاحظوا تغيير في عنوان بروتوكول الإنترنت (IP) الذي تم منه تسجيل الدخول والمقترن مع الحساب والتناقضات مع التدوينات السابقة:

⁵¹ <https://hackforums.net/member.php?action=profile&uid=80618>

⁵² ([https://en.wikipedia.org/wiki/trojan_horse_\(computing\)](https://en.wikipedia.org/wiki/trojan_horse_(computing)))

⁵³ <https://hackforums.net/showthread.php?tid=114215&pid=1057777#pid1057777>

⁵⁴ <https://hackforums.net/showthread.php?tid=711096>

⁵⁵ <https://hackforums.net/showthread.php?tid=4777180&pid=45693982#pid45693982>

⁵⁶ <https://hackforums.net/showthread.php?tid=5083921&page=9>

12-06-2015, 07:39 PM #58

Ah-Muzen-Cab Wrote: » (12-06-2015, 07:35 PM)

Well I think we'd all like to know that reason then...

Let me comment, then.

- 1- Last IP Change Date: Yesterday
- 2- No GAuth/2FA enabled
- 3- All previous exchange threads, he has said he would go first. The PM someone posted here earlier, he said he wouldn't go first since he was scammed for \$1800. UNLESS that deal was taken off-site, he couldn't have been scammed, since the last thread he made for \$1800 deal (which the compromiser was referring to) was successfully completed. Even he posted about it.
- 4- The way nokia is speaking NOW compared to previous threads does not match up with his English. These recent posts know English, just no grammar. Real nokia has trouble with the actual English part of it.
- 5- nokia offered an 80% exchange rate on his last exchange, now he's only willing to pay 10%?

Comparatively, it would seem he was hacked.
Just my \$0.02

[closed@HF:]

Posts:	11,803
Threads:	1,025
B Rating:	0
Popularity:	0
Bytes:	0
Game XP:	0

في اليوم التالي، نشر الشخص المسيطر على حساب القحطاني تدوينة يسأل فيها عن تبادل 1,900 دولار إلى بيتكوين.⁵⁷ كتب جيسي لابروكا، مدير هاك فورمز، أن تلك التدوينة "لم تنشر من قبل صاحب الحساب"، ولكن ليس قبل أن يرسل أحد المستخدمين إلى القرصان الذي يسيطر على nokia2mon2 500 دولار عن طريق باي بال.

بعد ذلك بأسبوعين، بدأ القحطاني بسلسلة تدوينات جديدة بعنوان "لقد عدت" نصح فيها أعضاء المنتدى الآخرين بإعداد التحقق ثنائي العوامل على حساباتهم وأخبرهم بأنه "أصلحت ما فعله المحتال تحت اسمي بحيث لا يتأذى أحد بسبب غلطتي".⁵⁸

im back

12-21-2015, 12:20 AM (This post was last modified: 12-21-2015, 12:21 AM by nokia2mon2)

my advice to all
active the 2 step verification
my bad i didn't do it after i asked to remove it

thx for all who stand with me
and a big thx for omni of course

and i fixed what the scammer did under my name so no one got harm because of my mistake.

again active the 2 step verification guys 🙏

love u all

Regards

[closed@HF:]

Posts:	441
Threads:	117
B Rating:	0
Popularity:	0
Bytes:	1.69
Game XP:	0

الراتس (RATs) وشبكات البوت (Botnets) وهجمات حجب الخدمة (DDoS)

على مدى السنوات السبع التي قضاها في هاك فورمز، اعترف القحطاني بشراء أو استخدام حوالي أربع وعشرين من أدوات وخدمات القرصنة، والتي لم يحتج معظمها إلى معرفة تقنية واسعة. كانت الأدوات والخدمات التي استخدمها في الغالب راتس، وكريبترز، وورمز، وبوتات يتم تأجيرها لتنفيذ هجوم حجب الخدمة.

⁵⁷ <https://hackforums.net/showthread.php?tid=5084797>

⁵⁸ <https://hackforums.net/showthread.php?tid=5102030&pid=49047929#pid49047929>

استهداف استخدام الرات في عملية دولية لإنفاذ القانون

أظهر القحطاني اهتماماً في الراتس والكريبترز من أول أيامه في هاك فورمز (الكريبتر هو نوع من البرمجيات التي تقوم بتشفير أو تشوش مسار البرمجيات الخبيثة بحيث تجعل من الصعب الكشف عنها عن طريق برامج مكافحة الفيروسات). في تدوينته الثانية في المنتدى، في تموز/ يوليو 2009، طلب القحطاني تقديم توصيات بشأن "كريبتر قوي يمكن أن يعمل مع كل الراتس ويجعلها عسيرة على الاكتشاف بشكل كامل وأن يعمل بشكل مستقر جداً".⁵⁹

بحلول حزيران/ يونيو 2011، بعد أقل من عامين من انضمامه إلى المنتدى، قدر أن لديه 90 ٪ من الراتس المدفوعة والمجانية المعروضة في السوق.⁶⁰ وقد ذكر على وجه التحديد استخدام:

- بلاكشيدس (Blackshades)
- بوزن آيفي (Poison Ivy)
- سايبيرغيت (Cybergate)
- ألبرتينو أدفانسد رات (Albertino advanced rat)
- نولبوت (Nulbot)
- نيتواير (Netwire)

كما ذكر استخدام ما لا يقل عن تسعة كيربترز:

- ألفا كريبت (Alpha Crypt)
- تيجون كريبتر في 1.2 (Tejon Crypter v1.2)
- بولي كريبت (PolyCrypt)
- داملا بروتكتور (Damla Protector)
- دارتي (Darty)
- دارك أي (Dark Eye)
- ديزينيس (Dizziness)
- كيوب (Cube)
- (p3rfix)

في تدوينته في حزيران/ يونيو 2011 المذكورة أعلاه، تغنى ببلاكشيدز، واصفاً ذلك بأنه "أفضل خيار":

06-20-2011, 03:53 PM (This post was last modified: 06-20-2011, 03:55 PM by nokia2mon2)

i think i have 90% of the rats paid and free version on the market
No one can vs blackshades
the last update was amazing
they always amazed me with every update, i dont know what they will do in future but im sure they will continue surprised us.
Honestly the price is very very Cheap with all that features.
if you want a rat, this is your best choice and deal u can have.
and by the way the supporting are very professional team.

what i can say
i love blackshades :)

Posts: 441
Threads: 117
B Rating: 0
Popularity: 1.69
bytes: 1.69
Game XP: 0

وقد تم في سياق هذا التحقيق تحديد البنية التحتية المضيفة التي أنشأها القحطاني لاستخدام بلاكشيدز، ويرد تفصيلها في القسم V.

⁵⁹ <https://hackforums.net/showthread.php?tid=111226>

⁶⁰ <https://hackforums.net/showthread.php?tid=1250098&pid=12842475#pid12842475>

بلاكشيدز، التي تباع بما لا يزيد عن 40 دولار على هاك فورمز، تستهدف أنظمة تشغيل مايكروسوفت ويندوز وتسمح للقراصنة بالتحكم سراً وعن بعد في حاسوب الضحية عن طريق واجهة المستخدم الرسومية. وبمجرد الإصابة يمكن للقراصنة استخدام حاسوب الضحية للوصول إلى الملفات وتعديلها، وتفعيل كاميرا الويب، وتسجيل ضغطات المفاتيح، وسرقة كلمات السر، وإدراج الحاسوب في شبكة بوت للمشاركة في هجمات حجب الخدمة.

كان استخدام القحطاني للبلاكشيدز ملحوظاً، نظراً لأن تلك البرمجية الخبيثة كانت الدافع وراء ما وصفته وزارة العدل الأمريكية على أنه "أكبر عملية عالمية على الإطلاق لإنفاذ القانون السيبراني".⁶¹ في أيار/ مايو 2014، أعلنت وزارة العدل الأمريكية أن أكثر من 90 شخصاً تم اعتقالهم في 19 بلداً لمكافحة بيع واستخدام الـراتس التي تم شراؤها من قبل الآلاف من الأفراد في أكثر من 100 دولة والتي أصابت أكثر من 500 ألف جهاز كمبيوتر. وشملت العملية التي استغرقت يومين 359 عملية تفتيش للمنازل ومصادرة أكثر من 1100 جهاز إلكتروني، وفقاً لمكتب الشرطة الأوروبي.⁶²

من بين الذين تم اعتقالهم كان مايكل هوغ، أحد المشاركين في صناعة بلاكشيد، والذي شارك بهاك فورمز تحت اسم xVisceral.⁶³ في تدوينة في تشرين الأول/ أكتوبر 2010، كتب القحطاني أنه كان يواجه مشكلة في تثبيت النسخة المشفرة من بلاكشيد على 100 جهاز. دخل xVisceral⁶⁴ عن بعد إلى حاسوب القحطاني (أو "tv on my pc" كما وصفها القحطاني) وثبت 20 إصداراً غير مشفراً على 20 جهاز، بحيث أصبحت "تعمل بشكل جيد.. جيد جداً".

قد يكون القحطاني استخدم بلاكشيدز لهجمات حجب الخدمة (هناك تداخل بين بوتات هجمات حجب الخدمة والراتس التي تحمل قدرات هجمات حجب الخدمة). ومع ذلك، أظهر القحطاني أيضاً اهتماماً في الدخول عن بعد إلى ميكروفونات أجهزة الكمبيوتر للقيام بتسجيلات سرية.

في تدوينة في أيار/ مايو 2013، عرض القحطاني 100 دولار لأفضل توصية حول كيفية تسجيل غرفة خلسة وحفظ الملف وتحميله على خادم الويب الخاص به أو إرساله لنفسه عبر البريد الإلكتروني.⁶⁵ وقال إن لديه قدرة وصول مادية لحوالي 10 حواسيب ويندوز وأنه يحتاج إلى معرفة أي حاسوب جاء منه التسجيل. وأضاف بأنها "يجب أن تحفظ الأصوات في الغرف في أفضل جودة، ويجب أن تكون مستقرة جداً، وتحمل ملف الصوت كل ثلاث ساعات أو شيء من هذا القبيل"، وبالطبع يجب أن يكون كل شيء مخفياً حتى لا يعرف أحد أن صوته مسجل".

اقترح أحد أعضاء المنتدى بأن يستعمل رات جنباً إلى جنب مع برنامج تسجيل، لكن القحطاني أجاب بأنه حاول ذلك ولكنه يحتاج الآن إلى حل اختصاصي أكثر: "هذا ما استخدمته ولا يعجبني، أريد طريقة تخصيصية أكثر". اقترح مستخدم يدعى جلاسي (Glassy)⁶⁶ الحل الفائز، ولكن تم ذلك على ما يبدو عن طريق رسالة خاصة أو في تدوينة تم حذفها لاحقاً. يبدو أن القحطاني واصل العمل خلف الكواليس مع جلاسي. وبعد عام ونصف من اقتراح الحل الفائز، وصف جلاسي القحطاني بأنه "أفضل شريك لي" في تدوينة امتدحت القحطاني لتبرعه لهاك فورمز.⁶⁷

حاول توظيف مختص بهجمات حجب الخدمة لإدارة شبكة البوتات

كما هو الحال مع الـراتس، قال القحطاني أنه اشترى واستخدم "تقريباً كل" بوتات هجمات حجب الخدمة المعروضة للبيع على هاك فورمز.⁶⁸ من بين بوتات هجمات حجب الخدمة والخدمات المعروضة للأجار لتنفيذ هجمات حجب الخدمة التي استخدمها:

- دي دوسر - الإصداران 3.6 و4.2 (Doser-D)
- تشيكن إكس شيل شوب (Chickenx Shell Shop)
- أوبتيما (Optima)
- ثري في بوت (3vBot)
- تيببيس دي دي أو إس سرفيس (s DDOS service'Tippy)
- أنكل سام دي دي أو إس سيرفيس (UncleSam DDOS service)

⁶¹ [-charges-announce-charge-director-assistant-fbi-and-attorney-us-sdny/pr/manhattan-https://www.justice.gov/usao-connection](https://www.justice.gov/usao-charges-announce-charge-director-assistant-fbi-and-attorney-us-sdny/pr/manhattan-https://www.justice.gov/usao-connection)

⁶² [cybercriminals-against-operation-https://www.europol.europa.eu/newsroom/news/worldwide](https://www.europol.europa.eu/newsroom/news/worldwide-cybercriminals-against-operation-https://www.europol.europa.eu/newsroom/news/worldwide)

⁶³ [/arrested-creator-co-https://blog.malwarebytes.com/cybercrime/2012/07/blackshades](https://blog.malwarebytes.com/cybercrime/2012/07/blackshades-arrested-creator-co-https://blog.malwarebytes.com/cybercrime/2012/07/blackshades)

⁶⁴ [blackshades#pid7118882=https://hackforums.net/showthread.php?tid=742597&pid=7118882&highlight](https://hackforums.net/showthread.php?tid=742597&pid=7118882&highlight-blackshades#pid7118882=https://hackforums.net/showthread.php?tid=742597&pid=7118882&highlight)

⁶⁵ <https://hackforums.net/showthread.php?tid=3474577&pid=32582842#pid32582842>

⁶⁶ <https://hackforums.net/member.php?action=profile&uid=734805>

⁶⁷ <https://hackforums.net/showthread.php?tid=4473706&pid=42672088#pid42672088>

⁶⁸ <https://hackforums.net/showthread.php?tid=966048&pid=12314690#pid12314690>

في البداية حاول القحطاني توظيف شخص ما لإدارة شبكة البوتات وهجمات حجب الخدمة له. في تشرين الأول/ أكتوبر 2009، بعد بضعة أشهر من انضمامه إلى المنتدى، نشر القحطاني إعلاناً يبحث فيه عن شخص ماهر في هجمات حجب الخدمة، وعرض راتب 500 دولار شهرياً.⁶⁹

بعد عدم تلقيه لأي رد، رفع الراتب إلى 700 دولار في الشهر وكتب "الشخص الأول توقف عن العمل بسبب تعليمه". وكتب القحطاني في وقت لاحق أنه "مازال ينتظر" رداً.

