LORD OF THE FLIES:

AN OPEN-SOURCE INVESTIGATION INTO SAUD AL-QAHTANI

bellingcat

Table of Contents

Introduction

Before tuning in via Skype[1] to oversee the murder and dismemberment of Saudi Arabian journalist Jamal Khashoggi, Saud al-Qahtani, a high-level adviser to the crown prince of Saudi Arabia, Mohammed bin Salman (MBS), was best known for running social media operations for the royal court and serving as MBS's chief propagandist and enforcer. His portfolio also included hacking and monitoring critics of the Kingdom and MBS.

In 2012 and again in 2015, someone identifying themselves as al-Qahtani attempted to procure surveillance tools from controversial[2] Italian spyware vendor Hacking Team. On July 5, 2015, this correspondence was unknowingly exposed by a hacker using the handle "Phineas Phisher," who stole and published approximately 400 gigabytes of Hacking Team's internal documents, source code and emails.[3]

Al-Qahtani's outreach to the spyware vendor appear to have gone unnoticed for years until August 29, 2017, when an Arabic-language Twitter account was created and began publicizing excerpts of al-Qahtani's emails to Hacking Team.[4]

The account, which used the username @HIAHY and the display name تاريخ وذكريات (History and Memories), also tied the email addresses used by al-Qahtani to several online accounts. @HIAHY pointed out[5] that an email address used by the individual purporting to be al-Qahtani to communicate with Hacking Team — saudq1978@gmail.com — was also used to register an account under the handle nokia2mon2 on the popular hacking website Hack Forums, which itself was breached in June 2011 by hacktivist group LulzSec.[6]

Additional reporting by Motherboard in August 2018 revealed that the leaked Hacking Team correspondence included two additional email addresses used by the person purporting to be al-Qahtani: s.qahtani@royalcourt.gov.sa and saudq@saudq.com.[7]

Neither @HIAHY nor Motherboard were able to definitively prove that al-Qahtani owned the leaked email addresses, though both provided persuasive circumstantial evidence that al-Qahtani was indeed behind the emails to Hacking Team, and that he was the owner of the nokia2mon2 profile on Hack Forums.

This report expands on research and reporting by @HIAHY and Motherboard in seven sections. First, the report's key findings are summarized. Second, a short biography charts al-Qahtani's rise to power and summarizes his involvement in the Khashoggi murder. Third, al-Qahtani is shown to own the email

[1] https://www.reuters.com/article/us-saudi-khashoggi-adviser-insight/how-the-man-behind-khashoggi-murder-ran-the-killing-via-skype-idUSKCN1MW2HA
[2] https://citizenlab.ca/tag/hacking-team/
[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-al-qahtani-saudi-arabia-hacking-team

addresses in the Hacking Team dump as well as a previously unreported mobile phone number — +966 55 548 9750 — that also appears in the leaked Hacking Team emails. Fourth, al-Qahtani's activity on Hack Forums is examined in detail. Fifth, a previously unreported network of web infrastructure used by al-Qahtani for malicious purposes is identified and analyzed. Sixth, the contact information shown to belong to al-Qahtani in section three is used to uncover additional details about his online footprint, including his creation of fake social media profiles. Finally, the report's conclusion addresses al-Qahtani's unclear role in MBS's continued efforts to silence critics and dissidents.

All of the information in this report was identified solely through open-source research.

I. Key Findings

The following are among this report's key findings:

- Saud al-Qahtani owns the email addresses saudq1978@gmail.com, saud@saudq.com and s.qahtani@royalcourt.gov.sa as well as the mobile phone number +966 55 548 9750. This confirms that it was al-Qahtani who reached out to Hacking Team to purchase their spyware tools in 2012 and 2015.

    - The individual identifying themselves as al-Qahtani in emails to Hacking Team in 2012 and 2015 used two email addresses (saudq1978@gmail.com and saud@saudq.com) and a phone number (+966 55 548 9750) that can be definitively linked to al-Qahtani through information leakage from Google's and Twitter's password recovery pages. The same individual also used the email address s.qahtani@royalcourt.gov.sa to communicate with Hacking Team. Thought it was not possible to definitively demonstrate al-Qahtani's ownership of this email address through information leakage on password recovery pages, this report judges with high confidence that s.qahtani@royalcourt.gov.sa is al-Qahtani's official government email address, owing in part to a June 2015 email exchange with a Hacking Team representative that involved the seamless, contemporaneous use of s.qahtani@royalcourt.gov.sa and al-Qahtani's saud@saudq.com email address, which demonstrated a common owner of the two accounts.

- Al-Qahtani registered at least 22 domains since 2009, some of which have been used as command and control servers for malware. Al-Qahtani demonstrated exceptionally poor operational security when registering nearly all of these domains. The Whois records of all but three (saudq.com, saudqq.com and jasmn.info) included either his personal email address (saudq1978@gmail.com), mobile phone number (+966 55 548 9750) or variations on his real name. Just two of the domains are currently active: saudq.com and jasmn.info.

- Confirming that saudq1978@gmail.com is owned by al-Qahtani establishes that the Hack Forums account registered with that email address, nokia2mon2, also belongs to al-Qahtani. Among other things, al-Qahtani's posts on Hack Forums detail the hacking tools and services he purchased and used and the social media platforms and mobile apps he targeted. He also posted at least three times while drunk, by his own admission, and opined on topics unrelated to hacking such as the role of religion in politics and policy toward Iran.

- Using the contact information owned by al-Qahtani, it was possible to identify additional contact information for him and identify several accounts linked to these email addresses and phone numbers. He has a LinkedIn Premium account under the name "saud a" (al-Qahtani's middle name is Abdullah), where he describes himself as a "headhunter" based in Saudi Arabia. He created a Facebook profile under the persona of a pro-Mubarak "Egyptian citizen at the end of his life." Al-Qahtani also has accounts on Snapchat, WhatsApp and Signal.

II. From Poet To Enforcer

Born on July 7, 1978 in Riyadh, Saud bin Abdullah al-Qahtani earned a bachelor's degree in law from King Saud University before joining the Royal Saudi Air Force's officer training course, according to an Arab News profile.[8] Al-Qahtani was eventually promoted to the rank of captain and subsequently attended Naif Arab University for Security Sciences, where he earned a master's degree in criminal justice.

Al-Qahtani began his career promoting the royal family in columns for Saudi newspapers and publishing nationalist poems under the pseudonym "Dhari" (ضاري).

In the early 2000s, al-Qahtani was hired by the former head of the Saudi royal court, Khaled al-Tuwaijri, to run an electronic media army charged with protecting Saudi Arabia's image, according to reporting by Reuters.[9]

Al-Qahtani went on to hold several prominent roles in government, including legal adviser to the secretariat to then Crown Prince Abdullah bin Abdul Aziz in 2003 and media director of the same secretariat in 2004.

By 2008, al-Qahtani was Director General of the Center of Media Monitoring and Analysis in the Royal Court (مدير عام مركز الرصد والتحليل الإعلامي بالديوان الملكي). A year later, in 2009, he joined Hack Forums under the handle nokia2mon2. In 2011, he created his Twitter account, @saudq1978.

In 2012, al-Qahtani reached out to Hacking Team for the first time using his saudq1978@gmail.com email address. His second overture to the spyware vendor came in June 2015, when he used an official government email address, s.qahtani@royalcourt.gov.sa. As described below, the Saudi royal court likely did not have official email addresses in 2012, when al-Qahtani first contacted Hacking Team.

In December 2015, King Salman issued a royal decree promoting al-Qahtani to royal adviser at the rank of minister.[10] Roughly six months before, Salman had announced a major shift in Saudi Arabia's line of succession that put his son, MBS, second in line to the throne behind King Salman's nephew, Mohammed bin Nayef.

Al-Qahtani held several high-level positions in the Center for Studies and Media Affairs in the Royal Court (مركز الدراسات والشؤون الإعلامية في الديوان الملكي) during this period, eventually becoming director in 2016. Al-Qahtani used the Center, which operated without oversight by other ministries, as his base of operations to help King Salman and MBS consolidate power as the latter jockeyed for control with other members of the royal family.[11] These efforts ranged from typical influence operations, such as hiring high-end lobbying and

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

[9] https://www.reuters.com/article/us-saudi-khashoggi-adviser-insight-idUSKCN1MW2HA

[10] https://www.spa.gov.sa/1428315

[11] https://www.washingtonpost.com/opinions/global-opinions/mbss-rampaging-anger-will-not-silence-questions-about-jamal-khashoggi/2018/10/16/5a0bf43a-d182-11e8-b2d2-f397227b43f0_story.html

public relations firms, including BGR Group,[12] SGR[13] and Squire Patton Boggs,[14] to a full-fledged suppression and intimidation campaign involving kidnappings, torture and murder.

In the spring of 2017, al-Qahtani and the Center worked with a newly established “tiger squad” or “rapid intervention group” of Saudi intelligence operatives to organize the kidnappings of dissidents and critics inside the kingdom and abroad and to hold them in secret detention sites.[15] The tiger squad was involved in at least a dozen operations, including the murder of Khashoggi.[16]

In June 2017, MBS became crown prince after King Salman issued a royal decree ousting Nayef and relieving him of all official positions. Nayef was subsequently placed under house arrest. Five months later, in November 2017, MBS created and headed an “anti-corruption committee,” which was used to arrest and detain hundreds of Saudis seen as a threat to MBS’s consolidation of power, including princes, ministers, business people, clerics and politicians.

Months later, in November 2017, al-Qahtani was tapped to lead the interrogation of Lebanese prime minister Saad al-Hariri, who was detained in Riyadh, verbally humiliated, beaten and forced to resign.[17]

The Saudi suppression campaign continued into 2018, when prominent women’s rights activists who were campaigning for the right of Saudi women to drive were arrested and tortured. One activist, Loujain al-Hathloul, told her brother that she was waterboarded and electrocuted in the basement of a prison near Jeddah. The man who oversaw her torture was al-Qahtani, according to al-Hathloul’s brother, who said MBS’s close aide personally attended the torture the activist, laughing as he threatened to have her raped and murdered.[18]

Al-Qahtani also took to social media to silence dissent and identify critics of the regime and wage online campaigns against Saudi Arabia’s rivals, such as Iran and Qatar. In an August 2017 tweet, he implored his more than one million Twitter followers to use the hashtag #TheBlacklist (#القائمة_السوداء) to expose the names and identities of dissidents and activists expressing sympathy for Qatar during Saudi Arabia’s diplomatic crisis with the Gulf country.[19] Anyone added to the blacklist would be “followed,” according to al-Qahtani. Al-Qahtani also used his social media following to harass critics online, earning him the nickname “Lord of the Flies” — “electronic flies” being the term used by critics to describe al-Qahtani’s online bots and minions.

While MBS consolidated power, al-Qahtani’s cyber portfolio continued to grow. In October 2017, al-Qahtani became president of a newly established organization under the auspices of the Saudi Olympic

[12] https://efile.fara.gov/docs/5430-Exhibit-AB-20160315-53.pdf
[13] https://efile.fara.gov/docs/6379-Exhibit-AB-20160920-1.pdf
[14] https://efile.fara.gov/docs/2165-Exhibit-AB-20160920-67.pdf
[15] https://www.washingtonpost.com/opinions/global-opinions/the-khashoggi-killing-had-roots-in-a-cutthroat-saudi-family-feud/2018/11/27/6d79880c-f17b-11e8-bc79-68604ed88993_story.html
[16] https://www.nytimes.com/2019/03/17/world/middleeast/khashoggi-crown-prince-saudi.html
[17] https://www.reuters.com/article/us-saudi-khashoggi-adviser-insight/how-the-man-behind-khashoggi-murder-ran-the-killing-via-skype-idUSKCN1MW2HA
[18] https://www.bbc.com/news/world-middle-east-47956124
[19] https://twitter.com/saudq1978/status/898259368696725504

Committee called the Electronic Security and Software Alliance.[20] The purpose of the organization, which was later renamed the Saudi Federation for Cybersecurity, Programming and Drones (SAFCSP), is to "build national and professional capabilities in the fields of cyber security and programming [...] to expedite the ascent of the Kingdom of Saudi Arabia to the ranks of developed countries in the domain of technology innovation," according to the SAFCSP website.[21]

In February 2018, al-Qahtani changed his Twitter bio[22] to indicate that he was head of the Center of Excellence in information Assurance (CoEIA)[23] at King Saud University and the C4I Center for Advanced Systems[24] also at King Saud University (C4I refers to Command, Control, Communications, Computers and Intelligence). He also wrote that he was a member of several boards: the Misk Foundation, Misk Schools, the Royal Commission for al-Ula and the Darah Foundation.

Al-Qahtani's first confrontation with Khashoggi took place in late 2016, when the latter was working as a columnist for the London-based al-Hayat newspaper. Al-Qahtani called Khashoggi to inform him that he was "not allowed to tweet, not allowed to write, not allowed to talk," according to reporting by the Washington Post.[25] "You can't do anything anymore — you're done." After al-Qahtani's injunction fell on deaf ears, he changed tact and tried to woo Khashoggi back to the kingdom, assuring the journalist that his transgressions would be forgiven.

On October 2, 2018, al-Qahtani reportedly tuned in via Skype to oversee the murder and dismemberment of Khashoggi in the Saudi consulate in Istanbul.[26] After exchanging insults with Khashoggi, he ordered the members of the "tiger team" that had detained Khashoggi to "bring me the head of the dog." The CIA assessed with medium to high confidence that MBS ordered Khashoggi's killing, citing in part 11 text messages the crown prince exchanged with al-Qahtani before and after the murder.[27]

After denying any involvement in the killing for 18 days, the Saudi Ministry of Foreign Affairs issued a statement on October 20, 2018 acknowledging for the first time that Khashoggi had been killed at the hands of the Saudis, though accidentally, as the result of a fight.[28] That same day, King Salman issued a decree relieving al-Qahtani from his post as advisor at the royal court.[29] Al-Qahtani took to Twitter to express his gratitude to King Salman and MBS for allowing him to serve his country.[30] "I will continue to

[20] http://ara.tv/ntwtn
[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-security/jamal-khashoggis-final-months-an-exile-in-the-long-shadow-of-saudi-arabia/2018/12/21/d6fc68c2-0476-11e9-b6a9-0aa5c2fcc9e4_story.html
[26] https://www.reuters.com/article/us-saudi-khashoggi-adviser-insight/how-the-man-behind-khashoggi-murder-ran-the-killing-via-skype-idUSKCN1MW2HA
[27] https://www.washingtonpost.com/world/national-security/saudi-crown-prince-exchanged-messages-with-aide-alleged-to-have-overseen-khashoggi-killing/2018/12/01/faa43758-f5c3-11e8-9240-e8028a62c722_story.html
[28] https://twitter.com/KSAmofaEN/status/1053428352164548609
[29] https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=1830340
[30] https://twitter.com/saudq1978/status/1053438590095708160

be a loyal servant of my country for all eternity," he wrote. He sent a follow-up tweet thanking his colleagues at the Center and other departments of the royal court.[31]

Al-Qahtani has been officially sanctioned by two U.S. agencies. In November 2018, the U.S. Treasury Department sanctioned al-Qahtani and 15 other members of his tiger team for their roles in Khashoggi's murder.[32] Al-Qahtani was "part of the planning and execution of the operation that led to the killing of Mr. Khashoggi," according to the Treasury Department press release. The State Department followed suit in April 2019, designating al-Qahtani and 15 other Saudis as having a role in Khashoggi's murder.[33] As such, al-Qahtani and his immediate family are prohibited from entering the U.S.

