أمير الذباب: تحقيق مفتوح المصدر حول سعود القحطاني

ترجمة وتحرير فريق نون بوست

قبل مداخلته عبر السكايب للإشراف على عملية قتل وتقطيع الصحفي السعودي "جمال خاشقجي"، كان سعود القحطاني، المُستشار رفيع المستوى لدى ولي عهد المملكة العربية السعودية محمد بن سلمان، يُدير أنشطة الديوان الملكي على شبكات التواصل الاجتماعي ويشرف على الدعاية وتنفيذ أوامر بن سلمان. ويشمل ملف أعماله أيضا عمليات قرصنة ومُراقبة منتقدي المملكة وولي العهد.

فيما يلي مُلخّص لنتائج التحقيق المُتعلقة بأنشطة القحطاني:

خلال سنتي 2012 و2015، حاول شخص يطلق على نفسه اسم القحطاني شراء أدوات المراقبة من شركة تجسس إيطالية تعرف باسم هاكنغ تيم. وفي الخامس من تموز/يوليو سنة 2015، تم الكشف عن المراسلات التي دارت بين الطرفين من قبل أحد المخترقين الذي يستخدم اسم "فنياس فيشر"، الذي سرق ونشر حوالي 400 جيغابايت من الوثائق الداخلية والشفرة المصدرية ورسائل البريد الإلكتروني التابعين للشركة.

في الحقيقة، يبدو أن عمليات تواصل القحطاني مع شركة برامج التجسس لم يقع الكشف عنها إلى حدود 29 أغسطس/آب 2017، عندما جرى إنشاء حساب على موقع التويتر باللغة العربية بدأ في نشر مقتطفات من رسائل القحطاني الإلكترونية التي كان يرسلها لشركة هاكنغ تيم. وقد ربط الحساب، الذي يستعمل @HIAHY كاسم للمستخدم ويحمل اسم "تاريخ وذكريات"، عناوين البريد الإلكتروني المستخدمة من قبل القحطاني بعدة حسابات أخرى متواجدة عبر الإنترنت.

لقد أشار هذا الحساب إلى أن عنوان البريد الإلكتروني الذي يستخدمه الشخص الذي يزعم أنه

القحطاني للتواصل مع شركة هانغ تيم،com.gmail@saudq1978، استخدم أيضا لتسجيل حساب تحت اسم "نوكيا2مون2" على موقع قرصنة شهير يعرف باسم "هاك فورمز"، الذي جرى اختراقه في يونيو/حزيران سنة 2011 من قبل مجموعة قراصنة "لولزسيك" الشهيرة.

علاوة على ذلك، كشفت تقارير أخرى قدمها موقع ماذربورد في أغسطس/آب من سنة 2018 أن رسائل شركة هاكنغ تيم المُسرّبة تضمنت عنواني بريد إلكتروني إضافيين كان يستخدمهما الشخص الذي يزعم أنه القحطاني وهما sa.gov.royalcourt@qahtani.s وcom.saudq@saudq.

في الواقع، لم يتمكن كل من حساب "تاريخ وذكريات" وموقع "ماذربورد" من إثبات أن القحطاني يمتلك عناوين البريد الإلكتروني التي تم تسريبها، على الرغم من أن كلاهما قدّم أدلّة استنتاجية مُقنعة تُؤكد أن القحطاني هو من أرسل رسائل البريد الإلكتروني لفريق هاكنغ تيم، وهو من يملك حساب نوكيا2مون2 على موقع هاك فورمز.

يتطرق هذا التقرير إلى عمليات الأبحاث والإبلاغ التي قام بها كل من حساب "تاريخ وذكريات" وموقع "ماذربورد" الذي ينقسم إلى سبعة أقسام. ويتضمن القسم الأول تلخيصا لأهم نتائج التقرير. أما القسم الثاني، فيقدّم سيرة مُختصرة لرحلة صعود القحطاني إلى السلطة ويلخص كيفية تورطه في مقتل خاشقجي. ويكشف القسم الثالث عن امتلاك القحطاني لعناوين البريد الإلكتروني في ملف تفريغ تابع لشركة هاكنغ تيم بالإضافة إلى رقم هاتف جوال (+966 55 548 9750) لم يتم الإبلاغ عنه سابقا، وظهر أيضا في رسائل البريد الإلكتروني التي تم تسريبها.