بعد ذلك بعام، في أيلول/ سبتمبر 2010، نشر تدوينة بعنوان "مدير لمخدم هجمات حجب الخدمة" كتب فيها أنه كان يبدأ "من الصفر مرة أخرى" وأنه يحتاج إلى مدير جيد، وأنه كان على استعداد لدفع 500 دولار شهرياً.⁷⁰ وطلب 5000 بوت كبدائية/ تتم استضافتهم في الولايات المتحدة وكندا والمملكة المتحدة والمملكة العربية السعودية والكويت ودبي وأوروبا.

وفي اليوم التالي كتب أنه قد تلقى رسالة خاصة من المحتالين، وأنه سوف يطلب من المرشحين تنفيذ هجوم حجب الخدمة على واحد أو اثنين من المواقع "لمدة دقيقة للتأكد منك". وأضاف قائلاً أنه لن يقوم بالهجوم على أكثر من موقعين إلى ثلاثة مواقع في اليوم وأنه "لن أقوم بأي شيء لعدة أيام ... لكن الراتب سيدفع بكل الأحوال". وأشار أحد المستخدمين إلى أن القحطاني كانت يعرض راتباً مبالغاً به: "500؟ أنا لا أعرف ولكن يبدو هذا كثيراً نوعاً ما؟ إن كنت تستطيع أن تجهزه بنفسك يمكن أن يكون أرخص بكثير على ما أعتقد، لكنك غني بالتأكيد."

في تشرين الأول/ أكتوبر 2010، أوجز القحطاني⁷¹ ما كان يبحث عنه في بوت IRC:⁷²


<https://hackforums.net/showthread.php?tid=161701> ⁶⁹

<https://hackforums.net/showthread.php?tid=707209> ⁷⁰

<https://hackforums.net/showthread.php?tid=741728&pid=7037024#pid7037024> ⁷¹

<https://en.wikipedia.org/wiki/botnet#irc> ⁷²

10-15-2010, 05:07 AM (This post was last modified: 10-15-2010, 05:09 AM by nokia2mon2)



nokia2mon2
[closed@HF:]

Posts:	441
Threads:	117
B Rating:	0 0 0
Popularity:	59
Bytes:	1.69
Game XP:	0

hi
i want buy private irc bot that:
1- very stable
2- fud
3- have all strong ddos function: http udp tcp syn super syn viset ect
4- spread by email and msn and usp.
5- downloader
6- work on all windows ver. xp vista 7 2003 2008 /// 32/64
Waite for your offers on that thread with the future of the bot

BR

بعد ذلك بأيام ظن القحطاني أنه دفع 250 دولار مقابل "آلاف البوتات العظيمة" التي لديها كل التجهيزات للقيام بهجوم عنيف لحجب الخدمة". باستخدام الاسم الأول للقحطاني في عنوان التدوين، كما هو ذكر سابقاً، وصف مستخدم يدعى ReIVloteIVlod صفقة مع القحطاني والتي قد تكون عملية احتيال.

ادعى ReIVloteIVlod أنه بعد أن دفع القحطاني ثمن بوتات على شبكة بوتات صديقه قام ذلك الصديق بحجبه. عرض ReIVloteIVlod إنشاء مخدّم IRC لشبكة بوتات مقابل 20 دولار بدلاً عن ذلك. "وعد بأنه سيدعم المخدّم بالكامل ويتأكد من أن البوتات لن تخسر وبأنه سيعطيني الدعم الكامل لكل شيء حتى تحديث تشفير البوت" أجاب القحطاني. حاول أيضاً توظيف ReIVloteIVlod: "وعدته بأنه عندما ننتهي سوف أعطيه راتب شهري".

وناقش القحطاني جهوده في المواقع المختصة بهجمات حجب الخدمة في عدة مناسبات. لكنه لم يسم يوماً المواقع التي استهدفها. في تشرين الثاني/ نوفمبر 2009، كتب أنه كان يواجه مشاكل في ممارسة هجوم حجب الخدمة على أحد المواقع بسبب قيام مدير الموقع بحظر الاتصالات من جميع البلاد إلا واحد: "قمت بالهجوم من بوتاتي لكن الموقع ما زال يعمل".⁷³ في كانون الثاني/يناير 2011، أوصى باستخدام Optima: "قمت بتعطيل موقع كبير باستخدام 300 بوت فقط .. جميع بوتات IRC الخاصة بي لا يمكنها تعطيله باستخدام 3-4 k (: مدّش".⁷⁴ في نفس الشهر طلب القحطاني المشورة حول كيفية اختراق أو شن هجوم حجب الخدمة غرفة PalTalk تضم حوالي 2000 عضو.⁷⁵ في آذار/ مارس 2012، وصف خدمة تُجرّج هجوم حجب الخدمة تسمى UncleSam بأنها "أكثر خدمة مهنية استخدمتها في هذا المجال، وسوف استخدمها مرات عديدة في المستقبل: D"⁷⁶ عطل القحطاني موقعاً لمدة 48 ساعة ودفع بالضحية إلى تغيير مقدم استضافة الموقع، بحسب تدوينته.

استهداف المستخدمين على أحد منصات وسائل الإعلام الاجتماعية الرئيسية، خدمة واتس آب

تماماً كما تقترح سمعته على أنه اليد العليا فيما يتعلق بوسائل الإعلام الاجتماعية في السعودية، دفع القحطاني مبالغ مالية لحذف حسابات، وسعى إلى خلق نشاط إعلامي على كبريات وسائل الإعلام الاجتماعية الرئيسية، بما في ذلك يوتيوب وفيسبوك. سعى أيضاً للحصول على أداة تسمح له بتعليق حسابات تويتر وحاول استخدام وسيلة كان من المفترض بها أن تعطل حساب واتس آب لأحد المستخدمين. كما أظهر القحطاني جانبه السطحي بالسؤال عن كيفية طرد لاعبين من لعبة على فيسبوك.

دفع للحصول على قناة يوتيوب، وحذف أكثر من 20 فيديو

سعى القحطاني إلى طرق مصطنعة لرفع شعبية حسابات وفيديوهات على يوتيوب وادعى أن كان وراء "حذف الكثير من الفيديوهات على يوتيوب وقناة واحدة على الأقل من الموقع.

⁷³ <https://hackforums.net/showthread.php?tid=181966&pid=1717326&highlight=ddos#pid1717326>

⁷⁴ <https://hackforums.net/showthread.php?tid=906835&pid=9248605&highlight=ddos#pid9248605>

⁷⁵ <https://hackforums.net/showthread.php?tid=975055&pid=9054188#pid9054188>

⁷⁶ <https://hackforums.net/showthread.php?tid=2827716&pid=26375253&highlight=ddos#pid26375253>

في تشرين الأول/أكتوبر 2010 اشترى القحطاني iTube 2.2، وهو بوت يوتيوب موسوم على أنه "أداة ترويج متخصصة على يوتيوب".⁷⁷ شملت الأداة عدداً كبيراً من الميزات، بما في ذلك "فيوز بوستر" (Views Booster) الذي يسمح للمستخدمين بزيادة عدد المشاهدات على الفيديو بشكل مصطنع باستخدام شبكة بوتات، و "ماس فلاجر" (Mass Flagger) التي تسمح للمستخدمين استخدام حساباتهم على موقع يوتيوب للإشارة إلى فيديو منافس وحذفه من يوتيوب.

بعد عام من ذلك، في تشرين الأول/أكتوبر 2011، بدأ بتدوينه تشير إلى أنه كان مهتماً بشراء ما بين 1000 إلى 2000 حساب معرف على يوتيوب. "سأغير كلمات السر لتصبح الحسابات لي وحدي.. بحسب ما كتب. "ضع عرضك رجاء. "لم يستجب أحد علناً على طلب القحطاني، ولكن في اليوم التالي كفل مستخدماً يدعى bloodgen قال القحطاني بأنه اشترى منه 500 حساب يوتيوب ولكن تلقى 78,525 وفي نفس التدوينه قال أنه اشترى حسابات من قبل مستعملين آخرين لكنها لم تعمل أو لم تكن "pva" (حسابات يتم التحقق منها بالهاتف (accounts verified-phone)). في اليوم السابق لذلك اشترى القحطاني أيضاً 6000 إعجاب على يوتيوب.⁷⁹ في شباط/فبراير 2012، حاول القحطاني دون جدوى أن يطلب 100 ألف مشاهدة على يوتيوب.⁸⁰

كما دفع القحطاني لأعضاء هاك فورم لحذف فيديوهات على يوتيوب وقناة واحدة على الأقل. في شباط/فبراير 2011، كفل القحطاني مستخدم يدعى ruNe0، والذي عرض حذف أي فيديو يوتيوب مقابل ما لا يزيد عن 6 دولارات. (عندما طلب منه حذف فيديو جستن بيير، اعترف ruNe0 أنه لا يستطيع: "ها ها ها، مستحيل! هذا الطفل مشهور جداً وشريكه أيضاً، سوف يحظرونني أنا = D"). وصف القحطاني ruNe0 بأنه "حذف لي العديد والعديد من الفيديوهات على يوتيوب .. كل الصفقات كانت سلسلة"⁸¹ بعد ذلك بشهر قام القحطاني بكفالة ruNe0 مرة أخرى وقال إنه "حذف أكثر من 20 فيديو" له.⁸² في تشرين الأول/أكتوبر 2011، أخبر القحطاني ruNe0 أنه أرسل له قناة جديدة لحذفها عبر رسالة خاصة، مما يشير إلى أن ruNe0 قد حذف على الأقل قناة واحدة للقحطاني في السابق.

في حزيران/يونيو 2013 بدأ القحطاني تدوينه بعنوان "احذف فيديو من يوتيوب \$200" قائلاً: "قل لي الوقت الذي تحتاجه للقيام بهذه المهمة، أردها في اسرع وقت ممكن."⁸³ بعد ذلك بيومين، كتب مستخدم يدعى Venture Mogul بأنه أزاله. أجاب القحطاني: "تحقق من حسابك على paypal، لقد حصلت على \$200 ... تحياتي"

في نيسان/أبريل 2016 بدأ القحطاني بتدوينه تشير إلى أنه كان يبحث عن شخص لبناء بوت يوتيوب يمكنه:⁸⁴

- 1- استخدام قائمة بالوكالة مع منافذ (الوكيل الخاص)
- 2- إظهار جميع الأسماء ويمكن تغييرها ودعم يونيكود
- 3- زيادة المشاهدات
- 4 - زيادة عدد الإعجابات/ عدم الإعجاب
- 5- التعليق من php واختيار إرساله أو حفظ في المكتبة ومن ثم يمكن إرسالهم جميعاً أو فقط ما يوجد عليه مربع اختيار

وحدد أن الأداة يجب أن تكون له فقط. لم يذكر في التدوينه ما إذا كان قد نجح في العثور على مبرمج للمشروع.

بحث عن أداة لحظر حساب تويتر

في حزيران/يونيو 2011، حاول القحطاني شراء أدوات تسمح له بحظر حسابات تويتر: "أريد شراء أدوات يمكن أن تمنع أو تجمد حساب تويتر. أي عرض⁸⁵؟ وبعد تلقي ردود قليلة كتب أنه سيدفع 500 دولار مقابل أداة من شأنها حتى "تجميد" حساب لمدة 24 ساعة إذا استطاع أن يفعل ذلك مراراً. اقترح أحد المستخدمين أن مثل هذه الأدوات غير موجودة "ولكن إذا كانت لديك قدرة على الوصول إلى قاعدة بيانات تويتر يمكنك أن تفعل أي شيء".

⁷⁷ <https://hackforums.net/showthread.php?tid=753917&pid=7256067#pid7256067>

⁷⁸ <https://hackforums.net/showthread.php?tid=749400>

⁷⁹ <https://hackforums.net/showthread.php?tid=945525&pid=16578821#pid16578821>

⁸⁰ <https://hackforums.net/showthread.php?tid=1873394&pid=19632477#pid19632477>

⁸¹ <https://hackforums.net/showthread.php?tid=910111>

⁸² <https://hackforums.net/showthread.php?tid=910111&pid=10332009#pid10332009>

⁸³ <https://hackforums.net/showthread.php?tid=3557857&pid=33357383#pid33357383>

⁸⁴ <https://hackforums.net/showthread.php?tid=5230150>

⁸⁵ <https://hackforums.net/showthread.php?tid=1431286&pid=13126931&highlight=twitter#pid13126931>

في نيسان/ أبريل 2012، سأل القحطاني عن أداة تخترق حسابات تويتر تباع بـ 20 دولار.⁸⁶ "ما مدى سرعتها؟ كم كلمة سر في الثانية تحاول اختراقها؟" وسأل أيضاً عما إذا كانت تستطيع تجاوز خاصية التحقق CAPTCHA.

في تشرين الأول/ أكتوبر 2018، ذكرت صحيفة نيويورك تايمز أن القحطاني كان المخطط الاستراتيجي وراء محاولة لمضايقة وإسكات منتقدي المملكة على تويتر باستخدام مزارع الترويض المكونة من مئات الشباب في الرياض ومحولها.⁸⁷ ذكرت الصحيفة أيضاً أن أحد موظفي تويتر، علي الزبارة، تم إقناعه من قبل المخبرات السعودية "على التدقيق في عدة حسابات، وفقاً لثلاثة أشخاص مطلعين على هذه المسألة." كان لدى الزبارة، الذي انضم إلى تويتر في عام 2013، القدرة على الوصول إلى المعلومات الشخصية للمستخدمين ونشاط الحساب، بما في ذلك عناوين بروتوكول الإنترنت (IP) وأرقام الهواتف. وتم طرده في عام 2015، على الرغم من أن تويتر لم يجد أي دليل على أنه زود الحكومة السعودية ببيانات من تويتر. وقد عاد إلى المملكة العربية السعودية ويعمل الآن في الحكومة، وفقاً لمصدر صحيفة التايمز.