[31] https://twitter.com/saudq1978/status/1053493341147578368
[32] https://home.treasury.gov/news/press-releases/sm547
[33] https://translations.state.gov/2018/11/15/statement-by-secretary-pompeo-global-magnitsky-sanctions-on-individuals-involved-in-the-killing-of-jamal-khashoggi/

III. Leaked Contact Information Owned By Al-Qahtani

The individual identifying himself as Saud al-Qahtani in emails to Hacking Team used three email addresses:

- saudq1978@gmail.com in at least five emails in March 2012[34]
- saud@saudq.com in at least four emails from June 2015 to July 2015[35]
- s.qahtani@royalcourt.gov.sa in at least 14 emails from June 2015 to July 2015[36]

The same individual indicated in at least two emails sent from s.qahtani@royalcourt.gov.sa and saud@saudq.com that his mobile phone number was +966 55 548 9750.[37]

Using information leakage[38] from Google's and Twitter's password recovery pages, it is possible to conclusively link al-Qahtani to saud@saudq.com, saudq1978@gmail.com, s.qahtani@royalcourt.gov.sa and +966 55 548 9750.

Al-Qahtani Twitter Connected To Saudq@saud.com And Cell Number

Al-Qahtani's verified Twitter account, @saudq1978,[39] is linked to +966 55 548 9750 and saud@saudq.com, according to information leakage from Twitter's forgot password feature:

[34] https://wikileaks.org/hackingteam/emails/?q=&mfrom=saudq1978%40gmail.com&mto=&title=&notitle=&date=&nofrom =&nnot=&count=50&sort=1#searchresult

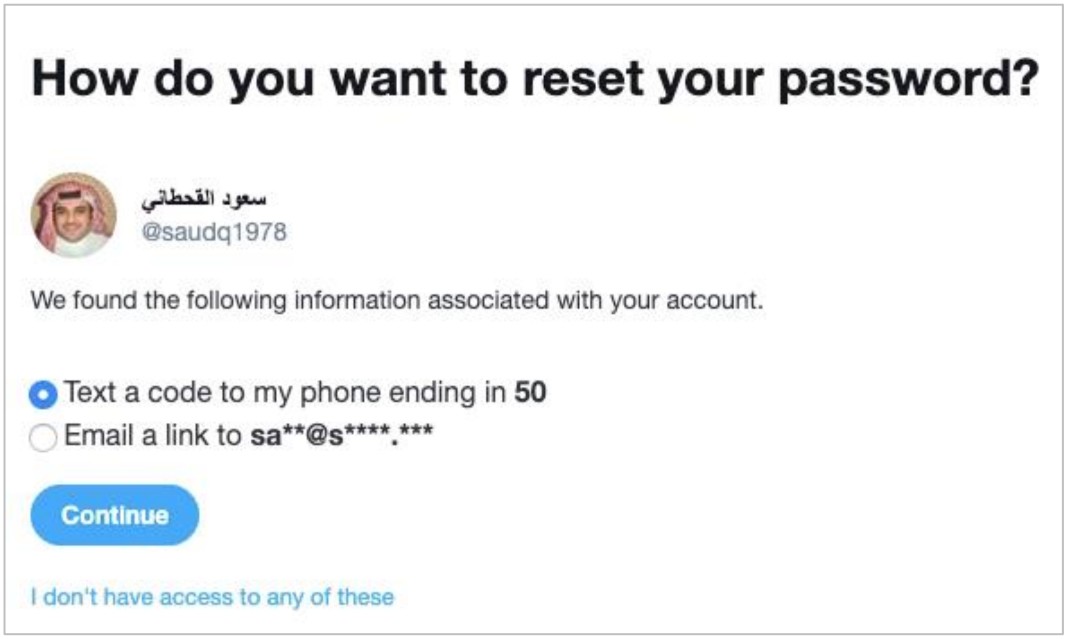
[35] https://wikileaks.org/hackingteam/emails/?q=&mfrom=saud%40saudq.com&mto=&title=&notitle=&date=&nofrom=& noto=&count=50&sort=1#searchresult

[36] https://wikileaks.org/hackingteam/emails/?q=&mfrom=s.qahtani%40royalcourt.gov.sa&mto=&title=&notitle=&date=&no from=&noto=&count=50&sort=1#searchresult

[37] https://wikileaks.org/hackingteam/emails/emailid/1144691 and https://wikileaks.org/hackingteam/emails/emailid/1134945

[38] https://motherboard.vice.com/en_us/article/8q8x8a/twitter-password-reset

[39] https://twitter.com/saudq1978



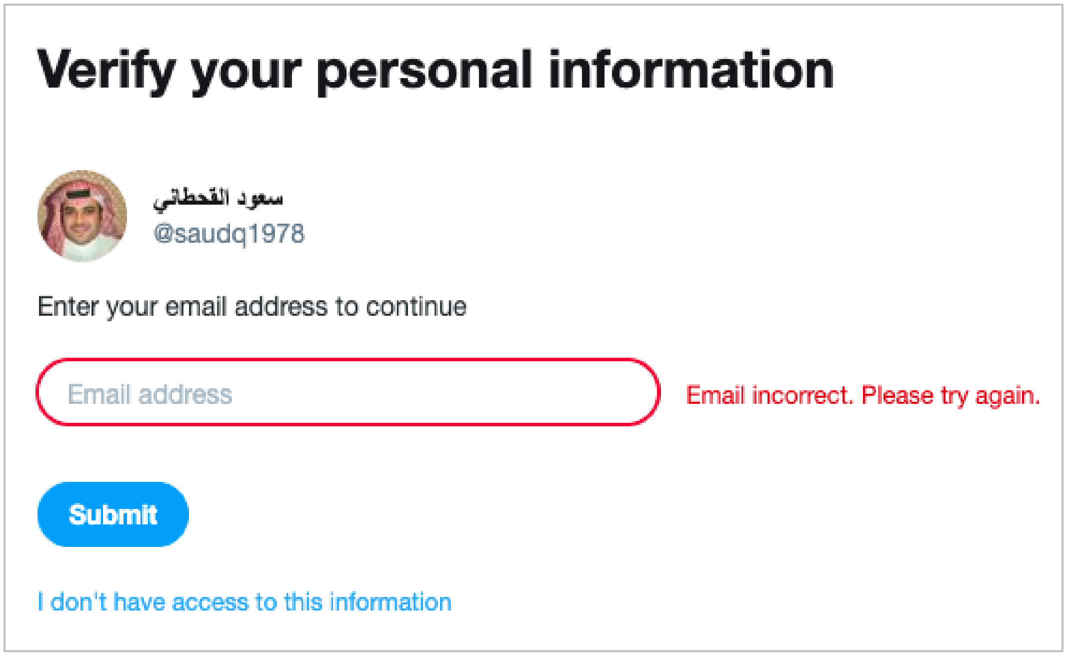
How do you want to reset your password?

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****.*****

In order to get to the password rest page in the screenshot above, the correct email address and phone number need to be entered. Providing an email address not associated with al-Qahtani's account returns an error:



Verify your personal information

سعود القحطاني
@saudq1978

Enter your email address to continue

Email address

Email incorrect. Please try again.

A similar error is returned when an incorrect phone number is provided.

Royal Court Email Used To Provide Al-Qahtani Phone Number, Email

Given that al-Qahtani is the owner of the phone number +966 55 548 9750 and the email address saud@saudq.com, it is highly likely that the Saudi government email address s.qahtani@royalcourt.gov.sa also belongs to al-Qahtani.

On June 29, 2015, Hacking Team founder and CEO David Vincenzetti received the initial emails sent from s.qahtani@royalcourt.gov.sa to Hacking Team. In one email, the sender asked that Vincenzetti contact him "on my private mobile (+966 55 548 9750)" via mobile encrypted messaging apps Threema or Telegram (emphasis added):[40]

> *Dear David*
>
> *Considering your esteemed reputation and professionalism, we here at the Center for Media Monitoring and Analysis at the Saudi Royal Court (THE King Office) would like to be in productive cooperation with you and develop a long and strategic partnership.*
>
> *I would like you to be so kind as to send us the complete list of services that your esteemed company offers, in addition to their prices, all explained in detail, as soon as possible please.*
>
> *You may contact me by Telegram or Threema on my private mobile (+966 55 548 9750) to arrange sending your information encrypted in a way that is convenient for you pgp or what ever you like.*
>
> *Best regards*
> *H.E. Saud Al-Qahtani*
> *Adviser at the Royal Court*
> *General Director of the Center for Media Monitoring and Analysis*

[Note, al-Qahtani is not a fluent English speaker. All errors of spelling, syntax and grammar as presented in this report are in the original.]

After struggling to properly attach his PGP key, the individual behind s.qahtani@royalcourt.gov.sa sent an email to Hacking Team account representative Emad Shehata on June 30, 2015 describing saud@saudq.com as his private email address:[41]

> *i sent it to you now from my private email*
> *saud@saudq.com*
> *as there is problem in attach in this email*
> *hope its work'*
> *Regards*

Two minutes earlier on the same day, al-Qahtani had sent an email to Shehata via saud@saudq.com with the subject "my key."[42] "Its attached hope its good now," al-Qahtani wrote. That email to Shehata was the first sent to Hacking Team using al-Qahtani's saud@saudq.com email address.

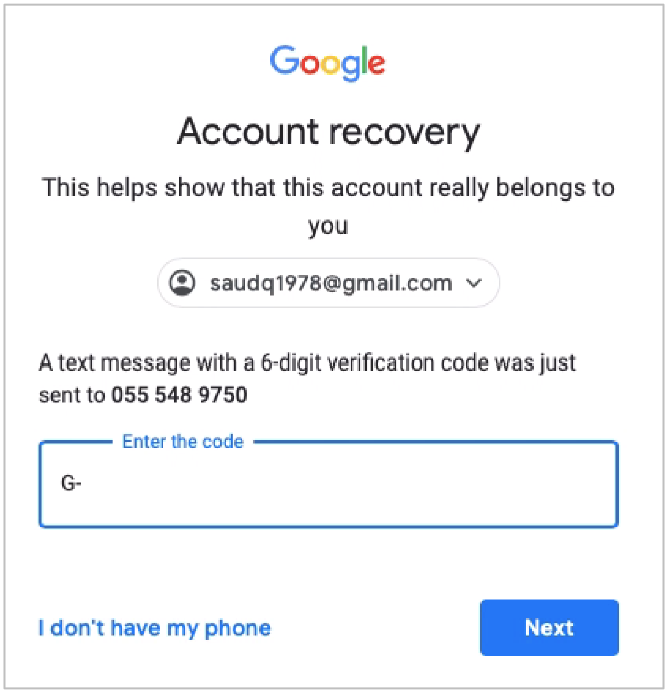
[40] https://wikileaks.org/hackingteam/emails/emailid/1144691
[41] https://wikileaks.org/hackingteam/emails/emailid/1134964
[42] https://wikileaks.org/hackingteam/emails/emailid/1134947

Shehata responded minutes later to al-Qahtani via saud@saudq.com that he received the key. At 9:00 UTC, al-Qahtani replied via saud@saudq.com, "great waiting for it so i sign it and we can go to the next step. im sdure your nda will be very profisional and will protect our privacy."[43] At 09:07 UTC, s.qahtani@royalcourt.gov.sa replied to an email from Shehata with the subject "NDA," writing "ok got it i will sign it later today and sent it to u again."[44]

Shehata's seamless, contemporaneous communication with the s.qahtani@royalcourt.gov.sa and saud@saudq.com email addresses regarding the same subject matter makes it highly likely that al-Qahtani is the owner the royal court email address.