أما القسم الرابع من هذا التقرير، فيبحث في نشاطات القحطاني في موقع هاك فورمز بالتفصيل. ويقوم القسم الخامس بتحديد وتحليل شبكة من البنية التحتية للإنترنت يستخدمها القحطاني لأغراض ضارة. أما القسم السادس، فيؤكد أن بيانات الإتصال التابعة للقحطاني التي وقع الكشف عنها في القسم الثالث استخدمت للكشف عن تفاصيل إضافية حول نشاطاته على الإنترنت، على غرار إنشائه لحسابات وهمية على وسائل التواصل الاجتماعي. ويتطرق القسم الأخير من التقرير إلى دور القحطاني غير الواضح في جهود بن سلمان المستمرة لإسكات النقاد والمعارضين.

فيما يلي بعض النتائج الرئيسية للتقرير:

القحطاني صاحب بيانات الاتصال المنسوبة إليه في بيانات هاكنغ تيم المسربة

في الواقع، يمتلك سعود القحطاني عناوين البريد الإلكتروني com.gmail@saudq1978 وsau@saud dq.comوs.qahtani@royalcourt.gov.sa بالإضافة إلى رقم الهاتف المحمول +966 55 548 9، الأمر الذي يؤكد أن القحطاني هو من تواصل مع شركة هاكنغ تيم لشراء أدوات التجسس خلال سنتي 2012 و2015.

علاوة على ذلك، استخدم الشخص الذي أطلق على نفسه اسم القحطاني في رسائل البريد الإلكتروني المُرسلة إلى هاكنغ تيم خلال سنتي 2012 و2015 عُنواني بريد إلكتروني وهما com.gmail@saudq1978 وcom.saudq@saud فضلا عن رقم هاتف +966 55 548 9750 الذين يمكن ربطهم بالقحطاني بشكل حاسم وذلك من خلال المعلومات المسربة من صفحات استعادة كلمة المرور الخاصة بغوغل وتويتر.

لقد استخدم الشخص نفسه عنوان البريد الإلكتروني sa.gov.royalcourt@qahtani.s للتواصل مع الشركة. وعلى الرغم من أنه لا يمكن إثبات ملكية القحطاني لهذا البريد الإلكتروني من خلال المعلومات المسربة من صفحات استعادة كلمة المرور، إلا أن هذا التقرير يحسم أن sa.gov.royalcourt@qahtani.s هو عنوان البريد الإلكتروني الحكومي الرسمي للقحطاني ويعزى ذلك جزئيا إلى أن رسائل البريد الإلكتروني التي يعود تاريخها إلى يونيو/حزيران 2015 مع ممثل الشركة استخدم خلالها البريدين الإلكترونيين التابعين للقحطاني، الأمر الذي كشف أن مالك الحسابين هو شخص واحد.

القحطاني يمتلك 22 نطاق إنترنت بعضها مخصص للبرامج الخبيثة والأخرى لهجمات حجب الخدمات

منذ سنة 2009، يمتلك القحطاني 22 نطاق إنترنت على الأقل استخدم البعض منها كخوادم للتحكم في البرامج الضارة:

الديوان-الملكي [.]كوم

الديوان-س أي [.]كوم

الديوان الملكي [.]كوم

الديوان كي اس آي [.]كوم

الديوان نيوز [.]كوم

ديوان ملكي [.]كوم

فهد سيرفر [.]كوم

جاسمن [.]أنفو

كي أس آي-الديوان-الملكي [.]كوم

كي تي-لابريري
[.]كوم
أم-دي-أس أي-نيوز [.]كوم
مركز-ديوان [.]كوم
مركز-ديوان [.]نت

مركز-رويال [.]كوم
مركز-رويال[.]نت
رويال كورت-كي اس آي [.]كوم
رويال كورت-أس آي [.]كوم
رويال كورت-العربية-السعودية [.]كوم
أس آي-الديوان-الملكي [.]كوم
ديوان سعودي [.]كوم
سعود كيو [.]كوم
سعود كيو كيو [.]كوم