امتلك "العديد من حسابات فيسبوك"

في شباط / فبراير 2011، بدأ القحطاني تدوينة بعنوان "نص أو برمجة لفيسبوك يمكنها أن تضيف الإعجاب والتعليقات على الآلاف من الحسابات." ⁸⁸ ليس من الواضح من التدوينة ما إذا كان يملك الآلاف من حسابات فيسبوك أو إذا كان يريد أداة تسمح له بالإعجاب والتعليق على الآلاف من الحسابات. حيث كتب "لدي العديد من حسابات فيسبوك". "أريد أفضل برمجة / نص يمكنني أن أدخل كل الحسابات عليه وأرسل الأمر من قبل البرمجة / النص.. ويمكنه أن يضع الإعجاب من كل الحسابات ويضيف تعليقات.."

بعد يوم من نشر التدوينة، كتب أنه كان "ما يزال بالانتظار."

اختبر أداة لاختراق واتس آب

أبدى القحطاني أيضاً اهتماماً بأدوات برنامج واتس آب. في كانون الأول/ ديسمبر 2014، كتب أنه حاول استخدام أداة من شأنها أن تخترق حسابات المستخدمين على واتس آب، ولكنها لم تعمل على iOS.⁸⁹

في أيار/ مايو 2015، بدأ بتدوينة يسأل فيها عن "أفضل منصة تحقق جماعي على واتس آب في السوق." ⁹⁰ رد مستخدمان، ولكن القحطاني لم ينشر مرة أخرى حول الموضوع.

أراد إخراج لاعبين من لعبة على فيسبوك، واشترى عملات للعبة بلياردو

كانت الإشارة الأخرى الوحيدة إلى فيسبوك في نيسان / أبريل 2013، عندما عرض دفع مبلغ 500 دولار من أجل نص من شأنه أن يظهر عنوان IP للاعبين في لعبة على فيسبوك تسمى (War Commander). "أحتاج برمجيات تبين لي عنوان IP للاعب في القطاع نفسه أو قطاع آخر باستخدام هويته أو اسمه. سادف 500 دولار لذلك، وقد أزيد ذلك المبلغ إن أعجبتني ما أراه. سأستخدمه لأخرج بعض اللاعبين السيئين (;)".

في تشرين الأول/ أكتوبر 2014، أشار أيضاً أنه اخترق لعبة بلياردو على iOS. في نفس اليوم عرض شراء جميع عملات لعبة البلياردو التي كان يبيعها أحد المستخدمين (2 دولار لكل مليون عملة)، وفي تدوينة أخرى في نفس اليوم عرض شراء حساب بلياردو بمليار عملة مقابل 700 دولار، على الرغم من أن مستخدم آخر ادعى بأنه باع مؤخراً حسابه ذي المليار عملة مقابل 25 دولار.

نشر آراءه عن الله وأوباما وكشمير

في أربع مقالات في 10 و 11 تشرين الأول/ أكتوبر 2010، نشر القحطاني رأيه في مواضيع لا علاقة لها بالقرصنة، بما في ذلك إيران وكشمير والدين. بدأ القحطاني تدوينة بعنوان "أوباما والسلطة الناعمة أو القوية أو الذكية.. ماذا سيعمل مع إيران؟" حيث وصف الرئيس أوباما آنذاك بأنه "زعيم إنساني حقيقي للأرض"، وجادل بأن الرئيس أوباما يحتاج إلى استخدام السلطة الناعمة والذكية والقوية عند التعامل مع إيران.⁹¹

<https://hackforums.net/showthread.php?tid=2424661&pid=21968194&highlight=twitter#pid21968194> ⁸⁶

[twitter.html-campaign-image-https://www.nytimes.com/2018/10/20/us/politics/saudi](https://www.nytimes.com/2018/10/20/us/politics/saudi) ⁸⁷

[pid=9894520#pid9894520&https://hackforums.net/showthread.php?tid=1065979](https://hackforums.net/showthread.php?tid=1065979) ⁸⁸

<https://hackforums.net/showthread.php?tid=4566034&pid=43622761#pid43622761> ⁸⁹

<https://hackforums.net/showthread.php?tid=4819790&pid=46116587#pid46116587> ⁹⁰

<https://hackforums.net/showthread.php?tid=732501&pid=6955346#pid6955346> ⁹¹

Obama and the soft or hard or smart power.. what will work with iran?

10-10-2010, 07:46 PM

i really respect the president Obama, he is a really humanity leader for the earth.
u remember that obama talk a lot about the soft power for America and Hillary Clinton talk a lot about the smart power. the president Bush dont believe in the 2. he just believe about the hard power.

on my opinion the wrong what the presdient Bush make that he use the hard power with iraq, he have did that for iran not for iraq if he just want to use it, he dont use the smart power smartly, and i think thats will work in iraq before 2003.

iran is On the contrary, i think president Obama need to use all the 3 powers Gradually.

i hope u all to read "Joseph Nye" book: the soft power. i read it translated to my language and i really interest on it.

for the guys who dont know the different between the 3 powers, pls make a search on the internet then tell us your opinions. im sure u will read the book after that.

BR

[closed@HF]

Posts:	441
Threads:	117
B Rating:	0 0
Popularity:	1.69
Bytes:	1.69
Game XP:	0

وفي تدوينة أخرى حول الهند وباكستان، قدم القحطاني رأيه حول نزاع كشمير: "الحل الوحيد هو منح شعب كشمير الحق في تقرير المصير تحت رعاية الأمم المتحدة، أو جعله أمة منفصلة".⁹²

وفي تدوينة أخرى عرض أفكاره عن الدين والسياسة:⁹³

الدين، مصدره هو العاطفة العارية من الاختيار الشخصي للفرد، علم العقل والتفكير هو الحقيقة المطلقة. أخطر تحدي للنظام العالمي الجديد هو سيطرة المواقف الدينية على القرار السياسي-السياسة والدين كلما التقيا كان إعلان الحرب.

في تدوينة بعنوان "أثبت وجود الله"، دعا⁹⁴ إلى حجة تعرف بـ "رهان باسكال"⁹⁵:

لا يمكن إثبات وجود الله علمياً كما لا يمكنك إنكار وجوده علمياً. هناك مفكر مشهور يدعى باسكال، قال كلمات جميلة: أنا أؤمن بوجود الرب لأن هناك احتمالين، أي منهما يمكن أن يكون موجوداً:
1- إن كان موجوداً فسيعطيني الجنة بعد أن أموت.
2- إن لم يكن موجوداً فلن أخسر شيئاً بتصديق قصته (:

نشر بينما كان ثملاً

كتب القحطاني أنه كان ثملاً في ثلاث تدوينات في نهاية عام 2010. الكحول غير قانوني في المملكة العربية السعودية ويعاقب عليه بالجلد أو ما هو أسوأ من ذلك، على الرغم من التقارير التي تفيد بأن بعض أفراد الأسرة المالكة قد انتهكوا الحظر دون عقاب.⁹⁶

في تشرين الأول/ أكتوبر 2010، رعى القحطاني مسابقة لأفضل دروس تتعلق بمجموعة من المواضيع، بما في ذلك البرمجة والرسوم البيانية والاختراق.⁹⁷ حصل الفائزون في المسابقة على ترقية في المنتدى اشتراها القحطاني. ورداً على رد الفعل الباهت على ما يبدو، كتب القحطاني أنه كان ثملاً وأراد دروساً تعليمية أفضل:

⁹² <https://hackforums.net/showthread.php?tid=720377&pid=6965503#pid6965503>

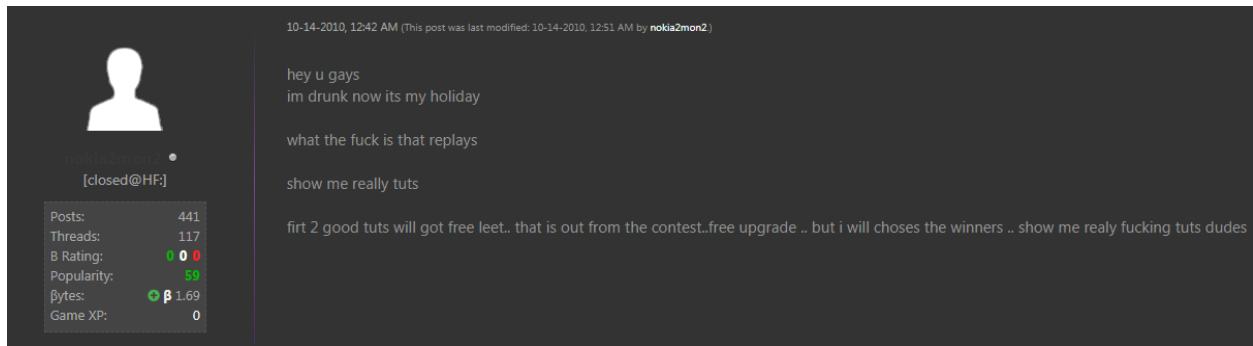
⁹³ <https://hackforums.net/showthread.php?tid=721169&pid=6965546#pid6965546>

⁹⁴ <https://hackforums.net/showthread.php?tid=305159&pid=6965603#pid6965603>

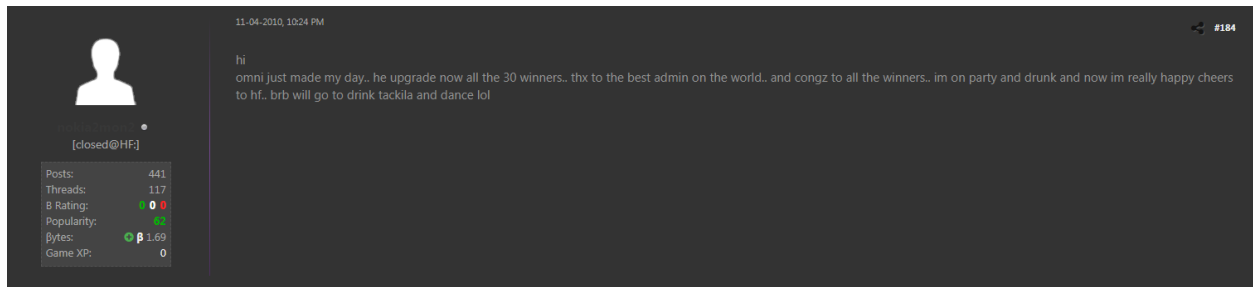
⁹⁵ <https://plato.stanford.edu/entries/pascal-wager/index.html>

⁹⁶ <https://www.theguardian.com/world/2010/dec/07/wikileaks-parties-princes-saudi-cables>

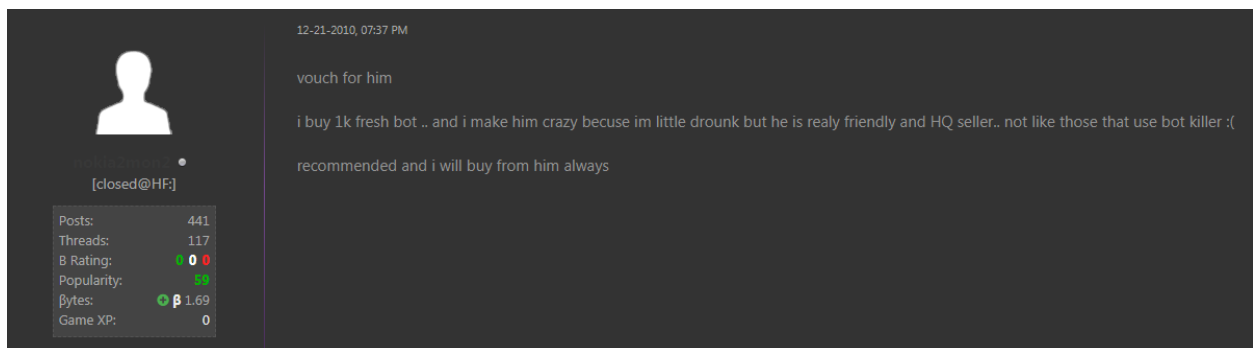
⁹⁷ <https://hackforums.net/showthread.php?tid=738021&pid=7014461#pid7014461>



في الشهر التالي رعى القحطاني مسابقة أخرى.⁹⁸ عندما انتهت المسابقة هنا القحطاني الفائزين وكتب: "أنا ثمل وأحتفل الآن، وأنا سعيد حقاً.. تحيات لهاك فورمز. سوف أذهب الآن لشرب التكيلا والرقص (لول)."