Gmail Linked To Same Al-Qahtani Phone Number And Email As Twitter

Al-Qahtani also owns the email address saudq1978@gmail.com, based on information leakage from Google's password recovery feature, which shows that the Gmail account is connected to al-Qahtani's phone number, +966 55 548 9750:



Account recovery

This helps show that this account really belongs to you

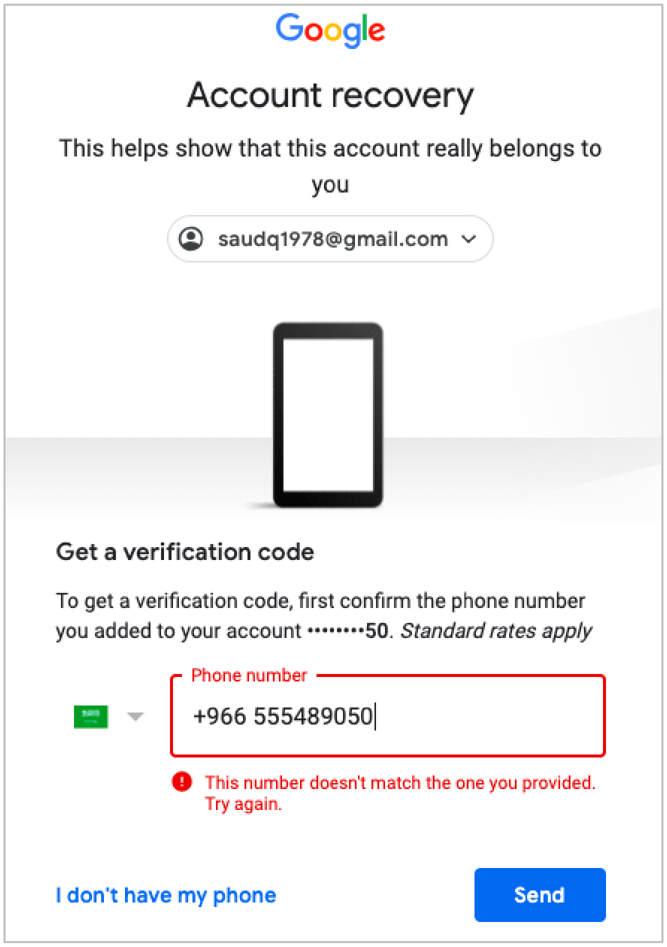
saudq1978@gmail.com

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

G-

As with Twitter's password recovery feature, providing a phone number not associated with al-Qahtani's account returns an error:

[43] https://wikileaks.org/hackingteam/emails/emailid/1134955
[44] https://wikileaks.org/hackingteam/emails/emailid/1134951



Account recovery

This helps show that this account really belongs to you

saudq1978@gmail.com

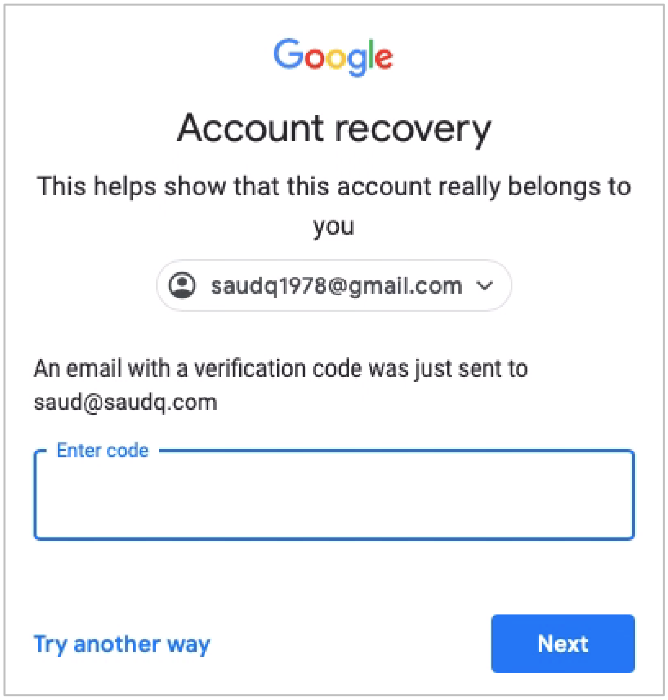
Get a verification code

To get a verification code, first confirm the phone number you added to your account ••••••••50. *Standard rates apply*

Phone number: +966 555489050

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

The same technique shows that al-Qahtani's saud@saudq.com email address is also connected to saudq1978@gmail.com:



Account recovery

This helps show that this account really belongs to you

saudq1978@gmail.com

An email with a verification code was just sent to saud@saudq.com

Enter code

Providing an incorrect email address produces an error similar to the phone number error above.

The first email to Hacking Team from al-Qahtani was sent via saudq1978@gmail.com on March 18, 2012 and requested that Hacking Team travel to Saudi Arabia to explain the company's offerings and provide training:[45]

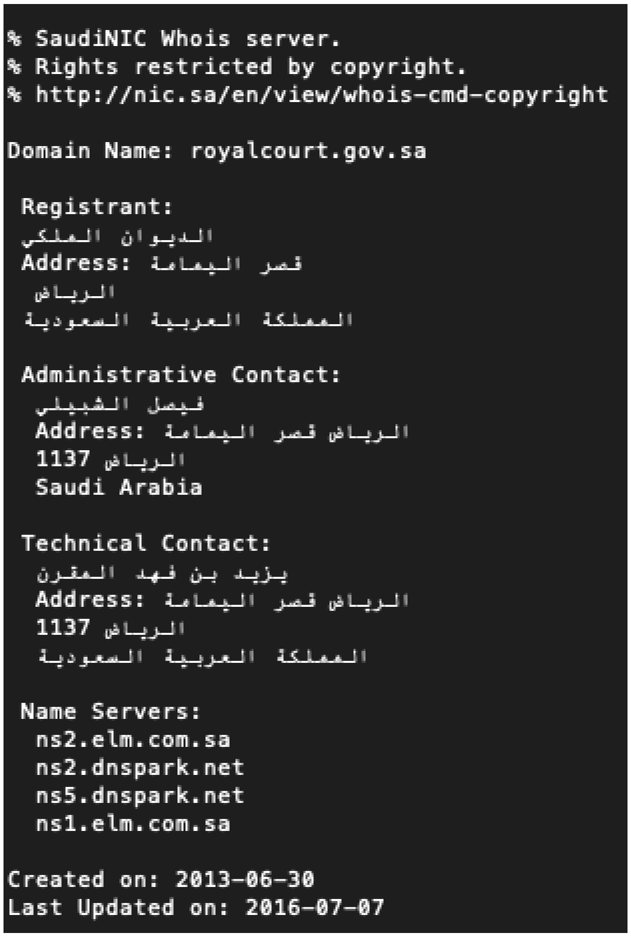
> *Dear Sir:*
> *We need people visit us in Hosted by the Saudi governmen that have high technical knowledge and high Authority in order to provide an integrated display and explain the solutions you offer and training and costs. we Will bear all the costs of the trip from a-z. please send to me all the info you need to*
> *manage that.*
>
> *Regards*
>
> *saud*

Hacking Team account manager Mostapha Maanna requested that al-Qahtani use an official email address "since our policy allows us to work with governmental agencies only." Al-Qahtani replied that the Royal Court did not have official email addresses:[46]

> *Dear Sir:im authorized from my government to contact you.we are from the royal court of saudi arabia, the king office.*
> *we don't have official emails and we use secure fax onlythe number is: +96612926120.if you want we can confirm that with you by the fax.*
> *or: send to me the name and the number and the country for the person that our Embassy will contact him. they will confirm official that we authorized him to contact your company. they will be not authorized to discuss any thing with you, they only will confirm - as you like- that is a governmental*
> *deal and its will be secure and that the fax number is our official fax and that we*
> *authorized to speak and deal in the name of the royal court of saudi arabia. after that we can go with the next step.hope that will be fine with you.*
>
> *Best Regards saud abdullah*

According to Whois records, the royalcourt.gov.sa domain, which al-Qahtani would later use to contact Hacking Team again in 2015, was not created until June 2013:

[45] https://wikileaks.org/hackingteam/emails/emailid/578260
[46] Ibid.



```
% 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 الشبيلي
  Address: الرياض قصر اليمامة
  1137 الرياض
  Saudi Arabia

 Technical Contact:
  يزيد بن فهد المقرن
  Address: الرياض قصر اليمامة
  1137 الرياض
  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. Hack Forums Activity

Al-Qahtani used saudq1978@gmail.com for a wide range of online activities, including registering accounts on forums and social media sites. Both the @HIAHY Twitter account and Motherboard reported that saudq1978@gmail.com was used to register an account on the hacking website Hack Forums under the username nokia2mon2.

Indeed, breach data from a June 2011 hack of the website, which is considered to be popular with low-skilled hackers and cybercriminals, associates saudq1978@gmail.com with the username nokia2mon2 and an IP address — 62.120.153[.]248 — that geolocates to Riyadh and is currently part of a subnet allocated to the Saudi telecommunications firm Etihad Etisalat.

Al-Qahtani was an active Hack Forums member, posting more than 500 times[47] and contributing more than $10,000 to the website between July 2009 and September 2016. He deleted at least 98 posts, as his member profile indicates that he posted 441 times, while a screenshot published by @HIAHY shows that he posted at least 539 times.

Al-Qahtani never revealed his identity on the forum, but he did share biographical information about himself in one post, and his first name was disclosed by another Hack Forums user in a thread detailing a deal between the user and al-Qahtani.

In October 2010, al-Qahtani wrote a post about himself in response to a thread recruiting members for a group calling itself The RATs Crew (a RAT, or "remote access trojan," is a type of malware that lets hackers access and control an infected computer remotely).[48] Al-Qahtani wrote that he was 33 years old and had used RATs since 2000. In fact, al-Qahtani was 32 at the time if he was born on July 7, 1978, as indicated by the U.S. Treasury Department.[49] He wrote that he was from Saudi Arabia, and that he stopped using RATs by 2002, "becuse making my future :)" As described above, al-Qahtani was hired by former head of the Saudi royal court, al-Tuwaijri, to run an electronic media army charged with protecting Saudi Arabia's image in the early 2000s.

The previous October, a user called RelVlotelVlod started a thread in the "Secondary Sellers Market" subforum that listed al-Qahtani's first name, Saud, in the the title of the post: "ME & saud Vps deal."[50] The deal described by RelVlotelVlod reads like a scam: al-Qahtani paid RelVlotelVlod $250 for bots on RelVlotelVlod's "friend's" botnet. RelVlotelVlod's friend then banned him, according to RelVlotelVlod's telling, so he asked al-Qahtani for an additional $20 to set up an IRC server for a botnet.

This section details al-Qahtani's activity on the forum, including:

- The scams he fell victim to

[47] https://twitter.com/HIAHY/status/902979053417848833/photo/1

[48] https://hackforums.net/showthread.php?tid=151065&pid=7031243&highlight=becuse+making+my+future#pid7031243

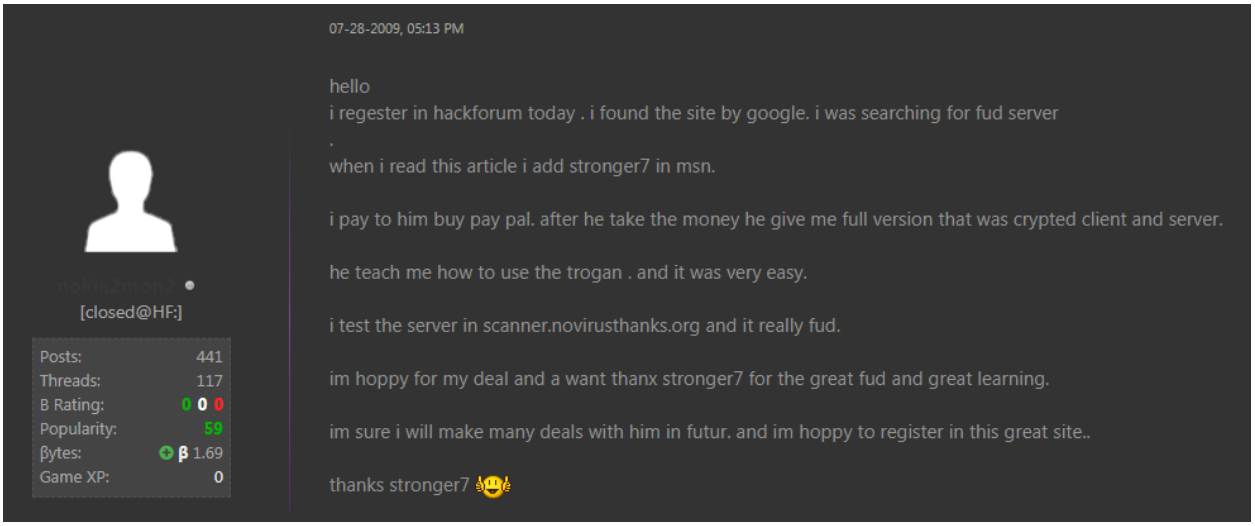
[49] https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20181115.aspx

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

- The hacking tools and services he purchased and used
- The social media platforms and mobile apps he targeted
- His opinions on God, religion, President Obama and Kashmir
- His admissions to being drunk
- His payment methods and use of an additional email address
- His attempts at cracking wireless networks

Scammed On Day One

Al-Qahtani had an inauspicious start on Hack Forums, where scams are not uncommon. He registered the nokia2mon2 account on July 28, 2009, according to his member profile.[51] His first post, published on the same day, stated that he found Hack Forums after searching for a "fud server." ("FUD" stands for "fully undetectable" and refers to malware that is fully undetectable by anti-virus software). He wrote that he bought a trojan[52] from a user called "stronger7," who taught him how to use the unnamed program:



nokia2mon2
[closed@HF:]

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

07-28-2009, 05:13 PM

hello
i regester in hackforum today . i found the site by google. i was searching for fud server
.
when i read this article i add stronger7 in msn.

i pay to him buy pay pal. after he take the money he give me full version that was crypted client and server.

he teach me how to use the trogan . and it was very easy.

i test the server in scanner.novirusthanks.org and it really fud.

im hoppy for my deal and a want thanx stronger7 for the great fud and great learning.

im sure i will make many deals with him in futur. and im hoppy to register in this great site..

thanks stronger7

Other users in the thread commented that software being sold by stronger7 looked like a repackaged version of a RAT called Cerberus. Days later, on August 2, 2009, al-Qahtani wrote that his PC was infected by a virus and that he had to reformat it.[53] Users immediately linked al-Qahtani's computer problem with stronger7: "Your PC was probably infected with Strong7's SpyNet bullshit or w/e its called. You did buy that didn't you?" Al-Qahtani replied, "yes i buy it !! is it inficted???? [...] i dont think Strong7's will do that for me.. i think he is a very good man and look trusted!!!" Another user chimed in, "An another poor victim !" Stronger7 was apparently later banned by Hack Forums moderators.

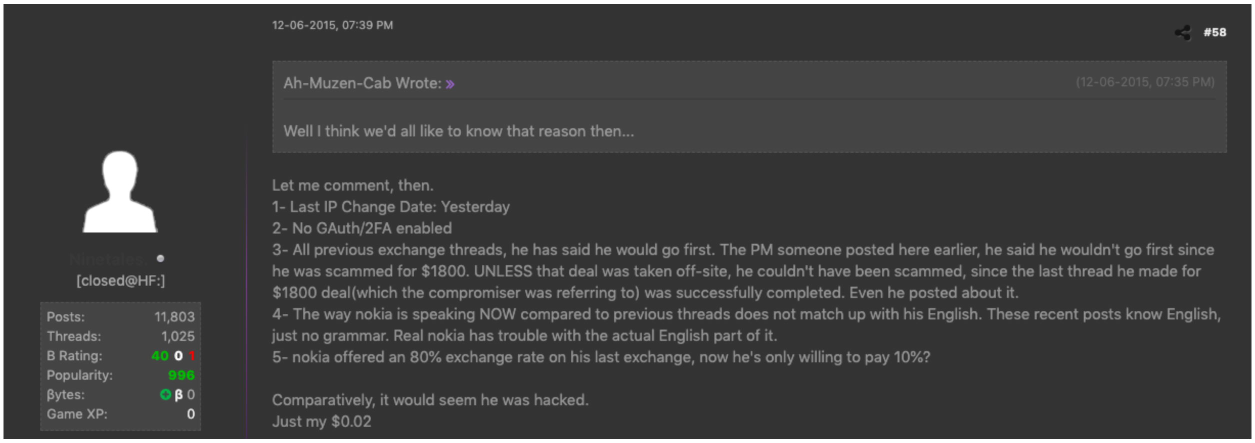
Al-Qahtani fell victim to at least two other scams while he was active on Hack Forums, and his account was hacked as well.

[51] https://hackforums.net/member.php?action=profile&uid=80618
[52] https://en.wikipedia.org/wiki/Trojan_horse_(computing)
[53] https://hackforums.net/showthread.php?tid=114215&pid=1057777#pid1057777

In September 2010, a year after he was infected by stronger7, he said he got scammed out of $150 after paying a user called “MoBreeze” via Western Union “to give me my hacked hotmail password.”[54]

Five years later, in April 2015, he wrote that he was scammed out of $3,000 in Bitcoin by a user called “υNk.”[55] Al-Qahtani did not indicate what he was trying to purchase. Al-Qahtani’s Bitcoin wallet address was not identified in the course of this investigation.

In December 2015, al-Qahtani’s account was hacked. Someone using his account posted a thread asking to exchange $8,000 to Bitcoin.[56] After three pages of posts vouching for nokia2mon2 and users expressing their amazement at the large sum, some Hack Forum members began suggesting that nokia2mon2’s account may have been hacked after noticing a change in the login IP address associated with the account and inconsistencies with previous posts:



12-06-2015, 07:39 PM

#58

Ninetales

[closed@HF:]

Posts:	11,803
Threads:	1,025
B Rating:	40 0 1
Popularity:	996
βytes:	β 0
Game XP:	0

> Ah-Muzen-Cab Wrote: » (12-06-2015, 07:35 PM)
>
> Well I think we'd all like to know that reason then...

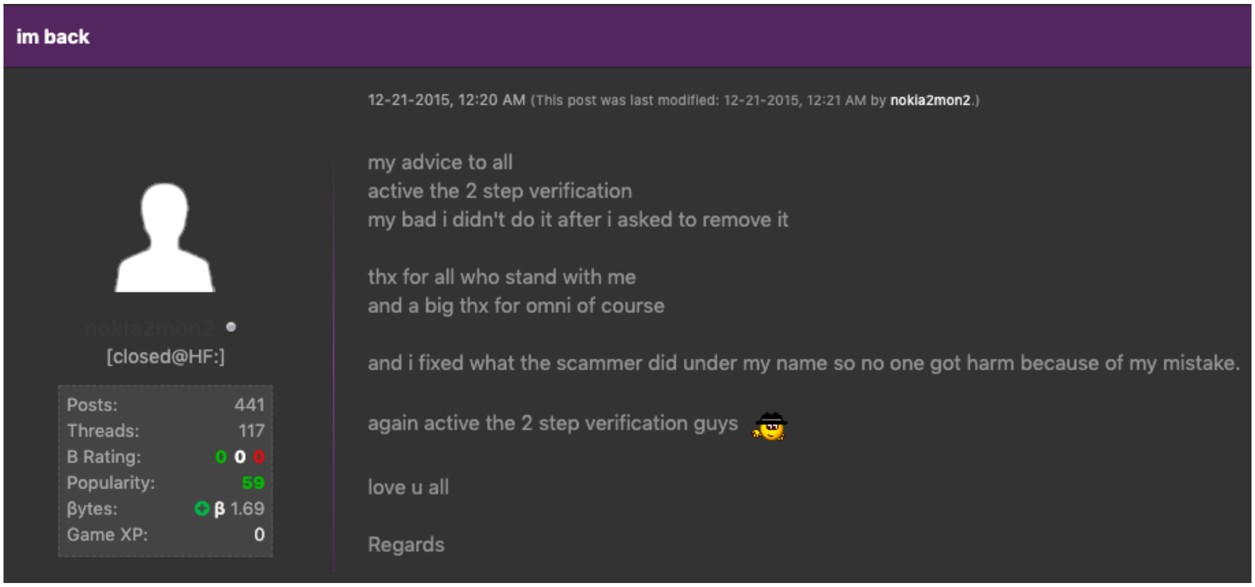
Let me comment, then.
1- Last IP Change Date: Yesterday
2- No GAuth/2FA enabled
3- All previous exchange threads, he has said he would go first. The PM someone posted here earlier, he said he wouldn't go first since he was scammed for $1800. UNLESS that deal was taken off-site, he couldn't have been 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

The next day, the person controlling al-Qahtani’s account posted a thread asking for someone to exchange $1,900 to Bitcoin.[57] Jesse LaBrocca, the administrator of Hack Forums, wrote that the thread “was not posted by account owner,” but not before a user sent the hacker controlling nokia2mon2 $500 via PayPal.

Two weeks later, al-Qahtani started a thread titled “im back” in which he advised other Hack Forum members to set up two-factor authentication on their accounts and that he “fixed what the scammer did under my name so no one got harm because of my mistake”:[58]

[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
[57] https://hackforums.net/showthread.php?tid=5084797
[58] https://hackforums.net/showthread.php?tid=5102030&pid=49047929#pid49047929



im back

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

nokia2mon2

[closed@HF:]

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

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

RATs, Botnets And DDoS Attacks

Over the course of the seven years that he was active on the Hack Forums, al-Qahtani acknowledged purchasing and using at least two dozen hacking tools and services, most of which require little technical knowhow. The tools and services he used were mostly RATs, crypters, worms and DDoS-for-hire bots.

Used RAT Targeted In Worldwide Law Enforcement Operation

Al-Qahtani showed an interest in RATs and crypters from the first days he joined Hack Forums (a crypter is a type of software that encrypts or otherwise obfuscates malware to make it harder to detect by anti-virus programs). In his second post on the forum, in July 2009, al-Qahtani asked for recommendations for "a powerfull crypter that can work with all rat and make it full FUD and work very stable."[59]

By June 2011, less than two years after joining the forum, he estimated that he had 90% of paid and free RATs on the market.[60] He specifically mentioned using:

- Blackshades
- Poison Ivy
- Cybergate
- Albertino Advanced RAT
- Nullbot
- Netwire

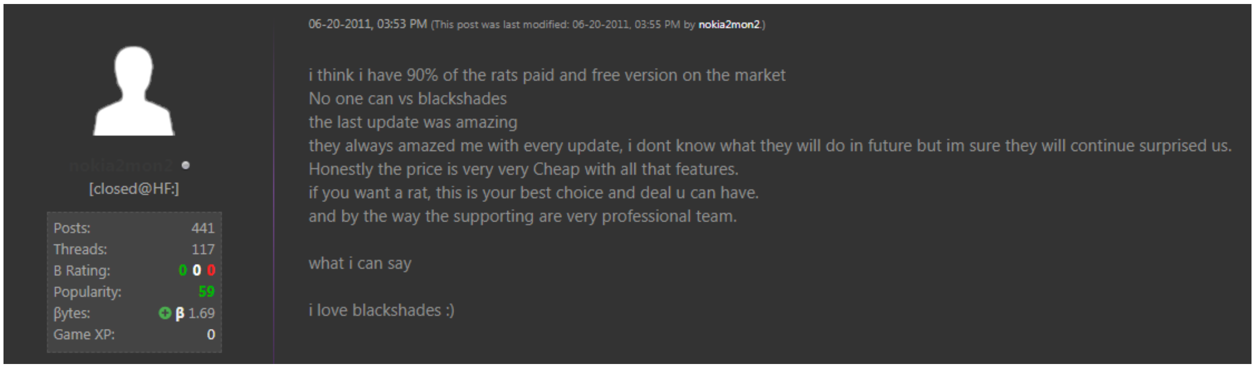
He also mentioned using at least nine crypters:

- Alpha Crypt
- Tejon Crypter v1.2

[59] https://hackforums.net/showthread.php?tid=111226
[60] https://hackforums.net/showthread.php?tid=1250098&pid=12842475#pid12842475

- PolyCrypt
- Damla Protector
- Darty
- Dark Eye
- Dizziness
- Cube
- p3rfix

In the June 2011 post mentioned above, he sang Blackshades' praises, describing it as the "best choice":



nokia2mon2
[closed@HF:]

Posts:	441
Threads:	117
B Rating:	0 0 0
Popularity:	59
βytes:	⊕ β 1.69
Game XP:	0

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 :)

The hosting infrastructure al-Qahtani set up to use Blackshades was identified in the course of this investigation and is detailed in Section V.

Blackshades, which sold for as little as $40 on Hack Forums, targets Microsoft Windows-based operating systems and allows hackers to secretly and remotely control a victim's computer via a graphical user interface. Once infected, a hacker can use the victim's computer to access and modify files; activate the webcam; record keystrokes; steal passwords; and include the computer in a botnet for DDoS attacks.

Al-Qahtani's use of Blackshades is notable, given that the malware was the impetus for what was described by the U.S. Department of Justice (DOJ) as the "largest-ever global cyber law enforcement operation."[61] In May 2014, the DOJ announced that more than 90 people had been arrested in 19 countries to combat the sale and use of the RAT, which had been purchased by thousands of individuals in more than 100 countries and had infected more than 500,000 computers. The two-day operation involved 359 house searches and the seizure of more than 1,100 electronic devices, according to EUROPOL.[62]

Among those arrested was Blackshades co-creator Michael Hogue, who went by xVisceral on Hack Forums.[63] In an October 2010 post, al-Qahtani wrote that he was having trouble installing the crypted version of Blackshades on 100 machines.[64] xVisceral remotely accessed al-Qahtani's computer (or "tv on

[61] https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection
[62] https://www.europol.europa.eu/newsroom/news/worldwide-operation-against-cybercriminals
[63] https://blog.malwarebytes.com/cybercrime/2012/07/blackshades-co-creator-arrested/
[64] https://hackforums.net/showthread.php?tid=742597&pid=7118882&highlight=blackshades#pid7118882

my pc," as al-Qahtani put it) and installed 20 uncrypted versions on 20 machines "and its work great.. very great."

Al-Qahtani may have used Blackshades for DDoS attacks (there is overlap between DDoS bots and RATs with DDoS capabilities). However, he also showed an interest in remotely accessing the microphones of computers to create secret recordings.

In a May 2013 thread, al-Qahtani offered $100 for the best recommendation on how to surreptitiously record a room, save the file and upload it to his web server or send it to himself via email.[65] He said he had physical access to about 10 Windows computers and that he needed to know which PC the recording had come from. "its must save the voices in the rooms in the best quality, and its must be very stable, and upload the sound file every 3 hours or something like that," he wrote. "and offcourse all must be hidden so no one knows that his voice is recorded."

One Hack Forums member suggested that he use a RAT along with a recording program, but al-Qahtani replied that he had tried that but wanted a more professional solution: "that what i used and i dont like it, i want better profeseenal way." A user called "Glassy"[66] suggested the winning solution, though apparently via private message or in a now-deleted post. Al-Qahtani appears to have continued to work behind the scenes with Glassy. A year and a half after suggesting the winning solution, Glassy described al-Qahtani as "my best partner" in a post lauding the Saudi for donating to Hack Forums.[67]

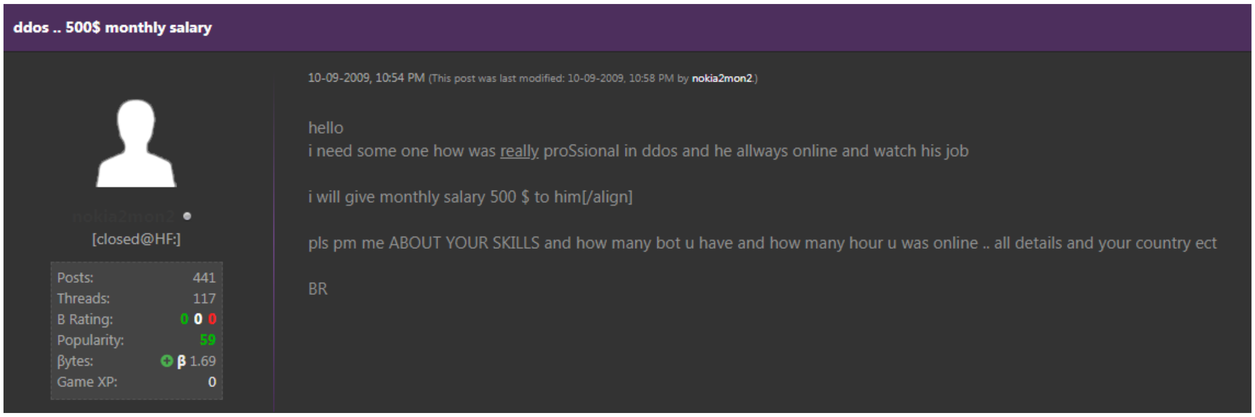
Tried To Hire DDoS Professional To Manage Botnet

As with RATs, al-Qahtani said he purchased and used "almost all" of the DDoS bots for sale on Hack Forums.[68] Among the DDoS bots and DDoS for hire services he used were:

- D-Doser (versions 3.6 and 4.2)
- ChickenX Shell Shop
- Optima
- 3vBot
- Tippy's DDOS service
- OncleSam DDOS service

Initially, al-Qahtani attempted to hire someone to manage his botnet and DDoS for him. In October 2009, a few months after he joined the forum, al-Qahtani posted an ad for someone who was skilled in DDoS attacks, offering a salary of $500 per month.[69]

[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
[69] https://hackforums.net/showthread.php?tid=161701



ddos .. 500$ monthly salary

nokia2mon2

[closed@HF:]

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

10-09-2009, 10:54 PM (This post was last modified: 10-09-2009, 10:58 PM by nokia2mon2.)

hello
i need some one how was really proSsional in ddos and he allways online and watch his job

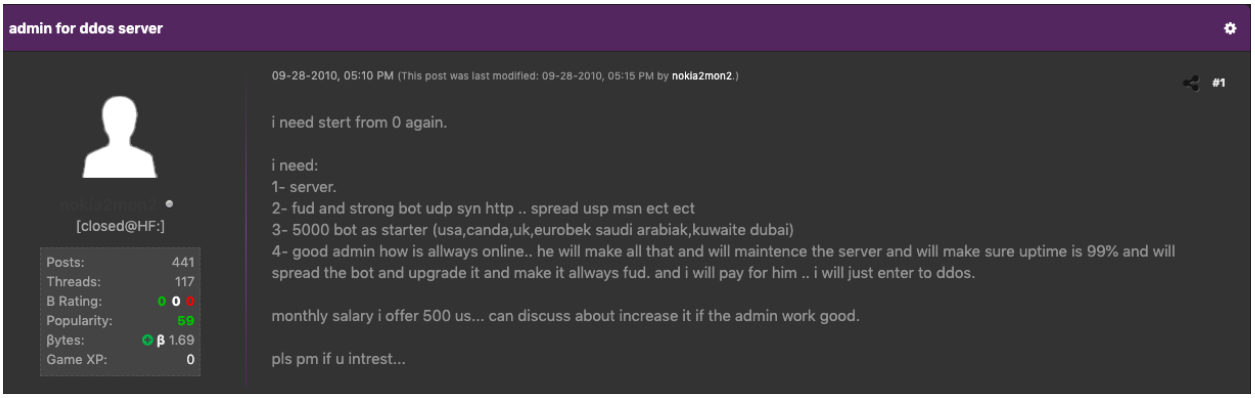
i will give monthly salary 500 $ to him[/align]

pls pm me ABOUT YOUR SKILLS and how many bot u have and how many hour u was online .. all details and your country ect

BR

After no one replied, he upped the salary to $700 per month and wrote, "my first dude stope working becuse his educiton." Al-Qahtani later wrote that he was "stell waiting" for a response.

A year later, in September 2010, he published a thread titled, "admin for ddos server" in which he wrote that he was starting "from 0 again" and that he needed a good admin that he was willing to pay $500 per month.[70] He asked for 5,000 bots to start, hosted in the U.S., Canada, U.K., Saudi Arabia, Kuwait, Dubai and "eurobek."



admin for ddos server

nokia2mon2

[closed@HF:]

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

09-28-2010, 05:10 PM (This post was last modified: 09-28-2010, 05:15 PM by nokia2mon2.) #1

i need stert from 0 again.

i need:
1- server.
2- fud and strong bot udp syn http .. spread usp msn ect ect
3- 5000 bot as starter (usa,canda,uk,eurobek saudi arabiak,kuwaite dubai)
4- good admin how is allways online.. he will make all that and will maintence the server and will make sure uptime is 99% and will spread the bot and upgrade it and make it allways fud. and i will pay for him .. i will just enter to ddos.

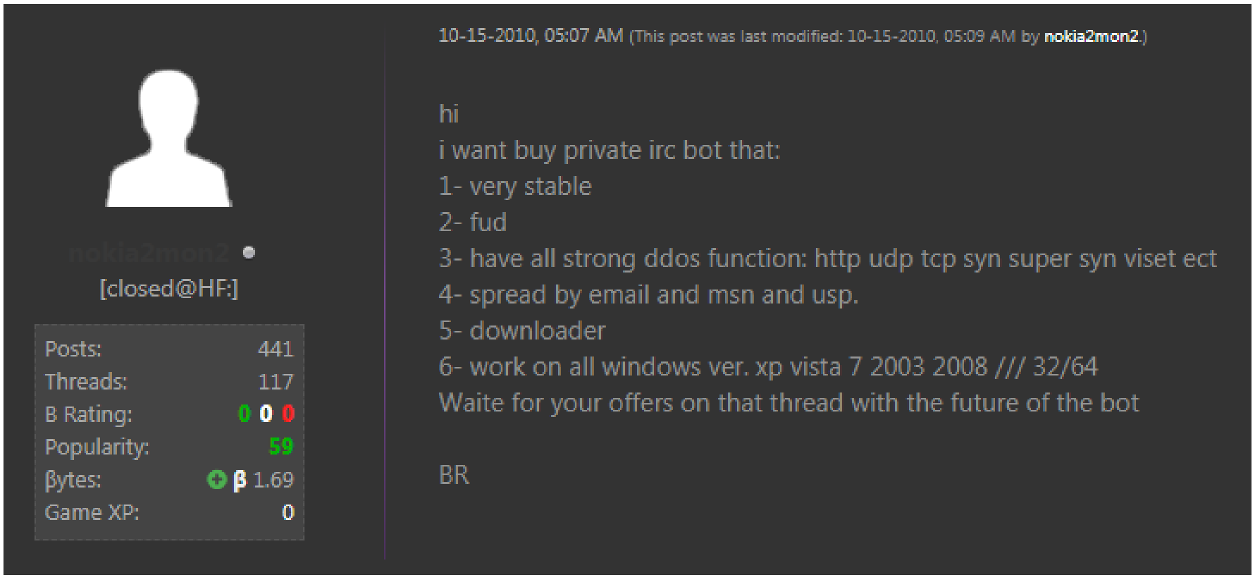
monthly salary i offer 500 us... can discuss about increase it if the admin work good.

pls pm if u intrest...

The following day, he wrote that he had been private messaged (PM'd) by scammers, and that he will ask candidates to DDoS one to two websites "for minute to make sure about u." He added that he would not DDoS more than two to three sites per day and that "for many days i will not do any thing ... but the salary will be paying any way." A user suggested that al-Qahtani was overpaying: "500? i dont know but that seems, a bit much? If you could set it up your self it could be much cheaper. i think, But you sure are rich :P"

In October 2010, he outlined[71] what he was looking for in an IRC bot:[72]

[70] https://hackforums.net/showthread.php?tid=707209
[71] https://hackforums.net/showthread.php?tid=741728&pid=7037024#pid7037024
[72] https://en.wikipedia.org/wiki/Botnet#IRC



nokia2mon2

[closed@HF:]

Posts:	441
Threads:	117
B Rating:	0 0 0
Popularity:	59
βytes:	⊕ β 1.69
Game XP:	0

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

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

Days later, al-Qahtani thought he had paid $250 for "thosands of great bot that have all facility to make heavy ddos attack." Using al-Qahtani's first name in the title of the thread, as described above, a user called RelVlotelVlod described a deal with al-Qahtani that may have been a scam.

RelVlotelVlod claimed that after al-Qahtani paid him for bots on his friend's botnet, his friend banned him. RelVlotelVlod offered to set up an IRC server for a botnet for $20 instead. "he promise he will full support the server and make sure bots not loses and he will give me a full support for every think even update bot crypted," al-Qahtani replied. He also tried hiring RelVlotelVlod: "i promise him that when we finish i will give him a monthly salary."

Al-Qahtani discussed his efforts at DDoSing sites on several occasions. He never named the websites he targeted. In November 2009, he wrote that he was having problems DDoSing a website due to the site's administrator blocking connections from all but one country: "i ddos site from my bots but site not down."[73] In January 2011, he recommended using Optima: "i down large site in 300 bot only .. all my irc bot cant down it in 3-4k :) amazing."[74] The same month, he asked for advice on how to hack or DDoS a PalTalk room with about 2,000 members.[75] In March 2012, he described a DDoS for hire service called OncleSam as "the most professional DDoS Services i used in the hf, i will use it again and again :D"[76] Al-Qahtani took down a site for 48 hours and caused the victim to change their hosting provider, according to his post.

Targeted Users On Major Social Media Platforms, WhatsApp

True to his reputation for being Saudi Arabia's social media enforcer, al-Qahtani paid to have accounts deleted and sought to manufacture engagement activity on major social media platforms, including YouTube and Facebook. He also sought a tool that would allow him to suspend Twitter accounts and

[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

tested an exploit that was supposed to crash a user's WhatsApp. Al-Qahtani also demonstrated his petty side by asking how to kick players from a Facebook game.

Paid To Have YouTube Channel, More Than 20 Videos Deleted

Al-Qahtani sought to artificially boost the popularity of unnamed YouTube accounts and videos and claimed to have had "many" YouTube videos and at least one channel deleted from the platform.

In October 2010, al-Qahtani purchased iTube 2.2, a YouTube bot billed as a "professional YouTube promotion tool."[77] The tool included a slew of features, including "Views Booster," which allows users to artificially increase the number of views on a video using a botnet, and "Mass Flagger," which let users use their YouTube accounts "to flag a competing video and have it removed from youtube."

A year later, in October 2011, he started a thread indicating that he was interested in purchasing 1,000 to 2,000 verified YouTube accounts. "i will change the passwords so its will be for me only.." he wrote. "Your offer please." No one publicly took al-Qahtani up on his request, but the following day, he vouched for a user called "bloodgen" from whom al-Qahtani said he purchased 500 YouTube accounts but received 525.[78] In the same post, he said he had been sold accounts by other users did not work or were not "pva" (phone-verified accounts). The day before, al-Qahtani had also purchased 6,000 YouTube likes.[79] In February 2012, he unsuccessfully tried to order 100,000 YouTube views.[80]

Al-Qahtani also paid Hack Forum members to delete YouTube videos and at least one channel. In February 2011, al-Qahtani vouched for a user called "ruNe0," who offered to delete any YouTube video for as low as $6. (When asked to delete a Justin Bieber video, ruNe0 conceded that he could not: "Hihihi its impossible this kid so famous and partner too, it's me who is to be banned = D.") Al-Qahtani said ruNe0 "delete for me many many youtube video .. all deals was smooth."[81] A month later, al-Qahtani vouched for ruNe0 again and said that he deleted "more than 20 videos" for him.[82] In October 2011, al-Qahtani told ruNe0 that he had PM'd him a new channel to delete, suggesting that ruNe0 had deleted at least one channel for al-Qahtani previously.

In June 2013, al-Qahtani started a thread titled, "delete video in youtube 200$," writing, "tell me the time u need to do the job ,, i want ASAP."[83] Two days later, a user called "Venture Mogul" wrote that he got it taken down. Al-Qahtani replied, "check your paypal , u got the 200$ … Regards."

In April 2016, al-Qahtani started a thread indicating that he was looking for someone to build a YouTube bot that would:[84]

[77] https://hackforums.net/showthread.php?tid=753917&pid=7256067#pid7256067
[78] https://hackforums.net/showthread.php?tid=749400&pid=16603568#pid16603568
[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&pid=10088370#pid10088370
[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&highlight=youtube

> *1- use proxy list with ports (private proxy)*
> *2- show all the names and can change it and support unicode*
> *3- increase view*
> *4- increase like / dislike*
> *5- comment from the php and chose to send it or save in library and then can send them all or just what check box on it*

He specified that the tool could only be for him. He did not indicate in the thread whether he had been successful in finding a coder for the project.

Sought Tool To Ban Twitter Account

In June 2011, al-Qahtani tried to buy tools that would let him ban Twitter accounts: "i want buy tools that can banned or freeze twitter account. any offer?"[85] After receiving few responses, he wrote that he would pay $500 for a tool that would even "freeze" an account for 24 hours if he could do it repeatedly. One user suggested that such tools do not exist, "but if you have access to the database for twitter then you can do anything."

In April 2012, al-Qahtani asked about a Twitter account-cracking tool being sold for $20.[86] "how fast is it? how many password in second its try?" He also asked whether it would bypass CAPTCHAs.

In October 2018, The New York Times reported that al-Qahtani was the strategist behind an effort to harass and silence critics of the kingdom on Twitter by using troll farms consisting of hundreds of young men in and around Riyadh.[87] The Times also reported that a Twitter employee, Ali Alzabarah, was persuaded by Saudi intelligence "to peer into several user accounts, according to three of the people briefed on the matter." Alzabarah, who joined Twitter in 2013, had access to users' personal information and account activity, including IP addresses and phone numbers. He was fired in 2015, despite Twitter having found no evidence that he provided the Saudi government with Twitter data. He returned to Saudi Arabia and now works in the government, according to a Times source.

Owned "Many Facebook Accounts"

In February 2011, al-Qahtani started a thread titled, "facebook script or software that can add like and comments for thousand of accounts."[88] It is not clear from the post whether he owned thousands of Facebook accounts or if he wanted a tool that would allow him to like and comment on thousands of accounts' posts. "i have many facebook accounts," he wrote. "i want the best software/script that i can insert all the accounts on it and send command by the software/script.. and its do the like from all the accounts and add comments.."

A day after he submitted the thread, he wrote that he was "steel waiting."

[85] https://hackforums.net/showthread.php?tid=1431286&pid=13126931&highlight=twitter#pid13126931
[86] https://hackforums.net/showthread.php?tid=2424661&pid=21968194&highlight=twitter#pid21968194
[87] https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html
[88] https://hackforums.net/showthread.php?tid=1065979&pid=9894520#pid9894520

Tested Exploit For Crashing WhatsApp

Al-Qahtani also indicated an interest in WhatsApp tools. In December 2014, he wrote that he tried using an exploit that would crash a users' WhatsApp, but it did not work for him on iOS.[89]

In May 2015, he started a thread asking for the "best whatsapp panel bulk/checker in market."[90] Two users responded, but al-Qahtani did not post again in the thread.

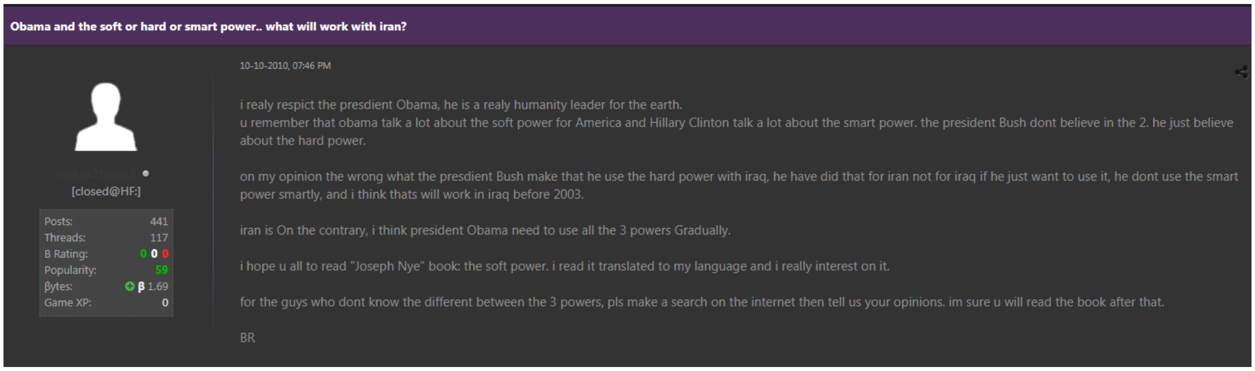
Wanted To Kick Players From Facebook Game, Bought Coins For 8 Ball Pool Game

The only other reference to Facebook identified was in April 2013, when he offered to pay $500 for a script that would show the IP address of players in a Facebook game called War Commander. "i need software show me any player ip in the same sector or other sector by there id or name. i will pay 500$ for that,, and mybey i will increase that if i like what i see. i will use it to kick some bad players ;)."

In October 2014, he also suggested that he had hacked the game 8 Ball Pool for iOS. The same day, he offered to buy all of the 8 Ball Pool coins being sold by a user ($2 for one million coins), and in another post on the same day, he offered to buy an 8 Ball Pool account with one billion coins for $700, even though another user claimed to have recently sold their one billion-coin account for $25.

Opined About God, Obama, Kashmir

In four posts on October 10 and 11, 2010, al-Qahtani opined on subjects unrelated to hacking, including Iran, Kashmir and religion. Al-Qahtani started a thread titled, "Obama and the soft or hard or smart power.. what will work with iran?" in which he called then-President Obama "a realy humanity leader for the earth" and argued that President Obama needed to use soft, smart and hard power when dealing with Iran.[91]



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

nokia2mon2
[closed@HF:]

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

10-10-2010, 07:46 PM

i realy respict the presdient Obama, he is a realy 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

In a thread on India and Pakistan, al-Qahtani weighed in on the Kashmir conflict: "the only solution is give Kashmirs people The right to self-determination under UN auspices, or make it a Separate Nation."[92]

[89] https://hackforums.net/showthread.php?tid=4566034&pid=43622761#pid43622761
[90] https://hackforums.net/showthread.php?tid=4819790&pid=46116587#pid46116587
[91] https://hackforums.net/showthread.php?tid=732501&pid=6955346#pid6955346
[92] https://hackforums.net/showthread.php?tid=720377&pid=6965503#pid6965503

In another thread, he offered his thoughts on religion and politics:[93]

> *Religion, its source is the naked emotion of personal choice of the individual Vmenbah The science of mind and thinking it is the absolute truth. The most serious challenge the new world order is the control of religious attitudes on the political decision-politics and religion whenever they met it was a declaration of war.*

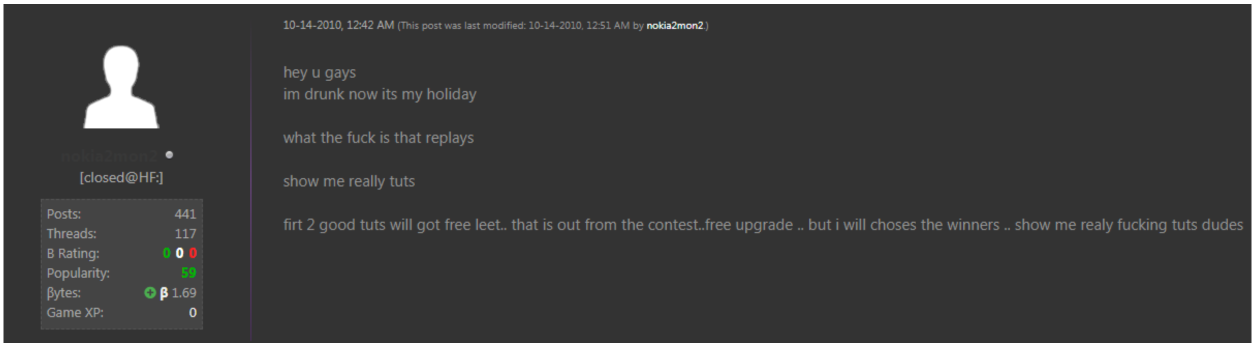
In a thread titled, "Prove God Exists," he advocated[94] for an argument known as "Pascal's wager":[95]

> *Can not prove the existence of God scientifically as you can not deny its existence scientifically. There is a famous thinker named Pascal said a beautiful words: I believe in the existence of God because there are two possibilities, either one can be located:*
> *1- if he is there he will give me the heaven after a die.*
> *2- if he is not there there nothing to lost when i believe his story :)*

Posted While Drunk

Al-Qahtani wrote that he was drunk in three posts at the end of 2010. Alcohol is illegal in Saudi Arabia and punishable by flogging or worse, though it has been reported that some members of the royal family have flouted the prohibition with impunity.[96]

In October 2010, al-Qahtani sponsored a contest for the best tutorials pertaining to a range of subjects, including programming, graphics, hacks and exploits.[97] The winners of the contest received forum upgrades purchased by al-Qahtani. Responding to the apparently lackluster response, al-Qahtani wrote that he was drunk and wanted better tutorials:



nokia2mon2
[closed@HF:]

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

10-14-2010, 12:42 AM (This post was last modified: 10-14-2010, 12:51 AM by nokia2mon2.)

hey u gays
im drunk now its my holiday

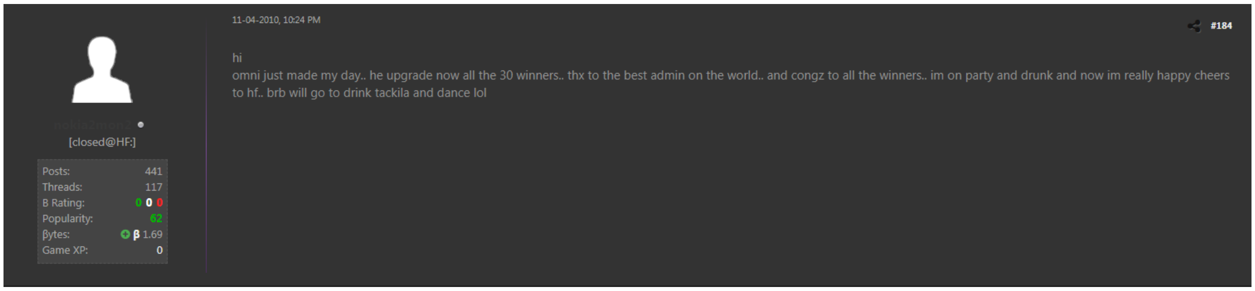
what the fuck is that replays

show me really tuts

firt 2 good tuts will got free leet.. that is out from the contest..free upgrade .. but i will choses the winners .. show me realy fucking tuts dudes

The following month, al-Qahtani sponsored another contest.[98] When the contest was over, he congratulated the winners and wrote, "im on party and drunk and now im really happy cheers to hf.. brb will go to drink tackila and dance lol."

[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-cables-saudi-princes-parties
[97] https://hackforums.net/showthread.php?tid=738021&pid=7014461#pid7014461
[98] https://hackforums.net/showthread.php?tid=781348&pid=7485785#pid7485785



nokia2mon2
[closed@HF:]

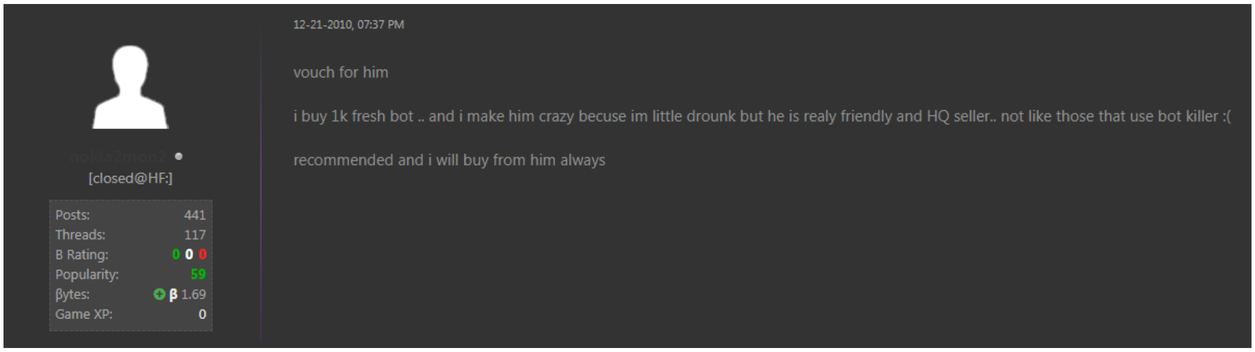
Posts:	441
Threads:	117
B Rating:	0 0 0
Popularity:	62
βytes:	β 1.69
Game XP:	0

11-04-2010, 10:24 PM

#184

hi
omni just made my day.. he upgrade now all the 30 winners.. thx to the best admin on the world.. and congz to all the winners.. im on party and drunk and now im really happy cheers to hf.. brb will go to drink tackila and dance lol

In December 2010, al-Qahtani wrote that he was a "little drounk" in a post vouching for a user from whom he said he purchased 1,000 bots:[99]



nokia2mon2
[closed@HF:]

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

12-21-2010, 07:37 PM

vouch for him

i buy 1k fresh bot .. and i make him crazy becuse im little drounk but he is realy friendly and HQ seller.. not like those that use bot killer :(

recommended and i will buy from him always

Used PayPal, Provided Hotmail Email

As seen in the screenshot in the beginning of this section, al-Qahtani wrote in his first Hack Forums post that he used PayPal to buy malware from the user stronger7. He would mention using PayPal for various purchases in at least a dozen other posts. In an April 2016 post, he specified that he could pay only via PayPal or Visa.[100]

According to information leakage from PayPal's password recovery site, saudq1978@gmail.com is connected to a PayPal account linked to a Visa ending in 10 and the following partially redacted phone number: 05* *** *750 that corresponds with al-Qahtani's Saudi Telecom Company cell phone number, +966 55 548 9750.[101]

In a December 2010 post, al-Qahtani sought to purchase 3,000 installs or updates.[102] He wrote that he would pay via "pp only," referring to PayPal. He also provided a new email address: nokia2mon2@hotmail.com. He posted the email address at least one other time two months earlier, in October 2010, when he asked the seller of a Windows server exploit to add him on MSN.[103]

Nokia2mon2@hotmail.com is connected to a Microsoft Live account and a Skype profile with the handle "test test 1." According to information leakage from Microsoft Live's password recovery page, the email

[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
[102] https://hackforums.net/showthread.php?tid=890641&pid=8276669#pid8276669
[103] https://hackforums.net/showthread.php?tid=746882&pid=7144180#pid7144180

address is connected to a partially redacted phone number (********72) and email address (al*****@hotmail.com) that were not identified during the course of this investigation.

Paid $1,500 For Hack Of Hotmail Accounts

Al-Qahtani hired Hack Forum members to hack specific Hotmail accounts and provide him with the credentials. In October 2010, he started a thread offering to pay $300 for the password to a Hotmail account.[104] Ten days later, he wrote that many users had tried but failed to hack the account. “i don't have any info about the account, only the account id, if any one can do it pls pm me.”

In March 2012, al-Qahtani started a thread requesting the hack of three Hotmail accounts, offering to pay $500 for each account.[105] He edited the thread six days later indicating his success: “i hacked the emails,” he wrote. “the offer is finished.”

Days later, al-Qahtani wrote that Microsoft had locked him out of one of the Hotmail accounts he had hacked. He posted the message he received, which read in part, “Often customers get here because someone else has access to your account and are using it without your knowledge to send spam.” Al-Qahtani said that his IP address was in the same country as the genuine account owner and that he knows the account owner’s “town and name only.” He did not say whether or not he had any luck getting back into the compromised account.

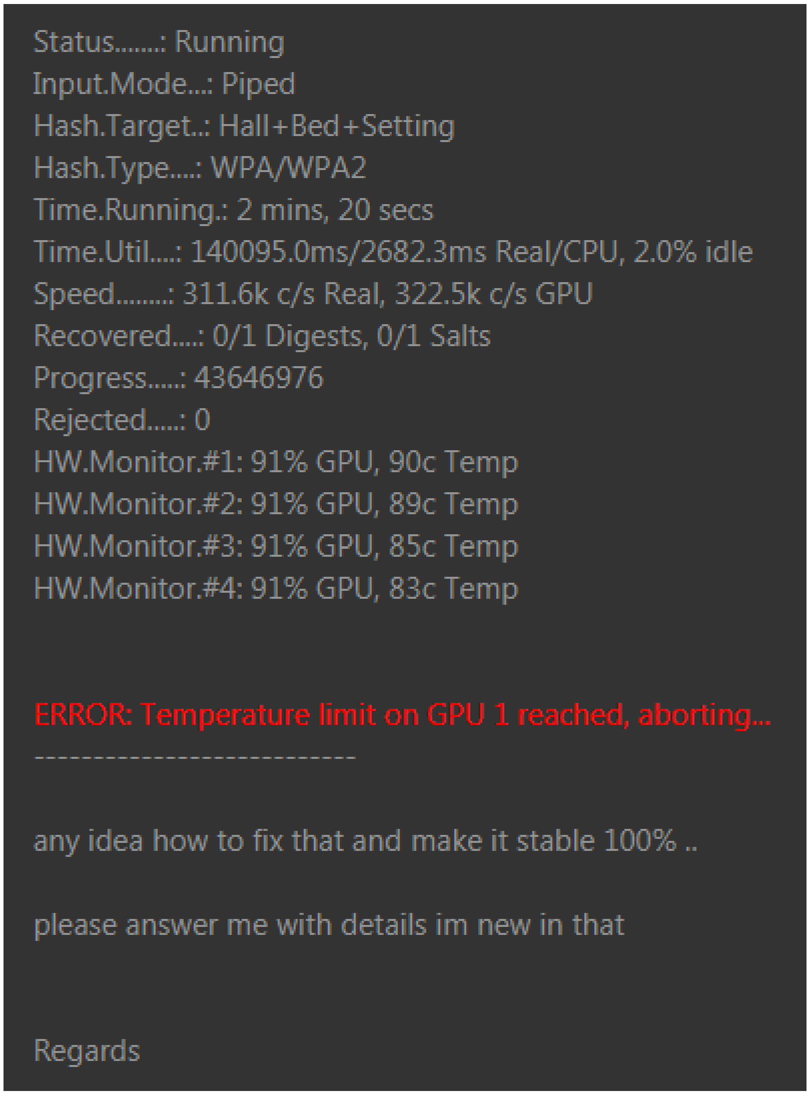
Tried Cracking Wireless Networks, Published First Script

Al-Qahtani showed an interest in cracking wireless networks (e.g. Wi-Fi) beginning in 2011. In September 2011, he responded to a thread by a user called “Middle,” who offered to sell their hacking skills or teach others for a fee.[106] Al-Qahtani wrote that Middle gave him “great lessons” on wireless cracking.

Two months later, in November 2011, al-Qahtani started a thread explaining that the wireless cracking tool Pyrit was not reading his graphics card and offered $20 to whomever could “fix it to me by tv and show me what was the wrong and how i can use pyrit.”[107]

Al-Qahtani indicated that he was using BackTrack 5 R, a predecessor to the penetration testing Linux distribution Kali Linux. Days later, he posted a thread asking for help with oclHashcat, a password cracking tool.[108] According to the tool’s output, which al-Qahtani included in his post, his system was overheating while trying to crack a hashed Wi-Fi password (WPA/WPA2), causing the tool to abort.

[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

Al-Qahtani concluded his Hashcat thread by explaining he was new to wireless cracking: "please answer me with details im new in that." Three years later, in December 2014, he shared[109] "a small script to help you crack WPA/WPA2" and posted a link to a Pastebin post[110] titled, "Red Lions WPA/WPA2 Cracker V1 BETA" (Red Lions was a Hack Forums group headed by al-Qahtani).

He wrote in the comments of the script that it was the first he had written and that it was "intended for the sole purpose of penetration testing only." Al-Qahtani created the Pastebin post using an account with the same username as his Hack Forums profile, nokia2mon2.[111] The account was created the same day that he shared the script on Hack Forums, and there were no other pastes under his account.

[109] https://hackforums.net/showthread.php?tid=4580080&pid=43766880#pid43766880
[110] https://pastebin.com/A7HMFDWQ
[111] https://pastebin.com/u/nokia2mon2

Sought iOS Spyware

In 2014 and 2015, al-Qahtani requested hacking tools for Apple products. In March 2014, he posted a thread asking whether any RATs existed that could infect Macs.[112] Some users mentioned jRAT but suggested that it was no longer being sold. As was often the case, al-Qahtani's request was time sensitive: "any other option guys?????? i need it now :D"

In October that same year, a user called "Sam Sung" started a thread in which he described seeing a spyware app on his friend's iPhone 5. In what was almost certainly a scam post, Sam Sung said that he tried to find the spyware online, but his friend said the developer wanted to keep a low profile to keep it hidden from Apple. Al-Qahtani was the first to comment on the thread, writing, "if u find it i will buy it and will give u bonus if its will work."[113] Sam Sung replied the next day, "hi yes I found it,please PM me your skype."

Tried Buying Fake Traffic For Twitter Follower's Website

In January 2012, al-Qahtani posted a thread asking to buy 100,000 visits to "a page on http://twitemail.com" and specified that delivery must be within 24 to 48 hours.[114] "i dont care if its fake.. its must only increase the counter." Twitemail.com was and continues to be registered to a Saleh Al-Zaid in Riyadh, according to Whois records. The domain redirects to twitmail.com, which is also owned by al-Zaid. Twitmail allows users to share their emails on Twitter, according to the website.

Zaid is a "partner technology strategist" for Microsoft in Riyadh, according to his LinkedIn profile.[115] He is also the CEO of LunarApps, a company he founded in 2011. Twitmail is one of LunarApps' three main products, the other two being Untiny.com — a shortened link expander — and TwtBase.com, a "classified directory of Twitter apps in the market," according to Zaid's LinkedIn profile.

Al-Zaid[116] and al-Qahtani follow each other on Twitter.

Sought Dedicated Server In Russia Or China To Host Exploits, Botnet

In 2010, al-Qahtani twice asked about purchasing servers for hosting exploits[117] and botnets. In October, he started a thread in the "Buyers Bay" sub-forum with the title, "hosting that will be house ing an expliot system and an http bot."[118] His post got right to the point: "i would like to purchase bullet proof hosting that will be house ing an expliot system and an http bot." Nine days later, a user said they could provide good hosting, but less than two months later, in December, al-Qahtani posted another thread with the same request: "need: dedicated server for botnet and exploits."[119]

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

Al-Qahtani expanded on what he was looking for, saying that he wanted a dedicated server located in Russia or China. "If you guys know any good company which are providing dedicated server and they allow irc botnet , exploits , etc . just drop their links .." This second thread received twice as many responses with one user saying that they had PM'd him and another cautioning that such servers could be expensive, but "For Russia check out wahome.ru."

In fact, al-Qahtani had been using a U.S.-based hosting provider, ThePlanet.com, which had a reputation for showing persistent malicious behavior, such as hosting botnets or drive-by download sites.[120] The following section details al-Qahtani's hosting infrastructure.

[120] https://krebsonsecurity.com/2010/03/naming-and-shaming-bad-isps/

V. Domains

This investigation assesses with medium to high confidence[121] that the following 22 domains were registered by al-Qahtani since 2009:

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

Al-Qahtani demonstrated exceptionally poor operational security when registering nearly all of these domains. The Whois records of all but three (saudq[.]com, saudqq[.]com and jasmn[.]info) included either

[121] False or inaccurate data can be submitted in Whois records. Therefore, this investigation has *medium confidence* in al-Qahtani's ownership of domains that were a) identified primarily through Whois records containing al-Qahtani's contact information and b) no other corroborating evidence was identified. This investigation has *high confidence* in al-Qahtani's ownership of domains that were identified based on multiple, complementary pieces of evidence. The medium confidence judgment—rather than low confidence—in al-Qahtani's ownership of domains based primarily on Whois records is due to several factors: a) al-Qahtani has included his name and contact information in Whois records for domains (e.g. markaz-royal[.]com) that this investigation judges with high confidence are owned by al-Qahtani, meaning this practice is consistent with al-Qahtani's known behavior; b) in this same vein, using contact information or other identifiers that could be directly linked back to him is consistent with al-Qahtani's pattern of sloppy tradecraft; and c) al-Qahtani's contact information had not been leaked when the earliest of the medium confidence domains were registered (2009), meaning someone other than al-Qahtani would have had to have known al-Qahtani's email address, phone number, location and affiliation with the Saudi royal court *and* wanted to create domains using that information. Parsimony suggests that the registrant of these domains was al-Qahtani, who had demonstrated a clear interest in hacking and web infrastructure by 2009, rather than an unidentified individual with an unknown motive.

his personal email address (saudq1978@gmail.com), mobile phone number (+966 55 548 9750) or variations on his real name.

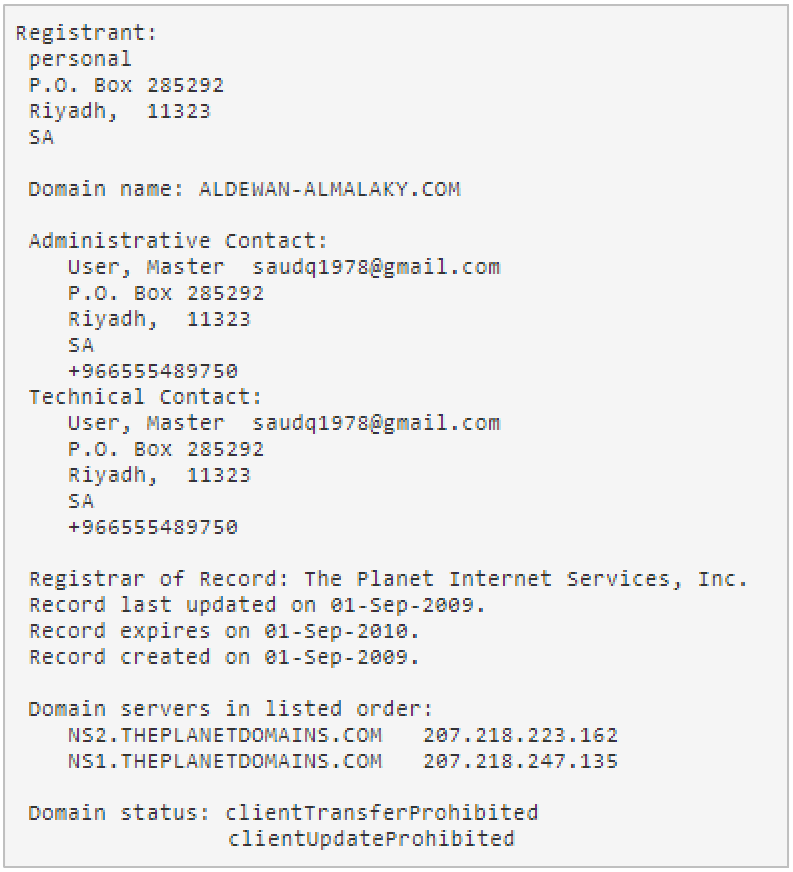
Al-Qahtani's tradecraft was similarly poor when it came to naming domains and subdomains. As with his Twitter and Gmail accounts, he used his first name and last initial for the names of two domains, and he used the same naming convention for at least half a dozen subdomains. He also used his Hack Forums handle on what appears to be one of his most-used domains, markaz-royal.com.

Several of the domains have been used as command and control servers for malware. Only two of the domains are currently active: saudq.com and jasmn.info. The rest have expired.

Note, this section is not exhaustive, and research into al-Qahtani's web infrastructure is ongoing.

Registered First 13 Domains With Gmail And Cell Number

Of the 22 domains identified by this investigation, the first two al-Qahtani created were markaz-dewan[.]net and markaz-dewan[.]com, which were both registered on October 28, 2009. Identical contact information, including al-Qahtani's Gmail and phone number, were listed in the Whois records for both domains. For example:



```
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
```

It is unclear what was affiliated with P.O. Box 285292 in Riyadh in 2009. Since at least 2015,[122] the same P.O. Box has been used by a company called Eras Technology Company (شركة عصور التقنيه), which describes itself as one of Saudi Arabia's leading electrical and mechanical contracting companies.[123]

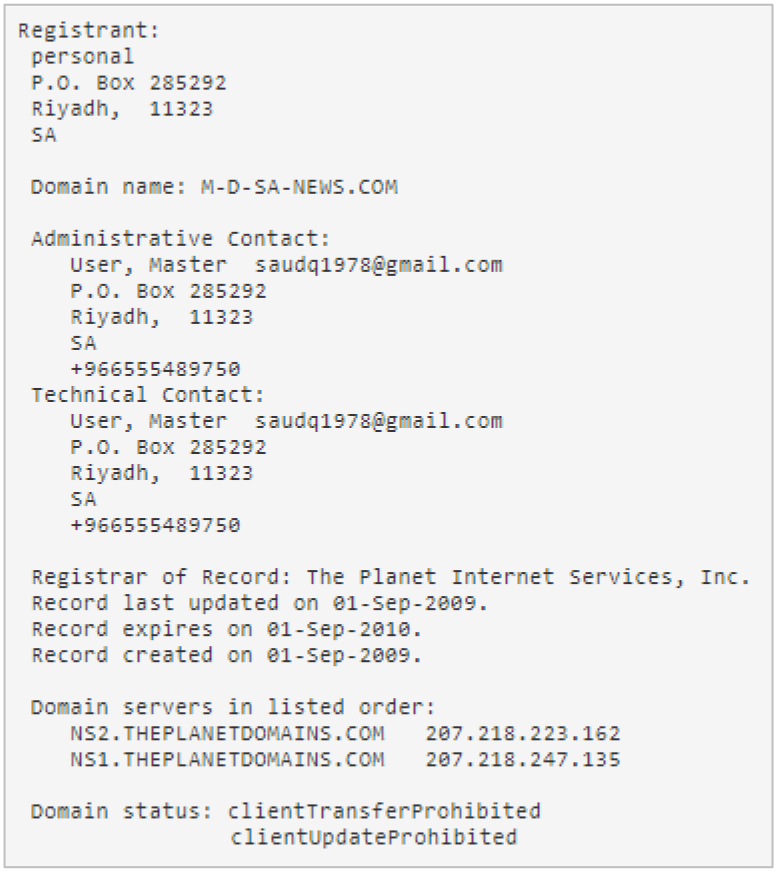
It is also unclear how al-Qahtani used markaz-dewan.net and markaz-dewan[.]com, though if his Hack Forum posts are any indication, they could have been used to host botnets or malware.

Days after registering the markaz-dewan domains, on September 1, 2009, al-Qahtani registered 11 other domains, most of which included the word "dewan," which has several meanings in Arabic, including "office" or "bureau." Some of the domains included the string "royalcourt":

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

The Whois records for the 11 domains contained the same contact information as the two markaz-dewan domains. For example:

[122] https://web.archive.org/web/20150211204347/http:/erastech.com/ContactsUs.aspx
[123] https://erastech.com/?page_id=75476&lang=en