على سبيل المثال، استخدم القحطاني العديد من النطاقات الفرعية التابعة لشبكة "مركز-رويال[.]نت" لاستضافة الحمولات الخبيثة، والتي وقع الكشف عنها على أنها برمجيات خبيثة وُضعت قيد العمل، على غرار بلاك شايدز، ودراكناس/أوبتيما. وأدرج المضيف "نوكيا2مون2.مركز رويال[.]نت" في قائمة تضم أكثر من 13 ألف مضيف حددها مكتب التحقيقات الفيدرالي على أنها تورطت في نشاط بلاك شايدز، كما لوحظ أنها تستضيف برنامج شال بوتر، الذي يتيح استخدام المواقع الإلكترونية المهددة بالاختراق لصالح هجمات الحرمان من الخدمات.

بالإضافة إلى ذلك، يوجد مجال فرعي آخر، وهو "سعود4.مركز-رويال [.]نت". لقد استضاف برنامج أوبتيما الضار، بناءً على اللقطات اللحظية التي التقطها "واي باك مشين"، والتي رصدت صفحة روسية للأسئلة الشائعة حول أوبتيما وصفحة تسجيل الدخول إلى لوحة تحكم في هذا البرنامج:

خلال شهري أيلول/ سبتمبر وتشرين الأول/ أكتوبر سنة 2016، حفظ موقع "واي باك مشين" تكرارين لملف نصي وقع استضافته على برنامج "سعود كيو كيو [.]كوم"، وأدرج ما يبدو أنه سجلات خدمة الرسالة القصيرة لرموز المصادقة ثنائية العوامل وإشعارات تسجيل الدخول وغيرها من الاتصالات المرسلة إلى حوالي 12 رقم هاتف في جميع أنحاء كندا.

تُظهر الصورة التي التقطتها الموقع خلال شهر أيلول/ سبتمبر 2016 سجلات 12 رسالة نصية قصيرة أُرسلت إلى أرقام هواتف كندية تحتوي على رموز منطقة كيبيك (450) ومقاطعة مانيتوبا (204). كما وقع إرسال الرسائل من أرقام هواتف كندية تحتوي على رموز منطقة أونتاريو (289، 705)، تورونتو (647)، مونتريال (438) وألبرتا (403). فضلا عن ذلك، تحتوي جميع الرسائل رموز تحقق واتساب، باستثناء رمز تحقق غوغل وحيد (وقع تنقيح معلومات التعريف الشخصية):

تحتوي الصورة التي التقطها الموقع خلال شهر كانون الأول/ أكتوبر من 2016 على 142 رسالة نصية قصيرة، وقع إرسالها إلى أرقام كنديّة مع رمز منطقة كيبيك 450. والجدير بالذكر أن خمسة أرقام فقط استُهدفت، حيث أُرسلت رسالة مرة واحدة لرقمين؛ وأُرسلت 17 رسالة لرقم آخر؛ فضلا عن أربعة رسائل أخرى لرقم مختلف؛ و76 رسالة لرقم رابع. وكان محتوى الرسائل مختلفا، حيث بدت كأنها رموز أمان أو تأكيد للعديد من المواقع والشركات والتطبيقات، على غرار كوينباس ووي شات وإنستغرام ومايكروسوفت وفكونتاكتي وواتس آب وستيم وإير بي إن بي وفايبر وآي أو أل.

بعض الرسائل تضمنت تحذيرات أمنية:

"شخص بصدد استبدال معلومات الأمان الخاصة بحساب مايكروسوفت [منقح] @ com.gmail، أليس أنت؟

"https://account.live[.]com/Proofs/Manage"

"رمز التحقق: [منقح]. يقع استخدام الرمز لإزالة القيود المفروضة على وي شات ولا تشاركه مع أي شخص".