في كانون الأول/ ديسمبر 2010، كتب القحطاني أنه كان "ثملاً قليلاً" في تدوينة كفل فيها مستخدماً قال أنه اشترى منه 1000 بوت:⁹⁹



استخدم باي بال، وقدم عنوان بريد على هوتميل

كما رأينا في الصورة في بداية هذا القسم، كتب القحطاني في أول تدوينة له على هاك فورمز أنه استخدم باي بال لشراء برمجيات خبيثة من المستخدم stronger7. ذكر القحطاني بعدها في ما لا يقل عن اثنتي عشرة تدوينة أخرى استخدامه لباي بال في عمليات شراء مختلفة. وفي نيسان/ أبريل 2016، حدد أنه لا يستطيع الدفع إلا عن طريق باي بال أو فيزا.¹⁰⁰

وفقاً لتسرب المعلومات من موقع استعادة كلمة سر لدى باي بال فإن البريد الإلكتروني saudq1978@gmail.com متصل بحساب باي بال مرتبط بفيزا تنتهي برقم 10 ورقم الهاتف المحجوب جزئياً: *05 *** *750 والذي يتوافق مع رقم هاتف القحطاني من الشركة السعودية للاتصالات +966 55 548 9750.¹⁰¹

⁹⁸ <https://hackforums.net/showthread.php?tid=781348&pid=7485785#pid7485785>
⁹⁹ <https://hackforums.net/showthread.php?tid=914890&pid=8487820#pid8487820>
¹⁰⁰ <https://hackforums.net/showthread.php?tid=5230150&pid=50476121#pid50476121>
¹⁰¹ https://en.wikipedia.org/wiki/telephone_numbers_in_saudi_arabia

في تدوينة في كانون الأول/ ديسمبر 2010، سعى القحطاني لشراء 3000 تنزيل أو تحديث.¹⁰² كتب أنه سيدفع عن طريق "بي بي فقط"، مشيراً إلى باي بال. وقدم أيضاً عنوان بريد إلكتروني جديد: nokia2mon2@hotmail.com نشر عنوان البريد الإلكتروني مرة أخرى على الأقل قبل ذلك بشهرين، في تشرين الأول/ أكتوبر 2010، عندما طلب من بائع مخدم ويندوز أداة خبيثة لإضافتها على MSN.¹⁰³

Nokia2mon2@hotmail.com متصل بحساب حي لمايكروسوفت وحساب سكايب باسم (test test 1). وفقاً لتسرب المعلومات من صفحة استعادة كلمة السر لدى مايكروسوفت لايف، فإن عنوان البريد الإلكتروني مرتبط برقم الهاتف المحجوب جزئياً (72*****72) وعنوان البريد الإلكتروني (al*****@hotmail.com) التي لم يتم تحديدها خلال هذا التحقيق.

دفع 1500 دولار لإختراق حسابات هوميل

استأجر القحطاني أعضاء هاك فورمز لاختراق حسابات هوميل محددة وتزويده بتفاصيل الدخول. في تشرين الأول/ أكتوبر 2010، بدأ تدوينة عرض فيها دفع 300 \$ مقابل كلمة المرور إلى حساب هوميل.¹⁰⁴ بعد ذلك بعشرة أيام، كتب أن العديد من المستخدمين حاولوا ولكن فشلوا في اختراق الحساب. "ليست لدي أي معلومات عن الحساب، فقط هوية الحساب، إذا كان هناك شخص قادر أن يفعل ذلك فليبعث لي برسالة خاصة."

في آذار/ مارس 2012، بدأ القحطاني تدوينة يطلب فيها اختراق ثلاثة حسابات هوميل، وعرض دفع 500 دولار لكل حساب.¹⁰⁵ قام بتحرير التدوينة بعد ستة أيام مشيراً إلى نجاحه: "اخترقت حسابات البريد الإلكتروني"، "العرض انتهى."

بعد ذلك بأيام، كتب القحطاني أن مايكروسوفت طردته من أحد حسابات هوميل التي اخترقها. وقد نشر الرسالة التي تلقاها والتي تضمنت النص التالي "غالباً ما يأتي الزبائن إلى هنا لأن شخصاً آخر لديه صلاحية الوصول إلى حسابك ويستخدمه دون علمك لإرسال رسائل مزعجة." وقال القحطاني أن عنوان IP الخاص به كان في نفس بلد صاحب الحساب الأصلي وبأنه يعرف عن صاحب الحساب "اسمه واسم مدينته فقط." لم يقل ما إذا تمكن من العودة إلى الحساب الذي قام باختراقه.

حاول اختراق الشبكات اللاسلكية، نشر أول برنامج نصي

أظهر القحطاني اهتماماً في اختراق الشبكات اللاسلكية (مثل الواي فاي) ابتداء من عام 2011. في أيلول/ سبتمبر 2011، استجاب لتدوينة من قبل مستخدم يدعى Middle، والذي عرض بيع مهارات القرصنة الخاصة به أو تعليم الآخرين مقابل رسوم.¹⁰⁶ كتب القحطاني أن Middle أعطاه "دروس عظيمة" حول اختراق اللاسلكي.

بعد شهرين، في نوفمبر/ تشرين الثاني 2011، بدأ القحطاني تدوينة شرح فيها أن أداة اختراق الشبكات اللاسلكية Pyrit لم تقرأ له بطاقة الرسومات، وعرض 20 دولار لمن يمكن "إصلاحه لي (من قبل التلفزيون) و تبيان ما هو الخطأ وكيف يمكن استخدام Pyrit."¹⁰⁷

وأشار القحطاني إلى أنه كان يستخدم BackTrack 5 R، وهو سلف اختبار الاختراق من لينوكس Kali Linux. بعد ذلك بأيام، نشر تدوينة يطلب فيها المساعدة مع oclhashcat، أداة لاختراق كلمات السر.¹⁰⁸ وفقاً لمخرجات الأداة، التي وضعها القحطاني في تدوينته، كان نظامه يسخن بينما كان يحاول اختراق كلمة سر لشبكة واي فاي (WPA/WPA2)، مما أدى إلى إلغاء الأداة.

¹⁰² <https://hackforums.net/showthread.php?tid=890641&pid=8276669#pid8276669>

¹⁰³ <https://hackforums.net/showthread.php?tid=746882&pid=7144180#pid7144180>

¹⁰⁴ <https://hackforums.net/showthread.php?tid=713739&pid=6781390#pid6781390>

¹⁰⁵ <https://hackforums.net/showthread.php?tid=2303129&pid=20776371#pid20776371>

¹⁰⁶ <https://hackforums.net/showthread.php?tid=1700336>

¹⁰⁷ <https://hackforums.net/showthread.php?tid=1899278&pid=17200084#pid17200084>

¹⁰⁸ <https://hackforums.net/showthread.php?tid=1907397&pid=17267259#pid17267259>

```
Status.....: Running
Input.Mode...: Piped
Hash.Target..: Hall+Bed+Setting
Hash.Type....: WPA/WPA2
Time.Running.: 2 mins, 20 secs
Time.Util....: 140095.0ms/2682.3ms Real/CPU, 2.0% idle
Speed.....: 311.6k c/s Real, 322.5k c/s GPU
Recovered....: 0/1 Digests, 0/1 Salts
Progress.....: 43646976
Rejected.....: 0
HW.Monitor.#1: 91% GPU, 90c Temp
HW.Monitor.#2: 91% GPU, 89c Temp
HW.Monitor.#3: 91% GPU, 85c Temp
HW.Monitor.#4: 91% GPU, 83c Temp
```

ERROR: Temperature limit on GPU 1 reached, aborting...

any idea how to fix that and make it stable 100% ..

please answer me with details im new in that

Regards

أنهى القحطاني التدوينة بقوله أنه جديد على اختراق شبكات اللاسلكي: "رجاء أجبني بالتفاصيل أنا جديد في ذلك." بعد ذلك بثلاث سنوات في كانون الأول / ديسمبر 2014، شارك القحطاني¹⁰⁹ برنامج نصي صغير لمساعدتك على اختراق "WPA/WPA2" و نشر رابط إلى تدوينة Pastebin¹¹⁰ بعنوان (Red Lions WPA/WPA2 Cracker V1 BETA) (كانت ريد لايونز مجموعة على هاك فورمز يرأسها القحطاني).

وكتب في تعليقات البرنامج النصي أنه كان أول برنامج يكتبه وأنه كان "الغرض اختبار الاختراق فقط." خلق القحطاني تدوينة Pastebin باستخدام حساب مع نفس اسم المستخدم الذي يستخدمه على هاك فورمز: nokia2mon2¹¹¹. تم إنشاء الحساب في نفس اليوم الذي شارك فيه النص في هاك فورمز، ولم يكن هناك تدوينات أخرى تحت حسابه.

سعى للحصول على برمجيات تجسس على iOS

في 2014 و 2015 طلب القحطاني أدوات قرصنة لمنتجات أبل. في آذار/ مارس 2014، نشر تدوينة سأل فيها عما إذا كانت هناك أية راتس يمكن أن تصيب أجهزة ماك¹¹². ذكر بعض المستخدمين جيه رات لكنهم أشاروا إلى أنه لم يعد يباع. وكما كان الحال في كثير من الأحيان، كان طلب القحطاني لا يحتمل الانتظار: "أي خيار آخر يا رفاق؟؟؟؟ أحتاجه الآن"

¹⁰⁹ <https://hackforums.net/showthread.php?tid=4580080&pid=43766880#pid43766880>

¹¹⁰ <https://pastebin.com/A7HMFWDWQ>

¹¹¹ <https://pastebin.com/u/nokia2mon2>

¹¹² <https://hackforums.net/showthread.php?tid=4114113&pid=38887802#pid38887802>

في تشرين الأول/ أكتوبر من نفس العام، بدأ مستخدم يدعى Sam Sung تدوينه وصف فيها رؤية تطبيق تجسس على جهاز الأيفون 5 التابع لصديقه. قال Sam Sung فيما كان واضحاً أنه تدوينه احتيالي، أنه حاول العثور على برمجية تجسس على الإنترنت، لكن صديقه قال أن المطور يريد أن يبقى بعيداً عن الأنظار ليبيقيه مخفياً عن آبل. كان القحطاني أول من علق على الموضوع، وكتب: "إذا تمكنت من العثور عليه سوف اشتريه وسوف أعطي مكافأة إضافية إذا عمل بشكل صحيح".¹¹³ رد Sam Sung في اليوم التالي، "مرحباً، نعم وجدته، من فضلك أرسل لي تفاصيل سكايب الخاص بك برسالة خاصة."

حاول شراء حركة زائفة لموقع لمتابعي تويتر

في كانون الثاني/ يناير 2012، نشر القحطاني تدوينه طلب فيها شراء 100,000 زيارة لـ "صفحة على http://twitemail.com" وحدد أن التسليم يجب أن يكون في غضون 24 إلى 48 ساعة¹¹⁴. "لا يهمني إذا كانت وهمية.. يجب فقط أن يزيد العداد." Twitemail.com كانت ولا تزال مسجلة باسم صالح الزيد في الرياض، وفقاً لسجلات Whois. النطاق يعيد التوجيه إلى twitemail.com والذي يملكه أيضاً الزيد. يسمح Twitemail للمستخدمين مشاركة بريدهم الإلكتروني على تويتر، وفقاً للموقع.

زيد هو "شريك إستراتيجي تكنولوجي" لمايكروسوفت في الرياض، وفقاً لملفه الشخصي على لينكد إن.¹¹⁵ وهو أيضاً المدير التنفيذي لشركة LunarApps، وهي شركة أسسها في عام 2011. Twitemail هو واحد من منتجات LunarApps الرئيسية الثلاثة. الاثنان الآخران هما Untiny.com — موسع الروابط المختصرة — و TwtBase.com وهو "فهرس خاص لتطبيقات تويتر في السوق" وفقاً لصفحة زيد على لينكد إن.

الزيد¹¹⁶ والقحطاني يتبعان بعضهما البعض على تويتر.

سعى للحصول على مخدّم مخصص في روسيا أو الصين لاستضافة أعمال الاختراق وشبكة البوتات

في عام 2010، سأل القحطاني مرتين عن شراء خوادم لاستضافة أعمال الاختراق¹¹⁷ وشبكات البوتات. في تشرين الأول/ أكتوبر، بدأ بتدوينه في المنتدى الفرعي Buyers Bay بعنوان: "استضافة ذلك سيكون استضافة نظام اختراق وشبكة بوت."¹¹⁸ تدوينته ذكرت المختصر المفيد: "أود أن أشتري استضافة مضادة للبرصا ستأوي نظام اختراق وشبكة بوت." بعد ذلك بتسعة أيام، قال مستخدم أنه يمكن أن يوفر استضافة جيدة، ولكن بعد أقل من شهرين، في كانون الأول/ ديسمبر، نشر القحطاني تدوينه أخرى مع نفس الطلب: "بحاجة إلى مخدّم مخصص لشبكة بوتات وأنظمة اختراق."¹¹⁹

توسع القحطاني في شرح ما كان يبحث عنه قائلاً أنه يريد مخدّم مخصص يقع في روسيا أو الصين. "إذا كنتم تعرفون أي شركة جيدة توفر خادم مخصص وتسمح بشبكة بوتات IRC وأنظمة اختراق وما إلى ذلك يرجى إضافة الروابط في التعليقات..". تلقت هذه التدوينة الثانية ضعف عدد الردود، حيث قال أحد المستخدمين أنه أرسل له رسالة خاصة، وحذره آخر من أن مثل هذه الخوادم يمكن أن تكون مكلفة، ولكن "فيما يتعلق بروسيا تحقق من wahome.ru".

في الواقع، كان القحطاني يستخدم خدمة استضافة في الولايات المتحدة، وهي ThePlanet.com، الذي كان له سمعة إظهار استمرار سلوك ضار، مثل استضافة شبكة بوتات أو مواقع تنزيل المرور العابر.¹²⁰ يقدم القسم التالي تفاصيل عن البنية التحتية للاستضافة التي امتلكها القحطاني.