```
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
```

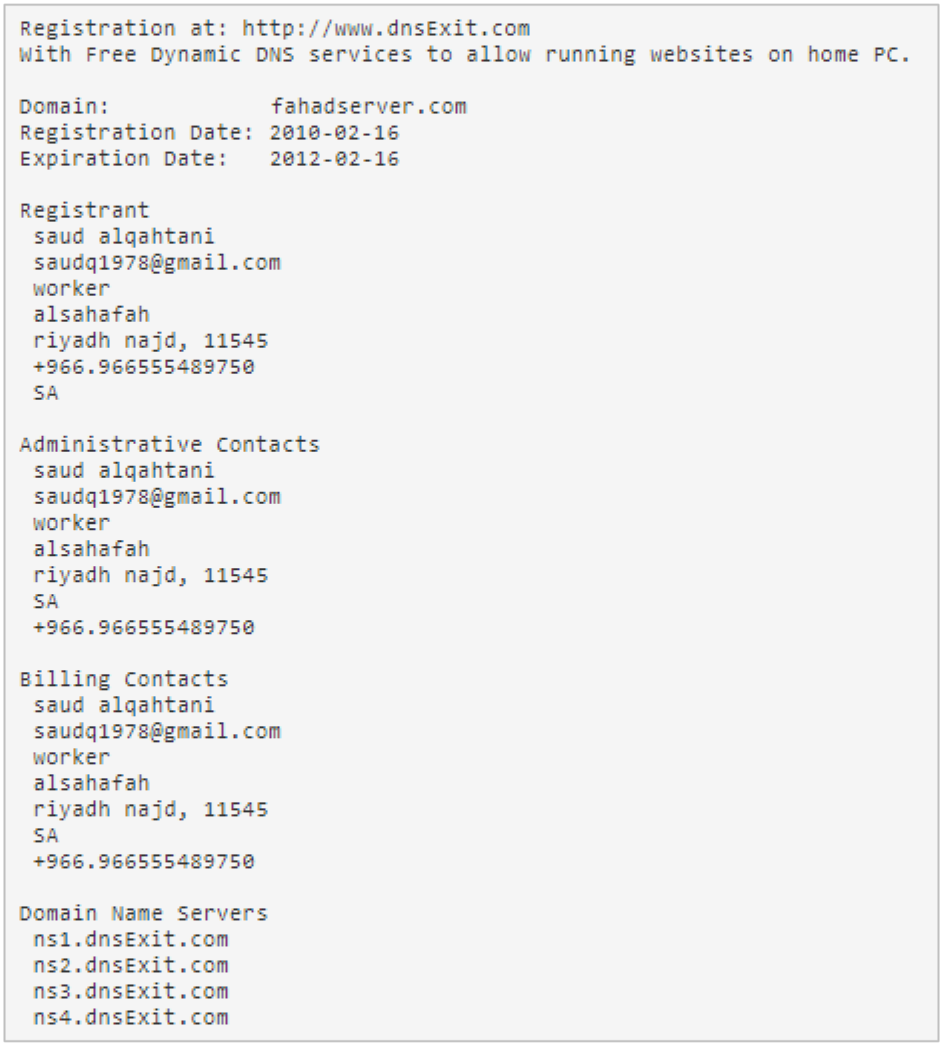
As described above, the official Saudi royal court domain — royalcourt.gov.sa — was not created until 2013. However, al-Qahtani was working within the royal court during this period as the director general of the Center of Media Monitoring and Analysis, which should not be confused with the Center for Studies and Media Affairs in the Royal Court, which he would head a few years later.

The registrations for all 13 of the domains registered in August and September 2009 were set to expire one year after their creation, according to Whois records. This likely explains why al-Qahtani took to Hack Forums in October and December 2010 to inquire about hosting providers in Russia and China that would allow him to host botnets and exploits.

Al-Qahtani let the 11 domains expire in 2010, but he renewed the registration for the two markaz-dewan domains for two more years. They expired on August 29, 2012 and have not been registered since.

Included Real Name In Whois Records

Two months after inquiring about dedicated servers in Hack Forums, al-Qahtani registered fahadserver[.]com in February 2010 and listed not only his personal email address and phone number, but his actual name in Whois records:



```
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
```

Three days earlier, on February 13, 2010, al-Qahtani posted in Hack Forums asking to buy 3,000 bots "from us canada eurpe middleest stable and very fast ..im hurry."[124]

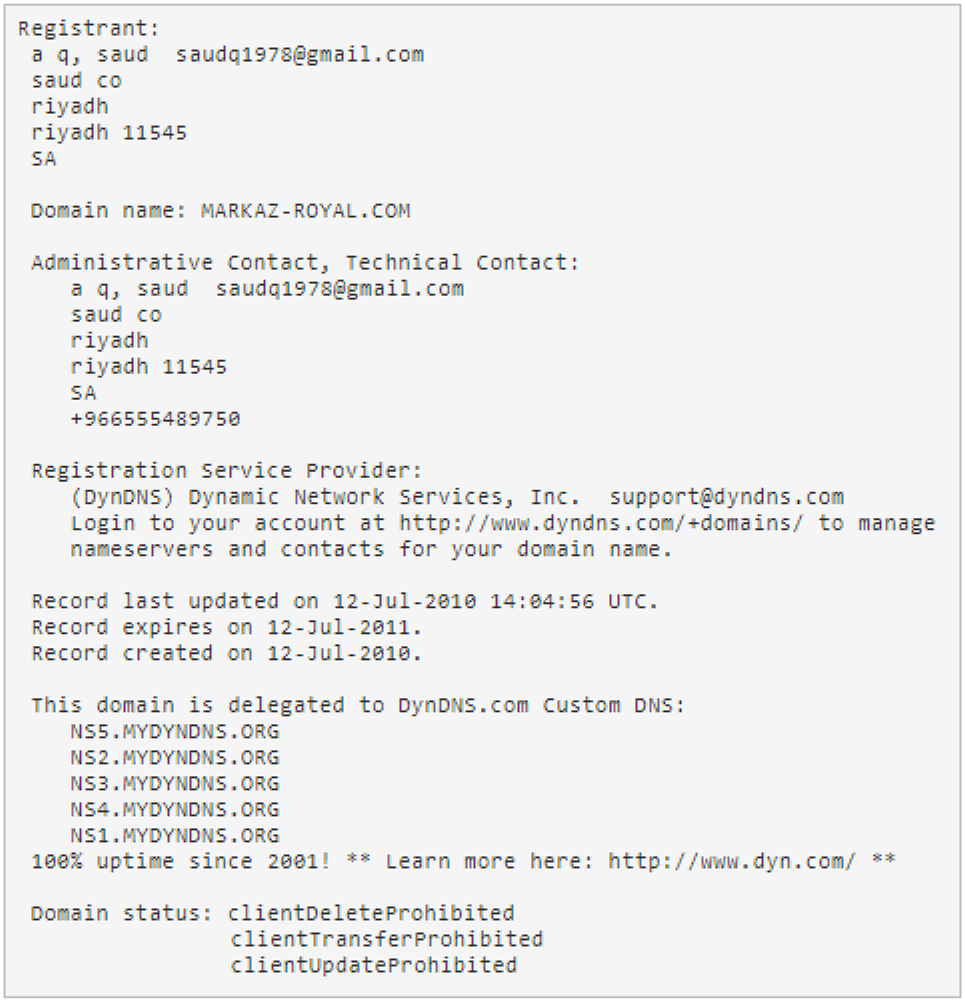
The domain expired in February 2012.

Used "Nokia2mon2" As Subdomain For C2 Server

In July 2010, al-Qahtani continued to use personally identifiable information in Whois records when registering domains when he created markaz-royal[.]com under the name "a q, saud" (as mentioned above, al-Qahtani's middle name is Abdullah, and he signed his name as "Saud Abdullah" in at least one email to Hacking Team).

Al-Qahtani also listed his Gmail and phone number again and included the name of a company, "saud co."

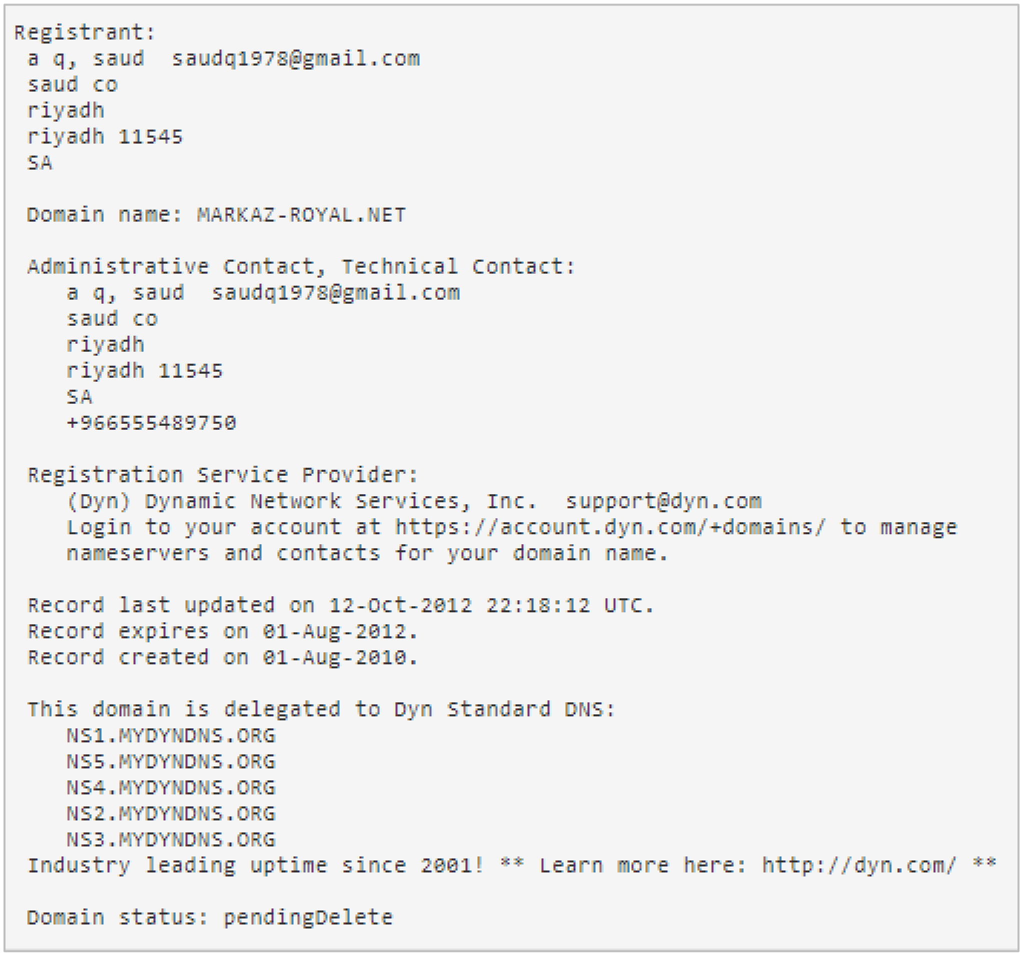
[124] https://hackforums.net/showthread.php?tid=269999&pid=2555346#pid2555346