"تسجيل دخول غير عادي لحساب مايكروسوفت [منقح]. راجع على https: // الحساب.

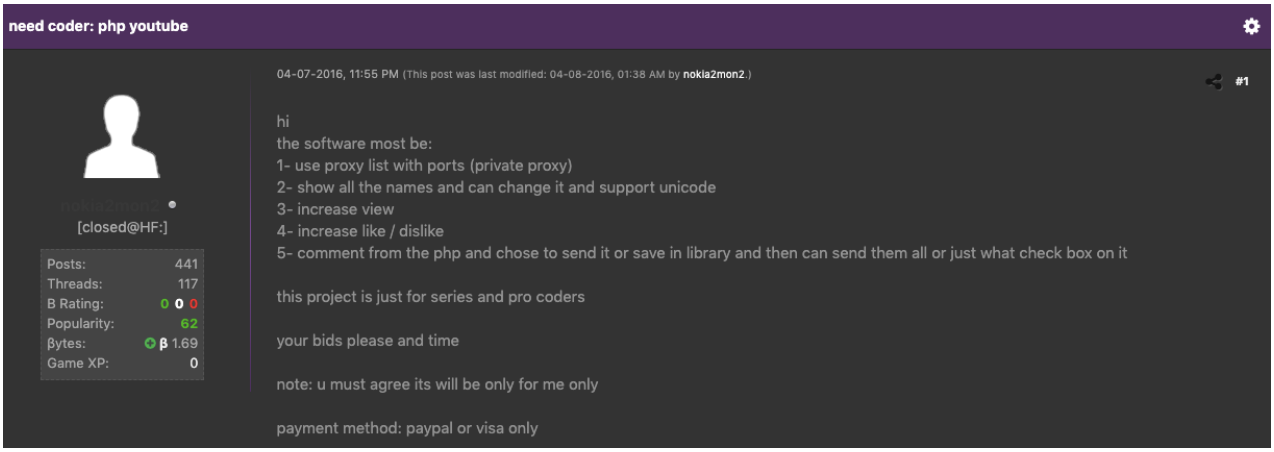
أظهر القحطاني ضعفًا في الأمن التشغيلي بشكل استثنائي عند تسجيله في جميع هذه المجالات تقريبا. وتتضمن سجلات "هوإيز" جميعها باستثناء ثلاثة (سعود كيو [.]كوم و "سعود كيو كيو [.]كوم" و"جاسمن [.]أنفو") إما عنوان بريده الإلكتروني الشخصي (com.gmail@saudq1978) أو رقم هاتفه المحمول (966 55 548 9750) أو متغيرات باسمه الحقيقي.

يوجد مجالين من المجالات المذكورة أعلاه فحسب نشطة في الوقت الراهن، وهي سعود كيو [.]كوم وجاسمن [.]أنفو.

كان القحطاني مستخدما نشطا في هاك فرومز، يشترى برامج تجسس، ويشارك منشورات وهو في حالة سكر