¹¹³ <https://hackforums.net/showthread.php?tid=4473189&pid=42687570#pid42687570>

¹¹⁴ <https://hackforums.net/showthread.php?tid=2167789&pid=19561996&highlight=vistes#pid19561996>

¹¹⁵ <https://www.linkedin.com/in/salehalzaid>

¹¹⁶ <https://twitter.com/alzaid>

¹¹⁷ [Exploit \(computer security\)/https://en.wikipedia.org/wiki](https://en.wikipedia.org/wiki/Exploit_(computer_security))

¹¹⁸ <https://hackforums.net/showthread.php?tid=713372&pid=6777840#pid6777840>

¹¹⁹ <https://hackforums.net/showthread.php?tid=927958&pid=8602127#pid8602127>

¹²⁰ <https://isps-bad-shaming-and-https://krebsonsecurity.com/2010/03/naming>

٧. النطاقات

يقيم هذا التحقيق بثقة متوسطة إلى عالية¹²¹ أن النطاقات الـ 22 التالية قد سجلها القحطاني منذ عام 2009:

- almalaky[.]com-aldewan
- sa[.]com-aldewan
- aldewanalmalaky[.]com
- aldewanksa[.]com
- aldewannews[.]com
- dewanmalaky[.]com
- fahadserver[.]com
- jasmn[.]info
- almalaky[.]com-aldewan-ksa
- library[.]com-kt
- news[.]com-sa-d-m
- dewan[.]com-markaz
- dewan[.]net-markaz
- royal[.]com-markaz
- royal[.]net-markaz
- ksa[.]com-royalcourt
- sa[.]com-royalcourt
- arabia[.]com-saudi-royalcourt
- almalaky[.]com-aldewan-sa
- saudidewan[.]com
- saudq[.]com
- saudqq[.]com

وأظهر القحطاني ضعفاً شديداً فيما يتعلق بأمنه التشغيلي عند تسجيل معظم هذه النطاقات. تظهر سجلات Whois أن جميع النطاقات ما عدا ثلاثة هي (saudq[.]com, saudqq[.]com و jasmn[.]info) تضمنت إما عنوان بريده الإلكتروني saudq1978@gmail.com أو رقم الهاتف المحمول +966 55 548 9750 أو تنويغات من اسمه الحقيقي.

وكانت ممارسات القحطاني خرقاء على نحو مماثل عندما تعلق الأمر بتسمية النطاقات الرئيسية والفرعية. وكما هو الحال مع حساباته على تويتر وجيميل، استخدم اسمه الأول والحرف الأول من اسمه الأخير لتسمية نطاقين، واستخدم نفس طريقة التسمية لما لا يقل عن ستة من النطاقات الفرعية. كما أنه استخدم حسابه على هاك فورمز للتعامل مع ما يبدو أنه أحد النطاقات الأكثر استخداماً من قبله، royal.com-markaz.

وقد استخدم العديد من النطاقات كخدمات للقيادة والتحكم للبرمجيات الخبيثة. ولم يبق من نطاقاته إلا اثنين فعالين لليوم وهما: saudq.com و jasmn.info. البقية انتهت صلاحيتها.

¹²¹ يمكن تقديم بيانات خاطئة أو غير دقيقة في سجلات Whois. ولذلك لدى هذا التحقيق ثقة متوسطة في ملكية القحطاني للنطاقات التي: 1- تم تحديدها في المقام الأول من خلال سجلات Whois التي تحتوي معلومات الاتصال بالقحطاني و 2- لم يتم تحديد أية أدلة متوافقة أخرى لها. لدى هذا التحقيق ثقة كبيرة في ملكية القحطاني لنطاقات تم تحديدها استناداً إلى أدلة متعددة ومتكاملة. إن الثقة المتوسطة في الحكم - بدلاً من أن تكون ثقة منخفضة - في ملكية القحطاني للنطاقات والتي تستند في المقام الأول على سجلات Whois ترجع إلى عدة عوامل: (أ) أدرج القحطاني اسمه ومعلومات الاتصال به في سجلات Whois للنطاقات (على سبيل المثال royal[.]com-markaz) مما يدفع هذا التحقيق للحكم بثقة عالية من أنها مملوكة من قبل القحطاني، بمعنى أن هذه الممارسة تتسق مع سلوك القحطاني المعروف؛ (ب) في هذا السياق نفسه، وباستخدام معلومات الاتصال أو غيرها من المعارف التي يمكن وصلها مباشرة به، تتسق مع ممارسات القحطاني الخرقاء، (ج) لم تتسرب معلومات الاتصال الخاصة بالقحطاني عند تسجيل النطاقات الأولى بالثقة المتوسطة (عام 2009)، بما يعني أن شخصاً بخلاف القحطاني كان يعرف عنوان البريد الإلكتروني للقحطاني ورقم هاتفه وموقعه مع الديوان الملكي السعودي وأراد إنشاء النطاقات باستخدام تلك المعلومات. يشير Parsimony إلى أن مسجل هذه المجالات كان القحطاني، الذي أظهر اهتماماً واضحاً في القرصنة والبنية التحتية لشبكة الإنترنت بحلول عام 2009، بدلاً من شخص مجهول بدوافع مجهولة.

وتجدر الإشارة إلى أن هذا القسم ليس شاملاً، كما أن البحوث بشأن البنى التحتية لشبكة القحطاني ما زالت جارية.

سجل أول 13 نطاقاً مع جيميل ورقم الهاتف الخليوي

ومن بين المجالات الـ 22 التي حددها هذا التحقيق، كان أول اثنين أنشأهما القحطاني هما (dewan[.]com-markaz و dewan[.]net-markaz)، والذين سجلا في 28 تشرين الأول/أكتوبر 2009. وقد أدرجت معلومات اتصال متطابقة، بما في ذلك بريد جيميل الإلكتروني الخاص بالقحطاني ورقم هاتفه، في سجلات Whois لكلا النطاقين. على سبيل المثال:

```
Registrant:
personal
P.O. Box 285292
Riyadh, 11323
SA

Domain name: ALDEWAN-ALMALAKY.COM

Administrative Contact:
User, Master saudq1978@gmail.com
P.O. Box 285292
Riyadh, 11323
SA
+966555489750
Technical Contact:
User, Master saudq1978@gmail.com
P.O. Box 285292
Riyadh, 11323
SA
+966555489750

Registrar of Record: The Planet Internet Services, Inc.
Record last updated on 01-Sep-2009.
Record expires on 01-Sep-2010.
Record created on 01-Sep-2009.

Domain servers in listed order:
NS2.THEPLANETDOMAINS.COM 207.218.223.162
NS1.THEPLANETDOMAINS.COM 207.218.247.135

Domain status: clientTransferProhibited
clientUpdateProhibited
```

من غير الواضح ما الذي كان مرتبطاً بصندوق البريد 285292 في الرياض في عام 2009. منذ عام 2015 على الأقل،¹²² استخدم نفس صندوق البريد من قبل شركة تسمى شركة عصور التقنية (Eras Technology Company)، التي تصف نفسها بأنها واحدة من شركات المقاولات الكهربائية والميكانيكية الرائدة في المملكة العربية السعودية.¹²³

ومن غير الواضح أيضاً كيف استخدم القحطاني dewan.net-markaz و dewan[.]com-markaz. ولكن بالقياس على تدويناته في هاك فورمز، فإنها يمكن أن تكون قد استخدمت لاستضافة شبكات البوت أو البرمجيات الخبيثة.

بعد أيام من تسجيل نطاقات dewan-markaz في 1 أيلول/سبتمبر، 2009، سجل القحطاني 11 نطاقاً آخر، تضمنت معظمها كلمة "ديوان" الذي يمكن أن يعني "مكتب" أو "دائرة رسمية". تضمنت بعض النطاقات تنويعات من "royalcourt":

• almalaky[.]com-aldewan

¹²² <https://web.archive.org/web/20150211204347/http://erastech.com/contactsus.aspx>
¹²³ https://erastech.com/?page_id=75476&lang=en

- sa[.]com-aldewan
- aldewanalmalaky[.]com
- aldewanksa[.]com
- dewanmalaky[.]com
- almalaky[.]com-aldewan-ksa
- news[.]com-sa-d-m
- ksa[.]com-royalcourt
- arabia[.]com-saudi-royalcourt
- almalaky[.]com-aldewan-sa
- saudidewan[.]com

تضمنت سجلات Whois للنطاقات الـ 11 نفس معلومات الاتصال الواردة في نطاقي dewan-markaz. على سبيل المثال:

```

Registrant:
personal
P.O. Box 285292
Riyadh, 11323
SA

Domain name: M-D-SA-NEWS.COM

Administrative Contact:
User, Master saudq1978@gmail.com
P.O. Box 285292
Riyadh, 11323
SA
+966555489750
Technical Contact:
User, Master saudq1978@gmail.com
P.O. Box 285292
Riyadh, 11323
SA
+966555489750

Registrar of Record: The Planet Internet Services, Inc.
Record last updated on 01-Sep-2009.
Record expires on 01-Sep-2010.
Record created on 01-Sep-2009.

Domain servers in listed order:
NS2.THEPLANETDOMAINS.COM 207.218.223.162
NS1.THEPLANETDOMAINS.COM 207.218.247.135

Domain status: clientTransferProhibited
clientUpdateProhibited

```

كما ذكر سابقاً، فإن النطاق الرسمي للديوان الملكي السعودي - royalcourt.gov.sa - لم يتم إنشاؤه حتى عام 2013. غير أن القحطاني كان يعمل في الديوان الملكي خلال هذه الفترة بمنصب مدير عام مركز الرصد والتحليل الإعلامي، والذي يجب ألا يخلط مع مركز الدراسات والشؤون الإعلامية في الديوان الملكي، الذي سيقترأسه القحطاني بعد ذلك ببضعة سنوات.

تم تحديد جميع النطاقات الـ 13 المسجلة في آب/ أغسطس وأيلول/ سبتمبر 2009 لتنتهي صلاحيتها بعد سنة من إنشائها، وذلك بحسب سجلات Whois. وهذا على الأرجح ما يفسر لجوء القحطاني إلى هاك فورمز في تشرين الأول/ أكتوبر وكانون الأول/ ديسمبر 2010 للاستفسار عن خدمات استضافة في روسيا والصين من شأنها أن تسمح له باستضافة شبكات بوت وبرامج اختراق.

وترك القحطاني 11 نطاقاً لتنتهي صلاحيتها في عام 2010، لكنه جدد تسجيل نطاقه dewan-markaz لمدة سنتين آخرين. وقد انتهت صلاحيتها في 29 آب/ أغسطس 2012 ولم يتم تسجيلها منذ ذلك الحين.

أدرج الاسم الحقيقي في سجلات Whois

بعد شهرين من السؤال حول مخدّمات مخصصة في هاك فورمز، سجل القحطاني fahadserver[.]com في شباط / فبراير 2010 وأدرج عنوان بريده الإلكتروني ورقم هاتفه بل واسمه الحقيقي في سجلات Whois:

```
Registration at: http://www.dnsExit.com
With Free Dynamic DNS services to allow running websites on home PC.

Domain:          fahadserver.com
Registration Date: 2010-02-16
Expiration Date: 2012-02-16

Registrant
saud alqahtani
saudq1978@gmail.com
worker
alsahafah
riyadh najd, 11545
+966.966555489750
SA

Administrative Contacts
saud alqahtani
saudq1978@gmail.com
worker
alsahafah
riyadh najd, 11545
SA
+966.966555489750

Billing Contacts
saud alqahtani
saudq1978@gmail.com
worker
alsahafah
riyadh najd, 11545
SA
+966.966555489750

Domain Name Servers
ns1.dnsExit.com
ns2.dnsExit.com
ns3.dnsExit.com
ns4.dnsExit.com
```

قبل ذلك بثلاثة أيام، في 13 شباط/ فبراير 2010، نشر القحطاني في هاك فورمز طالباً شراء 3000 بوت "من الولايات المتحدة أو كندا أو أوروبا أو الشرق الأوسط وتكون مستقرة وبسرعة فأنا على عجل".¹²⁴

انتهت صلاحية النطاق في شباط/ فبراير 2012.

استعمل nokia2mon2 كمنطقة فرعية لمخدم C2

في تموز/ يوليو 2010 استمر القحطاني في استخدام معلوماته الشخصية في سجلات Whois عند تسجيل النطاقات حين أنشأ royal[.]com-markaz تحت اسم "a q, saud" (كما ذكر أعلاه، الاسم الأوسط للقحطاني هو عبد الله، حيث وقع اسمه "سعود عبد الله" في واحدة على الأقل من رسائل البريد الإلكتروني إلى هاكنغ تيم).

كما أدرج القحطاني بريده الإلكتروني على جيميل ورقم هاتفه مرة أخرى بالإضافة إلى اسم شركة "saud co".

```
Registrant:
a q, saud saudq1978@gmail.com
saud co
riyadh
riyadh 11545
SA

Domain name: MARKAZ-ROYAL.COM

Administrative Contact, Technical Contact:
a q, saud saudq1978@gmail.com
saud co
riyadh
riyadh 11545
SA
+966555489750

Registration Service Provider:
(DynDNS) Dynamic Network Services, Inc. support@dyndns.com
Login to your account at http://www.dyndns.com/+domains/ to manage
nameservers and contacts for your domain name.

Record last updated on 12-Jul-2010 14:04:56 UTC.
Record expires on 12-Jul-2011.
Record created on 12-Jul-2010.

This domain is delegated to DynDNS.com Custom DNS:
NS5.MYDYDNS.ORG
NS2.MYDYDNS.ORG
NS3.MYDYDNS.ORG
NS4.MYDYDNS.ORG
NS1.MYDYDNS.ORG
100% uptime since 2001! ** Learn more here: http://www.dyn.com/ **

Domain status: clientDeleteProhibited
clientTransferProhibited
clientUpdateProhibited
```

لم يحدد هذا النطاق بعد عام، وانتهت صلاحيته في تموز/ يوليو 2011.

في آب/ أغسطس 2010، بعد أقل من شهر من تسجيله لـ royal[.]com-markaz، أنشأ القحطاني royal[.]net-markaz والذي سيستخدمه لاحقاً كمخدم للقيادة والتحكم (C2) لبلاكشيدز وغيره من البرامج الضارة. ولأول مرة، استخدم القحطاني خدمات الخصوصية على Whois بحيث لا يرتبط اسمه ومعلومات الاتصال به علناً بهذا النطاق. ونجح في تجديد تسجيل النطاق باستخدام خدمات الخصوصية لـ Whois في عام 2011، ولكن من كانون الثاني/يناير 2012 إلى آب/ أغسطس 2012، عندما انتهت صلاحية النطاق وخدمة حماية الخصوصية، أصبحت المعلومات الشخصية للقحطاني عامة:

```

Registrant:
a q, saud saudq1978@gmail.com
saud co
riyadh
riyadh 11545
SA

Domain name: MARKAZ-ROYAL.NET

Administrative Contact, Technical Contact:
a q, saud saudq1978@gmail.com
saud co
riyadh
riyadh 11545
SA
+966555489750

Registration Service Provider:
(Dyn) Dynamic Network Services, Inc. support@dyn.com
Login to your account at https://account.dyn.com/+domains/ to manage
nameservers and contacts for your domain name.

Record last updated on 12-Oct-2012 22:18:12 UTC.
Record expires on 01-Aug-2012.
Record created on 01-Aug-2010.

This domain is delegated to Dyn Standard DNS:
NS1.MYDYDNS.ORG
NS5.MYDYDNS.ORG
NS4.MYDYDNS.ORG
NS2.MYDYDNS.ORG
NS3.MYDYDNS.ORG
Industry leading uptime since 2001! ** Learn more here: http://dyn.com/ **

Domain status: pendingDelete

```

استخدم القحطاني العديد من النطاقات الفرعية لـ royal.net-markaz لاستضافة حملات خبيثة، واكتشف بأنها تشغل برامج خبيثة تعمل مثل بلاكشيدز وداركنس/ أوبتيما.¹²⁵ في مثال آخر على الممارسات الخرقاء، استخدم القحطاني اسم المستخدم الخاص به على هاك فورمز كنطاق فرعي royal[.]net-nokia2mon2.markaz

ذلك النطاق الفرعي أدرج ضمن قائمة بأكثر من 13000 مضيف حدهم مكتب التحقيقات الفدرالي على أنهم شاركوا في نشاط بلاكشيدز.¹²⁶ وعلى وجه التحديد، لوحظ أن النطاقات تلقت تحديثات للحالة أو شاركت في هجمات سابقة، وفقاً لإخطار غير مصنّف من القطاع الخاص.¹²⁷ كما أدرج royal[.]net-Nokia.markaz أيضاً في قائمة مكتب التحقيقات الفدرالي.

كما لوحظ بأن royal[.]net-Nokia.markaz يستخدم أيضاً لاستضافة "shell booter"، مما يسمح باستخدام مواقع إلكترونية مخترقة في هجمات حجب الخدمة.¹²⁸ كان عنوان بروتوكول الإنترنت (IP) الذي يسيّطيف النطاق الفرعي في ذلك الحين، 134[.]77.30.55، يعود لعنوان IP لمشارك منزلي مملوك من قبل شركة الاتصالات السعودية في الرياض، بحسب سجلات Whois.

تضمنت النطاقات الفرعية الأخرى royal[.]net-markaz الاسم الأول للقحطاني:

- royal[.]net-Saud.markaz
- royal[.]net-Saud2.markaz
- royal[.]net-Saud4.markaz

¹²⁵ [/bot-ddos-optima-darkness-the-inside-peek-https://www.webroot.com/blog/2012/03/08/a](https://www.webroot.com/blog/2012/03/08/a-bot-ddos-optima-darkness-the-inside-peek)

¹²⁶ [blackshadesdomains.txt-net/fbi.https://info.publicintelligence](https://info.publicintelligence.blackshadesdomains.txt-net/fbi)

¹²⁷ [/bulletins-blackshades-https://publicintelligence.net/fbi](https://publicintelligence.net/fbi/bulletins-blackshades)

¹²⁸ [royalnetshellbooter.html-https://www.exposedbotnets.com/2011/01/nokia2mon2markaz](https://www.exposedbotnets.com/2011/01/nokia2mon2markaz)

- royal[.]net-Saud5.markaz
- royal[.]net-Saud6.markaz
- royal[.]net-Saud9.markaz

برمجية خبيثة على ويندوز مرتبطة مع بوت روسي لتنفيذ هجوم حجب الخدمة مسمى داركنس أو أوبتيما تمت ملاحظتها وهي تتصل بثلاثة مضيفين: royal[.]net-saud4.markaz و royal[.]net-saud5.markaz و royal[.]net-saud6.markaz¹²⁹.

تم العثور على عنواني URL لـ royal[.]net-saud4.markaz في وايباك ماشين في تموز/ يوليو 2011 وآب/ أغسطس 2011: صفحة أسئلة شائعة روسية عن أوبتيما¹³⁰ و صفحة تسجيل الدخول على لوحة تحكم أوبتيما¹³¹ وفيما يلي مقتطفات من صفحة الأسئلة الشائعة، مترجمة إلى الإنكليزية باستخدام مترجم آلي:

What types of attacks does DDOS support ?

Starting from version 2.02 b, the bot supports three types of attacks ;

- **Intellectual attack by HTTP protocol** . All links are retrieved from the page, leading out of the site are filtered, then their call starts in a random order of 100 threads. Multiple parent URLs are supported. Attention, the presence of the http: // prefix in the command is **mandatory!**

An example of a simple command to attack : **dd1 = http://ya.ru**

Examples of the attacking team : **dd1 = http://ya.ru; http://mail.ru; http://rambler.ru** ; (the presence of the symbol " ; " after each url is **mandatory !**)

- **Date-Attack** . Generation of the maximum possible traffic to the host, in order to overuse traffic or use all the bandwidth of the communication channel at the host.

usage example : dd2 = host.ru

- **Thrash Attack** . An attack on host services, such as FTP for denial of service.

usage example : dd3 = host.ru: 21

How can I install the control panel?

Installation is as simple as possible; you just need to copy the files to the server, create a database, load a dump of data through PHPMyAdmin and set the data in include / config.php . Administrator and guest passwords are also set there. On the file config.php you need to install chmod 666 .

How to multiply the bot?

The easiest and most convenient way is installation services. All you need to do is pay for downloads and report the link on which the bot is located. We recommend using purchased installations only for tests, for work to organize your own.

Recommend where to buy quality downloads.

In our deep conviction to buy them is not possible. We advise to organize your own.

Yesterday I bought 3000 downloads, and today I have only 400 bots, why?

This is the norm. Discussion of download services is beyond the scope of this FAQ , but nevertheless the percentage of "survival rate" of about 15-20% can be considered successful. Read more about download services here .

تم برمجة برمجية خبيثة مرتبطة بـ (Nullbot)، كان القحطاني قد كفلها في هاك فورمز، للاتصال بـ royal[.]net-saud.markaz و royal[.]net-nokia2mon2.markaz¹³² كما أدرج اسم القحطاني الأول في اسم ملفين على الأقل من الملفات التي أنشأها البرنامج الخبيث عندما تم تنفيذه من قبل ضحية: NullBot_saud[.]exe و .02423B30[.]pf-NULLBOT_SAUD.EXE

مضيف آخر، royal[.]net-dan.markaz، تمت مراقبته¹³³ وهو يعمل كمخدم للقيادة والتحكم لبرمجية Zeus الخبيثة.¹³⁴

¹²⁹ https://www.virustotal.com/gui/file/df539e60a2c3c878cc6f0236d0ba7836a1ec1488b9e0320851e9d09d8a55e_b3e كشف

¹³⁰ <http://faq.html/royal.net:80-https://web.archive.org/web/20110820013508/http://saud4.markaz>

¹³¹ <http://royal.net:80/adm/auth.php-https://web.archive.org/web/20110718034435/http://saud4.markaz>

¹³² <http://security-reports/3815ec73533c286a25a0e5f2356f58e5.html-malware-research.dyndns.org/pub/botnet/ponmocup/tazerweb-http://security>

¹³³ <http://royal.net-https://zeustracker.abuse.ch/monitor.php?host=dan.markaz>

¹³⁴ <https://zeustracker.abuse.ch/faq.php>

بعد انتهاء صلاحية تسجيل royal[.]net-markaz في آب/ أغسطس 2012، لم تجدد مرة أخرى حتى تشرين الأول/ أكتوبر 2016، عندما قام ديف لوفتوس من أربور نتوركس سيكيورتي إنجينيرنج أند ريسپونس تيم (Arbor Networks Security Engineering & Response Team) في أن أربور في ميتشغن، بتسجيل النطاق وحوله إلى مجرى (sinkhole)¹³⁵ في sinkhole.net-arbor لمدة عام.

نطاقين فعالين متصلين بخدمة بريد إلكتروني مشفر

سجل القحطاني نطاقين هما saudq[.]com و jasmn[.]info يستخدمان هشميل، وهو خدمة بريد إلكتروني مشفر من الطرف إلى الطرف. كلا المجالان نشيطان، وإن لم يكن لأي منهما موقع نشط على شبكة الإنترنت. لم يتم العثور على أي موقع تاريخي لأي من هذين النطاقين على خدمات أرشفة الصفحات الإلكترونية. استخدم القحطاني عنوان البريد الإلكتروني saudq@saudq.com في عدة رسائل إلكترونية مع هاكنغ تيم. لم يتم التعرف على عنوان البريد الإلكتروني jasmn[.]info التابع للقحطاني.

في 14 تشرين الثاني/ نوفمبر 2014، نشر القحطاني تدوينة على هاك فورمز يعرض 100 دولار لشعار لـ "موقع وييميل" الخاص به الذي يتضمن كلمة "JASMN" ويشبه شعار هشميل.¹³⁶ "يمكنك أن تضيف فكرة تظهر أنه بريد إلكتروني آمن ومشفر" بحسب ما كتب.

نشر أعضاء هاك فورمز ما لا يقل عن اثني عشر مثلاً، بما في ذلك أمثلة عديدة تضمنت النطاق العام الرفيع المستوى .com، والذي أصر القحطاني على أنه لم يكن ضرورياً: "لا حاجة لإضافة .com، إنه فقط: jasmn، ويجب إضافة شيء يظهر أنه آمن ومشفر." في اليوم التالي، اختار فائزين، أحدهما كان هذا الشعار:¹³⁷



سبب عدم رغبة القحطاني في تضمين jasmn في الشعار كان لأنه سجل النطاق jasmn[.]info، الذي أنشأ في 13 تشرين الثاني/ نوفمبر 2014، قبل يوم من طلبه للشعار في هاك فورمز. تم تحديد Jasmn[.]info عن طريق مراجعة تاريخ الاستضافة لدى saudq[.]com الذي يتشارك عنوان IP مع jasmn[.]info كما هو مفصل أدناه.

قد يكون القحطاني استخدم jasmn.info لإرسال واستلام البريد الإلكتروني. Jasmn.info لديه مخدمان من هشميل في plsmtp1.hushmail.com و plsmtp2.hushmail.com وكان من الممكن تأكيد أن القحطاني لديه حساب هشميل بفضل تسرب المعلومات من صفحة تسجيل الدخول لهشميل. محاولات الدخول مع عنوان بريدي غير صحيح ستعيد واحدة من الرسالتين التاليتين:

¹³⁵ [sinkhole/#gref-https://resources.infosecinstitute.com/dns](https://resources.infosecinstitute.com/dns-sinkhole/#gref)

¹³⁶ <https://hackforums.net/showthread.php?tid=4537112&pid=43323397#pid43323397>

¹³⁷ https://photobucket.com/gallery/user/demiedealsnegspace/media/cqf0adovamfzbg9nb196chnlzmwn_dfhns5w_bmc

<p>Email address</p> <p>⚠ Sorry, we don't recognize that email address</p> <input type="text"/> <p>e.g. jane@hushmail.com</p>	<p>Email address</p> <p>⚠ We don't recognize the domain yourdomain.com</p> <input type="text" value="email@yourdomain.com"/> <p>e.g. jane@hushmail.com</p>
---	--

استخدام عنوان البريد الإلكتروني للقحطاني، saud@saudq.com يؤكد أن عنوان البريد الإلكتروني والنطاق تم تسجيلهما لدى هشميل:

وطوال عمر هذا النطاق، الذي ينتهي في 13 تشرين الثاني/نوفمبر 2019، استخدم القحطاني خدمة الخصوصية من Whois التي تقدمها Dyn Inc الشركة التابعة لـ أوراكل. ولمدة أسبوع تقريباً، استضيف هذا المجال أصلاً على 216.146.39 [.]125، وهو مخدم مشترك مملوك لشركة Dyn التي تستضيف حالياً نحو 3900 نطاق. منذ 22 تشرين الثاني/نوفمبر 2014، تمت استضافة هذا المجال على 148.130.4 [.]52، وهو مخدم مخصص مملوك من قبل S-MOS Systems, Inc، وهي شركة منتهية كانت موجودة في سان خوسيه اشترتها إحدى شركات إيبسون الفرعية في عام 1998، وفقاً لملفات وزارة الخارجية في كاليفورنيا.¹³⁸

في نفس اليوم الذي تم فيه تحويل jasmn[.]info إلى 148.130.4 [.]52، تمت استضافة نطاق saudq.com الذي كان قد أنشئ قبل أسبوع من jasmn[.]info أيضاً على نفس المخدم. Saudq.com قام منذ ذلك الحين بتغيير المضيف مرتين: في آذار/مارس 2015 إلى مخدم مشترك في 216.146.39 [.]125 وفي أيار/مايو 2015 إلى 159.8.206 [.]68، والذي يستضيف نطاق آخر هو saudq[.]com.

وكما هو الحال مع jasmn[.]info، سجل القحطاني saudq[.]com مع خدمة الخصوصية Whois من Dyn، وهو حالياً فعال، وتنتهي صلاحيته في 7 تشرين الثاني/نوفمبر 2019.