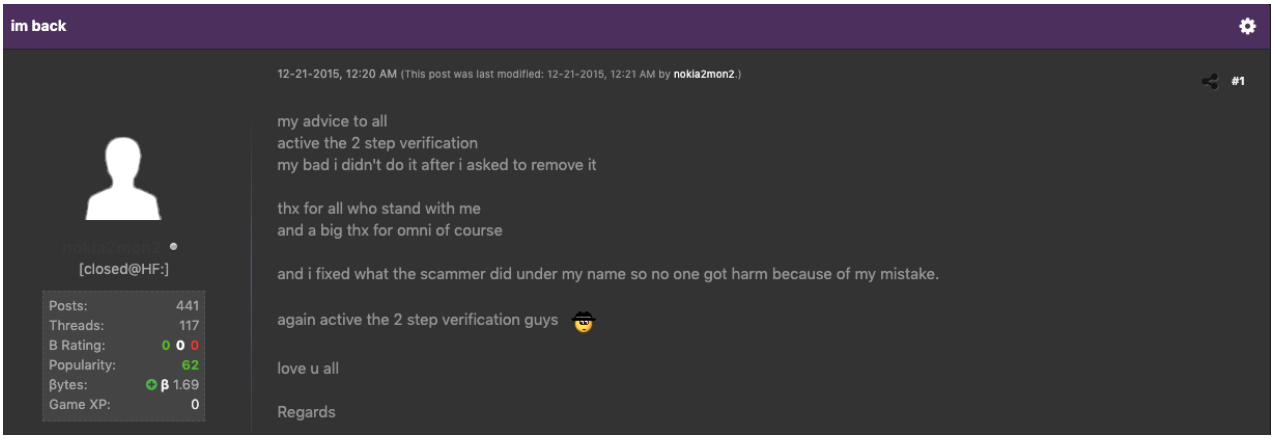
إن البريد الإلكتروني com.gmail@saudq1978 تابع للقحطاني، حيث يثبت حسابه على موقع "هاك فرومز" المسجل تحت عنوان البريد الإلكتروني، نوكيا2مون2، أنه ملك للقحطاني أيضا. وكان القحطاني يستخدم "هاك فرومز" بشكل نشط، حيث نشر أكثر من 500 منشور بين تموز/يوليو سنة 2009 وأيلول/سبتمبر سنة 2016.

وكان القحطاني يشارك بشكل مفصل منشورات على "هاك فرومز" يتناول فيها أدوات وخدمات الإختراق التي اشتراها واستخدمها ومنصات التواصل الاجتماعي وتطبيقات الجوال التي استهدفها. وبحلول حزيران/ يونيو سنة 2011، أي بعد مرور أقل من سنتين من انضمامه إلى هذا المنتدى، قدّر أنه يملك 90 بالمئة من أدوات الإدارة عن بعد المدفوعة والمجانية في السوق. وعموما، دفع القحطاني مقابلا ماديا لأعضاء "هاك فرومز" لحذف حساباتهم من مواقع التواصل الاجتماعي، كما سعى لتصنيع نشاط المشاركة على منصات التواصل الاجتماعي الرئيسية، بما في ذلك موقعي يوتيوب وفيسبوك.



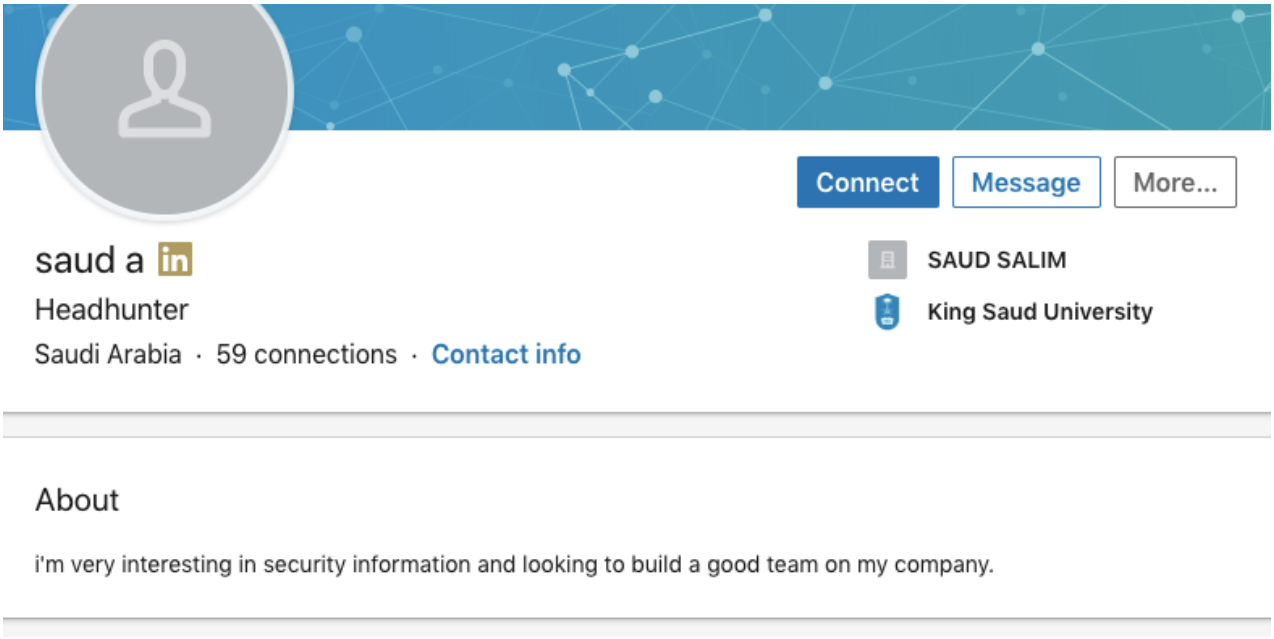
فضلا عن ذلك، شارك القحطاني منشورات في ثلاث مناسبات على الأقل وهو في حالة سكر، حيث اعترف بذلك بنفسه وركز على مواضيع لا علاقة لها بالاختراق، على غرار دور الدين في السياسة، والسياسة تجاه إيران.