استخدم نطاق Saudq كمخدم برمجيات خبيثة C2

Saudq[.]com، الذي تم إنشاؤه في نيسان/ أبريل 2015، كان لديه ما لا يقل عن 22 نطاق فرعي، بما في ذلك البعض مع روابط إلى وسائل الإعلام الاجتماعية ومنصات الرسائل مثل فيسبوك وإنستغرام وتلغرام:

- bot.saudqq[.]com
- botman.saudqq[.]com
- cpanel.saudqq[.]com
- am.saudqq[.]com
- quiz.saudqq[.]com
- codequiz.saudqq[.]com
- rsd.saudqq[.]com
- demo.saudqq[.]com
- ¹³⁹[redacted].saudqq[.]com
- tl.saudqq[.]com
- vote.saudqq[.]com
- w.saudqq[.]com
- ts.saudqq[.]com
- report.saudqq[.]com
- t1.saudqq[.]com
- proxy.saudqq[.]com
- xpress.saudqq[.]com
- tabeta.saudqq[.]com
- facebook.saudqq[.]com
- instagram.saudqq[.]com
- telegram.saudqq[.]com
- tam.saudqq[.]com

لا تزال البحوث جارية في هذه النطاقات الفرعية.

سجلات الرسائل النصية المستضافة على نطاقات فرعية مؤرشفة

في أيلول/ سبتمبر 2016، تم الحفاظ على نسختين من ملف نصي مستضاف على [redacted].saudqq[.]com وذلك من قبل واي باك ماشين، وتشمل ما يبدو أنها سجلات رسائل نصية من رموز التوثيق ذات العاملين، وإشعارات تسجيل الدخول وغير ذلك من الاتصالات المرسلة إلى حوالي اثني عشر رقماً هاتفياً في جميع أنحاء كندا.

يظهر التقاط أيلول/ سبتمبر 2016 سجلات ل 12 رسالة نصية للأرقام الكندية مع رموز منطقة كيبيك (450) ومانيتوبا (204). وقد أرسلت الرسائل من أرقام كندية مع رموز المنطقة لأونتاريو (705, 289) وتورونتو (647) ومونتريال (438) وألبيرتا (403). كل الرسائل هي رموز التحقق من واتس أب، باستثناء رمز تحقق واحد من جوجل:

¹³⁹ بعض المعلومات الواردة في هذا القسم تم حجبها للحفاظ على خصوصية الأفراد الذين يظهر بأن القحطاني استهدفهم.

```

Array
(
    [To] => 1450 [redacted]
    [From] => 1289 [redacted]
    [TotalRate] => 0
    [Units] => 1
    [Text] => WhatsApp code [redacted]

    You can also tap on this link to verify your phone: v.whatsapp.com/[redacted]
    [TotalAmount] => 0
    [Type] => sms
    [MessageUUID] => [redacted]
)
Array
(
    [To] => 1450 [redacted]
    [From] => 1647 [redacted]
    [TotalRate] => 0
    [Units] => 1
    [Text] => Your Google verification code is [redacted]
    [TotalAmount] => 0
    [Type] => sms
    [MessageUUID] => [redacted]
)

```

في تشرين الأول/أكتوبر 2016 تم النقاظ 142 رسالة نصية تم إرسالها إلى أرقام كندية مع رمز المنطقة 450 من كيبك. استهدفت خمسة أرقام فقط، منها رقمان تراسلا مرة واحدة، وواحد تلقى رسائل 17 مرة، وآخر تلقى رسائل 47 مرة، وآخر تلقى رسائل 76 مرة. وتباين مضمون الرسائل تبايناً كبيراً. كانت الرسائل التي تبدو وكأنها رموز أمنية أو تأكيدية قد أرسلت إلى كوينبائيس، ويتشات، إنستغرام، مايكروسوفت، في كي، واتس آب، ستيم، إيربنب، فايبر، أيه أو إل.

تضمنت بعض الرسائل تحذيرات أمنية:

- "شخص ما يستبدل معلومات الأمان لحساب مايكروسوفت [redacted]@gmail.com. ليس أنت؟
"https://account.live[.]com/Proofs/Manage"
- "رمز التحقق: [محبوب]. استخدم الرمز فقط لإزالة القيود على ويتشات. لا تشاركه مع أي أحد."
- "تسجيل دخول غير اعتيادي على حساب مايكروسوفت [محبوب]. استعراض على https://account.live.com/a"

رسائل أخرى أشارت إلى ملفات أوبر:

- "أوبر: هل تحتاج مساعدة في إنهاء ملف أوبر الخاص بك؟ تعال لزيارتنا خلال ساعات عملنا في المكتب (help-t.uber[.]com/indy) أو أكد حضورك لجلسة تعريفية الليلة: t.uber[.]com/uber101indy"
- "أوبر: دردش مباشرة مع خبير إنديانابوليس أوبر الآن حتى 10:30 صباحاً! سوف نجيب على كل أسئلتك ونأخذك على الطريق في أقرب وقت ممكن: t.uber[.]com/chatlive6"
- "أوبر: [محبوب] عطلة نهاية الأسبوع هي أفضل وقت للحصول على قيادة كبيرة مع أوبر ألدك أسئلة؟ تعال لزيارتنا غداً في (99 E Carmel Carmel, IN -Dr, Suite 150) بين 12 و 5 عصرًا!"
- "أوبر: تابع العملية للشراكة مع أوبر بالموافقة على عملية فرز سائقينا على https://partners.uber.com أي أسئلة؟ زر help.uber.com"

وشملت الرسائل أيضاً رسائل مزعجة من شركة توصيل الغداء peachd.com وخدمة تأجير الأصدقاء rentafriend.com وشركة الألعاب leovegas.com لم تتضمن الرسائل المزعجة الأخرى الموجهة إلى شركات وخدمات وعروض أخرى أية وصلات.

وكانت الرسائل في ست لغات مختلفة بالإضافة إلى الإنكليزية:

- العربية (رمز التفعيل لحسابك في شباك هو)
- الصينية (谢谢 , [redacted] 请输入后进行验证 : 您申请的手机验证码是)
- التايلندية (ของคุณ Instagram เพื่อตรวจสอบยืนยันบัญชีผู้ใช้ [redacted] ใช้)
- الروسية (VK :Код подтверждения для входа на Вашу страницу ВКонтакте :[محبوب])
- الفرنسية (Collectionnez 6 bonus & vos 90% de l'offre du jour chez JackpotCity RDV sur www.jpwcw.[jin] (nous pour desinscription-avec sugarmine. Contactez
- الإسبانية (Usa el código [redacted] para quitar este teléfono de tu cuenta)

تم إرسال عنواني URL مختصرين في رسالتين. تم إرسال goo[.]gl/sUAPbz مع الرسالة التالية "أودع 25 دولار واحصل على ما يصل إلى 5000 دولار نقداً! أدخل إلى حسابك التجاري Trade360 الآن" يتسع عنوان URL إلى [https://www.trade360\[.\]com/en-gb/trading/?af_chrome_lp=true&af_sub1=English&h&c=PVnodeposit_Oct10&pid=SMS&af_channel=Email+Marketing&af_keywords=Con](https://www.trade360[.]com/en-gb/trading/?af_chrome_lp=true&af_sub1=English&h&c=PVnodeposit_Oct10&pid=SMS&af_channel=Email+Marketing&af_keywords=Con) version&view=trading.cashier. ولا واحدة من العشرات من الملفات التي تم التعرف عليها بواسطة VirusTotal والتي تشير إلى trade360[.]com تم الكشف عنها على أنها خبيثة.¹⁴⁰

عنوان URL المختصر الآخر، gl/T6ajlO[.]goo، تم إرساله مع الرسالة التالية "اكسب المزيد من PeNNeY لإجراء المكالمات الدولية عن طريق تطبيقك على جوجل بلاي". عنوان URL يتسع إلى [https://play.google\[.\]com/store/apps/details?id=net.penchat.android](https://play.google[.]com/store/apps/details?id=net.penchat.android)، وهي وصلة مينة إلى تطبيق أندرويد يدعى PeN Chat وهو تطبيق "حول كل شيء" بما في ذلك الرسائل، والصوت، ووسائل الاعلام الاجتماعية والتجارة الإلكترونية، وفقاً للموقع الإلكتروني للتطبيق، مما يشير إلى أنه تم إنشاؤه من قبل دارك ماتر أيه بي (Dark Matter AB) في السويد.¹⁴¹ دارك ماتر، التي لا يبدو أن لها صلة بشركة الاختراق¹⁴² الموجودة في الإمارات العربية المتحدة والتي تحمل نفس الاسم، قدمت إفلاسها عام 2018.¹⁴³

تطبيق بواسطة SaudQ متوفر للتنزيل

استضاف النطاق الفرعي [redacted].saudqq[.]com أيضاً صفحة تنزيل لـ "تيم ورك تايمر"، ظاهرياً تطبيق لتتبع وقتك أثناء العمل، وفقاً للقطعة مأخوذة في آب/ أغسطس 2017 للصفحة بواسطة واي باك ماشين.

"هل أطلت الساعة الخامسة مساءً برأسها القبيح قبل أن تتوقع ذلك؟ لا تفقد إحساسك بالوقت مرة أخرى مع تطبيق تيم ورك تايمر. ابق دائماً مسيطراً على عمك بنقرة بسيطة." تتضمن الصفحة التي تظهر علامة حقوق الملكية لـ "SaudQ 2017"، وصلات مينة للتنزيل على ويندوز ولينكس وماك.

¹⁴⁰ <https://www.virustotal.com/#/domain/trade360.com>

¹⁴¹ <http://www.penchat.net/about>

¹⁴² <https://www.reuters.com/article/us-idUSKCN1PO19O-mercenarys-s-u-of>

¹⁴³ <https://www.allabolag.se/5590127915/befattningar>

Teamwork Timer

Did 5pm ever roll its ugly head around the corner before you expected it to? Never lose track of time again with the Teamwork Timer app. Keep on top of your work with a simple click.



Windows

[Download \(x32\)](#) [Download \(x64\)](#)

نطاقان فرعيان استخدمتا لتويتر

تم استخدام النطاقان الفرعيان tl.saudqq.com و tam.saudqq.com لتويتر، اعتماداً على لقطات مؤرشفة للمستضيفين ملتقطة من قبل واي باك ماشين.

لدى النطاق الفرعي tl.saudqq.com العشرات من الدلائل التي تشير إلى تغريدات، كما التقطت بواسطة واي باك ماشين، بما في ذلك:

URL	MIME TYPE	FROM	TO	CAPTURES
http://tl.saudqq.com:80/tweets/index/621/1	text/html	Jul 19, 2017	Jul 19, 2017	1
http://tl.saudqq.com:80/auth/login	text/html	Jul 8, 2016	Jul 18, 2017	30
http://tl.saudqq.com:80/libraries/index/1	text/html	Jul 9, 2016	Jul 18, 2017	6
http://tl.saudqq.com:80/tweets/index/317/1	text/html	Apr 22, 2017	Jun 24, 2017	3
http://tl.saudqq.com:80/auth/logout	text/html	Jul 12, 2016	Jun 24, 2017	6
http://tl.saudqq.com:80/tweets/index/316/1	text/html	Apr 22, 2017	Jun 24, 2017	3
http://tl.saudqq.com:80/tweets/index/330/1	text/html	Feb 15, 2017	Feb 15, 2017	1
http://tl.saudqq.com:80/tweets/delete_selected	text/html	Feb 4, 2017	Feb 4, 2017	1
http://tl.saudqq.com:80/tweets/index/287/1	text/html	Feb 4, 2017	Feb 4, 2017	1
http://tl.saudqq.com:80/tweets/index/286/1	text/html	Feb 4, 2017	Feb 4, 2017	1
http://tl.saudqq.com:80/tweets/index/205/2	text/html	Sep 28, 2016	Oct 30, 2016	2

كل عناوين URL الملتقطة توجه إلى صفحة تسجيل دخول ليبرونز: ¹⁴⁴

استضاف النطاق الفرعي tam.saudqq[.]com لوحة تحكم "مدير حساب تويتر"، وفقاً لنسخة مؤرشفة من الموقع من شباط/ فبراير 2017.¹⁴⁵ في آذار/ مارس 2016، تم نشر سجل دردشة على Pastebin التي يبدو أنها تنشأ من فريق يعمل على مدير حساب تويتر. ستة أفراد مشاركون أو مذكورون في الدردشة، بما في ذلك مطور برمجيات مستقل موجود في اسطنبول، تركيا، وفقاً لحسابه الشخصي على لينكد إن.¹⁴⁶

ذكرت الدردشة المشار إليها استخدام قاعدة بيانات مونغو لمكتبات التغريدات وشملت عدة وصلات ميته الآن، مثل http://tam.saudqq.com/tweetlibraries تناول أحد أعضاء الدردشة "مطوري مشروع واتس آب"، ولكن لم تذكر أي تفاصيل عن مشروع واتس آب.

نطاق فرعي تجريبي مستخدم في إدارة الترجمة

نسخة محفوظة من النطاق الفرعي التجريبي demo.saudqq[.]com تصل إلى صفحة تسجيل الدخول على barebones في تموز/ يوليو 2017 وآب/ أغسطس 2017 التي اشتملت على عبارة "إدارة الترجمة".¹⁴⁷ التقطت واي باك ماشين أيضاً 54 عنوان URL للنطاق الفرعي، والتي شملت الدلائل مثل التقارير/ الإحصاءات/المصادر/إنشاء.¹⁴⁸ جميع عناوين URL تمت إعادة توجيهها إلى نسخة مؤرشفة من صفحة تسجيل الدخول المذكورة آنفاً باستثناء sys/suspendedpage.cgi-demo.saudqq[.]com:80/cgi والتي وصلت إلى صفحة مؤرشفة "account suspended".

النطاق الفرعي تابيتا متضمن في تحليل تويتر للبريد المزعج

لم تتم أرشفة النطاقات الفرعية codequiz.saudqq[.]com و tabeta.saudqq[.]com في وايباك ماشين، ولكن ظهرت في تدوين وتحليل الرسائل المزعجة على تويتر، على التوالي. عنوان URL يظهر المضيف codequiz.saudqq[.]com تم تضمينه في نصين تم نشرهما على Pastebin في آذار/ مارس 2016 و آب/ أغسطس 2016. التدوين الأول، بعنوان "CURL test code"، تضمنت عنوان URL http://codequiz.saudqq[.]com/quiz1/login.php. التدوين الثاني¹⁵⁰ كان بدون عنوان واشتمل على نفس عنوان URL. تم إدراج النطاق الفرعي tabeta.saudqq[.]com في تحليل عنوان URL مختصر لبريد مزعج على تويتر¹⁵¹ - تلقى المضيف أربع نقرات، وفقاً للبحث.¹⁵²

¹⁴⁵ <https://web.archive.org/web/20170212205754/http://tam.saudqq.com:80>

¹⁴⁶ قد حجبت الصلة بسجل الدردشة، الذي لا يزال متاحاً على Pastebin عند كتابة هذه السطور، لحماية خصوصية أعضاء الدردشة، لأن طبيعة عملهم وعلاقتهم بالقحطاني والحكومة السعودية لم تكن واضحة.

¹⁴⁷ <https://web.archive.org/web/20170718214736/http://demo.saudqq.com:80/login>

¹⁴⁸ [*/https://web.archive.org/web/*/demo.saudqq.com](https://web.archive.org/web/*/demo.saudqq.com)

¹⁴⁹ <https://pastebin.com/iQDek6Ya/>://https

¹⁵⁰ <https://pastebin.com/jvrCBykY>

¹⁵¹ Classification-<https://github.com/HarshShah1997/Spam>

¹⁵² Classification/blob/master/Result/ClicksByDomains.txt-<https://github.com/HarshShah1997/Spam>

انتهت صلاحية النطاق مؤخراً

عندما تم إنشاء [saudqq\[.\]com](http://saudqq[.]com) في نيسان/ أبريل 2015، استضيف على [159.8.206\[.\]](http://159.8.206[.]) 68، المخدم الحالي المخصص لـ [saudq\[.\]com](http://saudq[.]com) كما ذكر أعلاه. ذلك العنوان الإلكتروني مملوك لشركة Softlayer Technologies Inc، وهي مزود استضافة اشترتها شركة IBM في عام 2011، والتي مثل ThePlanet.com التي اندمجت مع Softlayer في عام 2010، كانت لديها سمعة بأنها لا تفعل ما يكفي لإبعاد المخربين عن شبكتها.¹⁵³ منذ آذار/ مارس 2016، استضيف [saudqq\[.\]com](http://saudqq[.]com) على [93.168.220\[.\]](http://93.168.220[.]) 54، المملوك من قبل شركة الاتصالات السعودية في الرياض، وفقاً لسجلات Whois.

استخدمت خدمة الخصوصية من Whois التابعة لـ Dyn طيلة حياة النطاق، والتي انتهت في نهاية نيسان/ أبريل 2019. ولم يتم إعادة تسجيله حتى تاريخ كتابة هذه السطور.

VI. حسابات أخرى

باستخدام معلومات الاتصال التي ثبتت ملكيتها من قبل القحطاني في القسم III، أمكن تحديد معلومات اتصال إضافية له وتحديد عدة حسابات مرتبطة بعناوين البريد الإلكتروني وأرقام الهاتف هذه.

"باحثٌ عن العقول الفذة" (headhunter) على لينكدإن

يملك القحطاني حساب لينكدإن بريميم تحت اسم "saud a" حيث يصف نفسه بأنه "باحثٌ عن العقول الفذة" (headhunter) مقره في المملكة العربية السعودية.¹⁵⁴ حيث تقول سيرته الذاتية: "أنا مهتم جداً بالمعلومات الأمنية وأتطلع لبناء فريق جيد في شركتي".

ولا يتفق تاريخ العمل والتعليم الواردين في الحساب مع السيرة الذاتية الفعلية للقحطاني. يشير حساب لينكدإن إلى أنه كان الرئيس التنفيذي لشركة "سعود سالم" منذ أيار/ مايو 2009، وأنه كان في السابق مدير عام في "دار أمن المعلومات" من 2008 إلى 2009 في الرياض. يشير حساب القحطاني أيضاً إلى أنه ذهب إلى جامعة الملك سعود من عام 1998 إلى عام 2003 وحصل على درجة البكالوريوس في "أنظمة أمن الكمبيوتر والمعلومات".

التحق القحطاني بجامعة الملك سعود، لكنه حصل على درجة البكالوريوس في القانون منها قبل الانضمام إلى دورة تدريب ضباط القوات الجوية السعودية الملكية.¹⁵⁵

استخدم القحطاني saudq1978@gmail.com لتسجيل الملف الشخصي.

شخصية مؤيدة لمبارك على فيسبوك

لدى القحطاني أيضاً حساب وهمي على فيسبوك تحت اسم أحمد محمد مصطفى، نشر عليه محتوى موالٍ لمبارك عام 2011.¹⁵⁶ هناك حد أدنى من المحتوى العام على الحساب. التفاصيل العامة الوحيدة عن "أحمد" في جزء About هي أنه درس في القاهرة، دفعة عام 1967.

بلعب دور أحمد، "مواطن مصري في نهاية حياته"، نشر القحطاني مذكرة من 700 كلمة باللغة العربية في أيلول/ سبتمبر 2011، تقارن طريقة معاملة الرئيس المصري السابق حسني مبارك، الذي كان يخضع للمحاكمة في ذلك الوقت بعد أن قدم استقالته، مع الملك فاروق الذي أُطيح به في عام 1952. وقال أنه، خلافاً للذافي، الذي قصف شعبه وتعلق بالسلطة، تنحى مبارك باحترام عن الحكم ولكن مع ذلك تلقى معاملة غير عادلة. (هذا، على أقل تقدير، تفسير لا يستند على التاريخ لاستجابة الحكومة المصرية للثورة المصرية عام 2011، والتي أدت إلى مئات الوفيات والآلاف من الإصابات).¹⁵⁷

حساب أحمد معجب بصفحة واحدة تسمى "أنا أسف يا ريس"¹⁵⁸، وهي مكرسة للدفاع عن مبارك. يتبع القحطاني حساب تويتر لتلك الصفحة (@AseFYaryes)، ولكن الحساب لا يتبع القحطاني بالمقابل.¹⁵⁹

المحتوى العام الوحيد الآخر المرتبط بشخصية أحمد التابعة للقحطاني هو تعليق على مقال لصفحة مؤيدة لمبارك بنفس المذكرة المؤلفة من 700 كلمة.¹⁶⁰

حساب فيسبوك متصل بعنوان البريد الإلكتروني nokia2mon2@gmail.com، الذي يتصل بدوره بهاتف القحطاني الجوال: +966 55 548 9750، وبريد جيميل saudq1978@gmail.com، وذلك وفقاً لتسرب المعلومات من ميزة استعادة كلمة السر لدى جوجل.

من المحتمل أن القحطاني استخدم nokia2mon2@gmail.com لإنشاء حساب مع خدمة استضافة الويب المجانية 000webhost، إذ أن عنوان البريد الإلكتروني هو واحد من 15 مليون سجل لعملاء سرقت أثناء اختراق في آذار/ مارس 2015. اسم المستخدم المرتبط بحساب 000webhost هو

¹⁵⁴ /15821bbb-a-https://www.linkedin.com/in/saud

¹⁵⁵ arabia-http://www.arabnews.com/node/1326371/saudi

¹⁵⁶ https://www.facebook.com/profile.php?id=100002908691104

¹⁵⁷ revolution of 2011#Deaths https://en.wikipedia.org/wiki/Egyptian

¹⁵⁸ https://www.facebook.com/pg/AseF.Yarayes

¹⁵⁹ https://twitter.com/AseFYaryes

¹⁶⁰ https://www.facebook.com/AseF.Yarayes/photos/a.127012047369717/194016860669235

"nokia2mon2"، وكان عنوان IP 94.98.168.57، وهو عنوان IP آخر لمشترك منزلي مملوك من قبل شركة الاتصالات السعودية في الرياض، وفقاً لسجلات Whois.

عنوان البريد الإلكتروني nokia2mon2@gmail.com متصل أيضاً بحساب تويتر، استناداً إلى تسرب المعلومات من صفحة تويتر لاستعادة كلمة السر، ولكن الحساب المحدد لم يتم تعيينه.

رقم الهاتف المحمول متصل بسناب شات، واتس آب، وسيجنال

بالإضافة إلى ارتباطه بحسابه على تويتر والعديد من حسابات البريد الإلكتروني، يتصل رقم هاتف القحطاني المحمول، +966 55 548 9750 أيضاً بحسابات على سناب شات و واتس آب وسيجنال. لا توجد معلومات عامة مرتبطة بحسابات القحطاني على واتس آب أو سيجنال، مثل نبذة شخصية أو صورة للحساب. حسابيه على سناب شات فارغ أيضاً، على الرغم من أن اسم المستخدم الخاص به يمكن أن يرى: "saudq197" - وليس saudq1978

رقم هاتف القحطاني متصل أيضاً بحساب فيسبوك لم يتم تحديده.

استخدم اسم Nokia2mon2 على عدة منتديات

على الأرجح استخدم القحطاني اسم المستخدم "Nokia2mon2" ست مرات على الأقل على منتديات التكنولوجيا والقرصنة. تشبه المشاركات في هذه المنتديات مشاركات القحطاني على هاك فورمز شكلاً ومضموناً؛ فهي مكتوبة بلغة إنجليزية ضعيفة، ويتضمن بعضها نفس الطريقة التي يختم بها تدويناته "مع أطيب التحيات"، كما تنطوي إلى حد كبير على موضوعات مماثلة، غالباً ما دارت حول محاولات قرصنة فاشلة وعروض مالية أكبر من المعتاد مقابل الحصول على المساعدة.

في نيسان/ أبريل 2012، نشر مستخدم يسمى nokia2mon2 تدوينة¹⁶¹ في منتدى فرعي مخصص لـ FaceNiff¹⁶²، وهو تطبيق على أندرويد يسمح للمستخدمين سرقة تفاصيل الدخول من حسابات فيسبوك وتويتر ويوتيوب وأمازون أو اختراق جلسات عبر Fi-Wi. حيث كتب: "يمكنه الإمساك بفيسبوك ويوتيوب لكنه لم يمكسك رسائل البريد الإلكتروني وتويتر." كما طلب المستخدم إضافة vBulletin إلى قدرات الأداة. نشر القحطاني حول vBulletin أربع مرات على هاك فورمز، بما في ذلك في نيسان/ أبريل 2012، قبل أسبوع من تدوينة FaceNiff، عندما اشتكى أن هجوم الرجل-في-الوسط الذي شنه على على ثلاثة صفحات لـ vBulletin لم ينجح.¹⁶³

بعد ذلك بثلاث سنوات، في أبريل/ نيسان 2015، نشر nokia2mon2 تدوينة على منتدى developers.com-xda عرض فيه دفع ما يصل إلى 2000 دولار لأي شخص يستطيع مساعدته على تجذير هاتف فيرتو أستر يعمل بنظام أندرويد.¹⁶⁴ وعندما سئل لماذا لم يشتر هاتفاً ثانياً ببساطة، أجاب: "أريد أن أجذر هذا الجهاز لأسباب شخصية جداً." أربعة صور لهاتف فيرتو كانت مرفقة بتلك التدوينة تشير البيانات الوصفية من الصور إلى أنها التقطت بأي فون 6 بلس. استخدم القحطاني كل من أجهزة iOS، وأندرويد لينشر على تويتر، ولكن في الأيام المحيطة بالتدوينة على developers.com-xda، استخدم جهاز أي فون:

¹⁶¹ <http://forum.paranoid.me/viewtopic.php?t=519>

¹⁶² <https://mashable.com/2011/06/02/faceniff>

¹⁶³ <https://hackforums.net/showthread.php?tid=2373744&pid=21445663&highlight=vbulletin#pid21445663>

¹⁶⁴ t3091843-2000-payprice-aster-vertu-rooting-developers.com/android/help/help-https://forum.xda



من المرجح أن القحطاني أيضاً وراء حسابات nokia2mon2 على LinuxQuestions.org¹⁶⁵, org.UbuntuForums¹⁶⁶, Hashcat.net¹⁶⁷ و BlackHatWorld.com¹⁶⁸. عنوان IP المرتبط بحساب nokia2mon2 على BlackHatWorld في خرق البيانات 2.90.233.17 — مملوك من قبل شركة الاتصالات السعودية في الرياض، وفقاً لسجلات Whois.

¹⁶⁵ [-second-the-installed-i-after-blank-desktop-open-not-places/8-newbie-https://www.linuxquestions.org/questions/linux/913004-help-pls-6990-radeon.html](https://www.linuxquestions.org/questions/linux/913004-help-pls-6990-radeon.html)

¹⁶⁶ [.1671-https://hashcat.net/forum/user.html](https://hashcat.net/forum/user.html)

¹⁶⁷ <https://ubuntuforums.org/showthread.php?t=1878282>

¹⁶⁸ [/https://www.blackhatworld.com/members/nokia2mon2.263630/](https://www.blackhatworld.com/members/nokia2mon2.263630/)

ومن المقرر أن تقدم كالامارد نتائج تحقيقاتها إلى مجلس حقوق الإنسان التابع للأمم المتحدة في 27 حزيران / يونيو 2019.¹⁷⁹ وستخاطب خطيبة الخاشقجي، خديجة جنغيز، المجلس أيضاً.

إن النتائج الواردة في هذا التقرير ليست شاملة، كما أن البحث في البنى التحتية الشبكية للقحطاني ما زال جارياً. بالإضافة إلى النطاقات الـ 22 التي تم تحليلها في الجزء V من هذا التحقيق، حددت العديد من النطاقات الأخرى التي قد ترتبط بالقحطاني ولكنها تحتاج إلى مزيد من البحث والتحليل. وستنشر أية نتائج إضافية في تقرير تابع.

[#وش تعرف عن النحل](#)

¹⁷⁹ <https://twitter.com/RobertMMahoney/status/1142400309223817216/photo/1>