وتجدر الإشارة إلى أن القحطاني وقع ضحية ثلاثة عمليات احتيال على الأقل أثناء نشاطه على "هاك فرومز". وفي كانون الثاني/ديسمبر سنة 2015، تعرض حسابه للاختراق لفترة وجيزة. وعندما استعاد السيطرة على حسابه، نصح زملاءه من أعضاء "هاك فرومز" بتمكين المصادقة الثنائية.



إنشاء حسابات وهميّة على لينكد إن والفيسبوك

من خلال استخدام قائمة الاتصالات التي يملكها القحطاني، كان من الممكن تحديد معلومات إضافية عن معارفه والكشف عن عدة حسابات مرتبطة بعناوين البريد الإلكتروني وأرقام الهواتف. وفي الحقيقة، يملك القحطاني أيضا حساب على لينكد إن بريمير تحت اسم "سعود ع" (علما وأن اسم القحطاني الأوسط هو عبد الله)، حيث يصف نفسه بأنه "قاتل مأجور" ومقره المملكة العربية السعودية.



علاوة على ذلك، أنشأ القحطاني حسابا شخصيا على الفيسبوك لشخص مصري من مؤيّدي مبارك تحت اسم "مواطن مصري في آخر سنوات حياته"، بالإضافة إلى بعض الحسابات الأخرى التي يملكها على سناب شات وواتساب وسيجنال.

الخلاصة

في الواقع، تضلّ سياسة القمع التابعة لمحمّد بن سلمان نشطة وفعّالة، ويرجع الفضل في ذلك إلى رفض إدارة ترامب محاسبة هذا الرجل السعودي القويّ ونظامه. فمنذ مقتل خاشقجي في تشرين الأو/لأكتوبر الماضي، أدّت وكالة المخابرات المركزية "واجبها في التحذير" خلال ثلاث مناسبات منفصلة، حيث تبادلت المعلومات الاستخباراتية لتنبيه المعارضين المتمركزين في الولايات المتحدة وكندا والنرويج من التهديدات القادمة من السعودية.

من جهة أخرى، تضلّ قوّة الدور الذي لا يزال سعود القحطاني، مساعد ولي العهد، يلعبه في حملة التخويف التي تشنّها المملكة العربية السعودية غير واضحة تماما. لم تناقش الحكومة السعودية علنا مكان وجود القحطاني، ولكن على انفراد، يزعم المسؤولون السعوديون أنه قيد الإقامة الجبرية.

مع ذلك، استدلّت العديد من وسائل الإعلام ببعض المصادر التي صرّحت بأن القحطاني لا يزال في رعاية ولي العهد ويواصل عمله بنفس الصفة التي كان يحظى بها قبل إقالته رسميًا من البلاط الملكي. في كانون الثاني/يناير سنة 2019، ذكرت صحيفة واشنطن بوست أن القحطاني شوهد في مكاتب البلاط الملكي في الرياض. وفي نفس الشهر، ذكر كاتب عمود في واشنطن بوست، ديفيد إغناتيوس، نقلا عن مصادر أمريكية وسعودية، أن محمّد بن سلمان على اتصال منتظم بالقحطاني، الذي التقى مؤخرًا بكبار نوابه من المركز.

في نيسان/أبريل سنة 2019، أخبر أحد المصادر صحيفة الغارديان أن محمّد بن سلمان لا يزال مخلصًا للقحطاني، الذي "يشارك بنشاط" في دور مماثل للدور الذي شغله كرئيس للمركز، على الرغم من أنه يتواجد في الوقت الراهن في المكتب الخاص بولي العهد. وفي هذا الإطار، قدّمت صحيفة الغارديان أهم دليل حتى الآن يفيد بأن القحطاني يواصل أعماله المتعلقة بالقرصنة، كما ذكرت الصحيفة في حزيران/يونيو سنة 2019، أنها استُهدفت من قبل فريق اختراق سعودي بأمر من القحطاني.

في البداية، تلقّت الصحيفة التحذيرات من قبل مصدر في الرياض في وقت سابق من هذه السنة، وتم تأكيد هذا التهديد لاحقًا بموجب أمر داخلي سري وقع عليه القحطاني، واطلعت عليه الغارديان. وكُتبت هذه الوثيقة، المؤرخة في السابع من آذار/مارس سنة 2019، باللغة العربية، إذ أُصدرت تعليمات إلى "رؤساء الإدارات التكنولوجية والتقنية" التي تديرها مديرية الأمن السيبراني داخل المكتب الخاص لولي العهد، تأمرهم "باختراق أنظمة الحاسوب الخاصة بصحيفة الغارديان والأشخاص الذين عملوا على التقرير الذي نشر، مع الحرص على التعامل مع القضية بسرية تامة، ومن ثمّ إرسال جميع البيانات لهم في أقرب وقت ممكن".

لا يعدّ القحطاني من ضمن المشتبه بهم الأحد عشر الذين يواجهون المحاكمة في المملكة العربية السعودية بتهمة قتل خاشقجي. ففي 19 حزيران/يونيو 2019، نشرت أنييس كالامار، المقررة الخاصة للأمم المتحدة المعنية بعمليات الإعدام خارج نطاق القضاء أو بإجراءات الإعدام التعسفيّة، تقريرا عن وفاة خاشقجي، واصفة إياه بأنه "إعدام خارج نطاق القضاء مع سبق الإصرار" من تنفيذ الدولة السعودية.

وأضافت كلامار أن "مقتله كان نتيجة تخطيط تفصيلي تضمن تنسيقًا واسعًا وموارد بشرية ومالية كبيرة، كما كان هناك إشراف وتخطيط وتنفيذ من قبل مسؤولين رفيعي المستوى. وبالتالي فقد كان عملا متعمدا". فضلا عن ذلك، يذكر التقرير على وجه التحديد أن القحطاني ومحمد بن سلمان لم توجّه لهما أي تهم جنائية ولكن هناك "أدلة موثوقة ضدّهما تستحق المزيد من التحقيق".

من المقرر أن تُقدّم كالامار نتائج التحقيق الذي أجرته إلى مجلس حقوق الإنسان التابع للأمم المتحدة في 27 حزيران/يونيو سنة 2019، كما ستمثل خطيبة خاشقجي، خديجة جنكيز، بدورها أمام المجلس. وفي الواقع، لا تعد النتائج الواردة في هذا التقرير شاملة، كما أن البحث لا يزال جار فيما يتعلّق بشبكة اتصالات القحطاني. وبالإضافة إلى النطاقات الاثنين والعشرين التي تم تحليلها أعلاه، فقد كشف هذا التحقيق العديد من المجالات الأخرى التي يحتمل ارتباطها بالقحطاني ولكنها تتطلب مزيدًا من البحث والتحليل. علاوة على ذلك، ستنشر أية نتائج إضافية ضمن تقرير المتابعة.

المصدر: موقع بلينغكات

رابط المقال: https://www.noonpost.com/28321/