```
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.MYDYNDNS.ORG
    NS2.MYDYNDNS.ORG
    NS3.MYDYNDNS.ORG
    NS4.MYDYNDNS.ORG
    NS1.MYDYNDNS.ORG
 100% uptime since 2001! ** Learn more here: http://www.dyn.com/ **

 Domain status: clientDeleteProhibited
                clientTransferProhibited
                clientUpdateProhibited
```

The domain was not renewed after a year and expired in July 2011.

In August 2010, less than a month after he registered markaz-royal[.]com, al-Qahtani created markaz-royal[.]net, which he would set up as a command and control (C2) server for Blackshades and other malware. For the first time, al-Qahtani used Whois privacy services so that his name and contact information would not be publicly associated with the domain. He successfully renewed the domain's registration using Whois privacy services in 2011, but from January 2012 to August 2012, when the domain and privacy protection service expired, al-Qahtani's personal information was public:



```
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.MYDYNDNS.ORG
    NS5.MYDYNDNS.ORG
    NS4.MYDYNDNS.ORG
    NS2.MYDYNDNS.ORG
    NS3.MYDYNDNS.ORG
 Industry leading uptime since 2001! ** Learn more here: http://dyn.com/ **

 Domain status: pendingDelete
```

Several subdomains for markaz-royal.net were used by al-Qahtani to host malicious payloads and were detected as running malware such as Blackshades and Darkness/Optima.[125] In another example of sloppy tradecraft, al-Qahtani used his Hack Forums username as a subdomain — nokia2mon2.markaz-royal[.]net.

That subdomain was included in a list of more than 13,000 hosts identified by the FBI as being involved with Blackshades activity.[126] Specifically, the domains were observed to have received status updates or participated in previous attacks, according to an unclassified private industry notification.[127] Nokia.markaz-royal[.]net was also included in the FBI list.

Nokia2mon2.markaz-royal[.]net was also observed as hosting a shell booter, which allows compromised websites to be used for DDoS attacks.[128] The IP address hosting the subdomain at the time, 77.30.55[.]134, is a dynamic home subscriber IP address owned by Saudi Telecom Co. in Riyadh, according to Whois records.

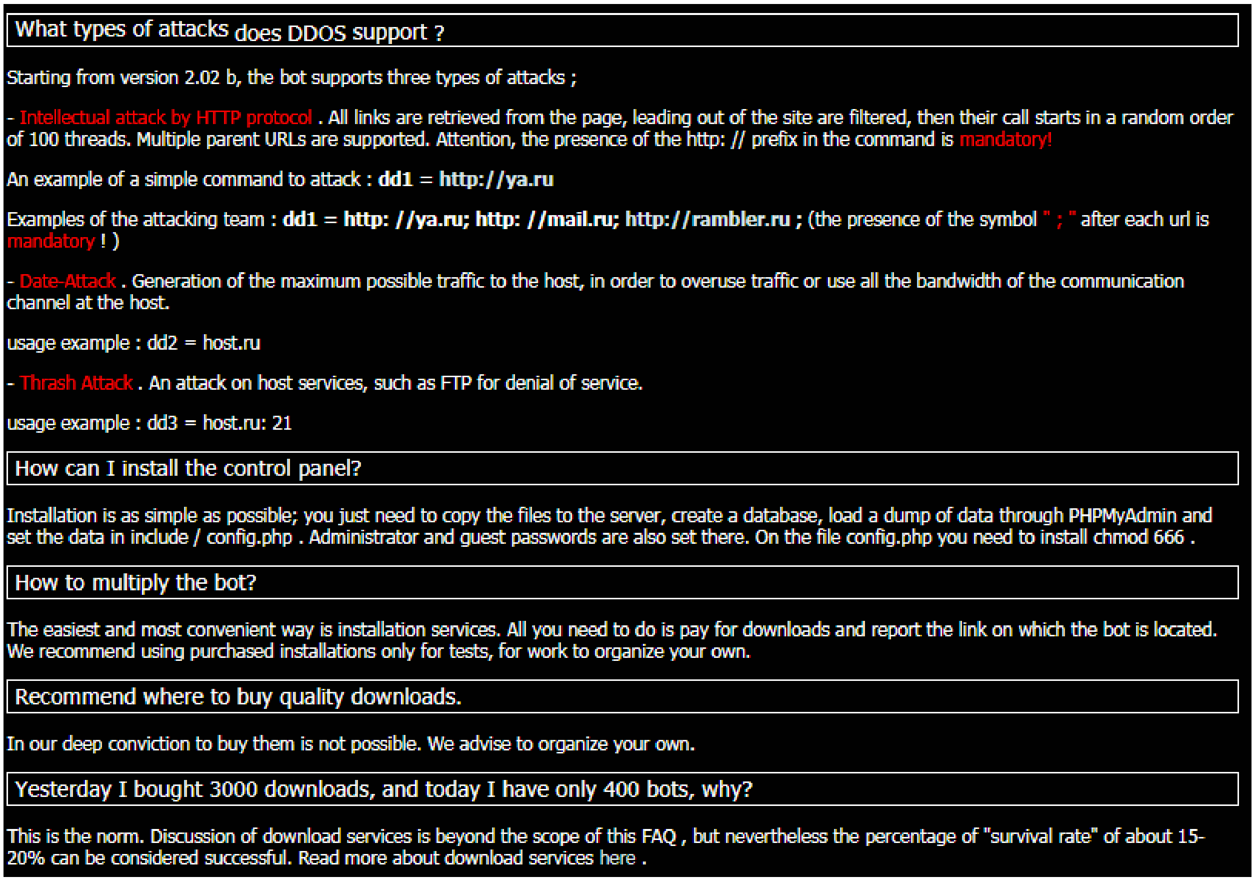
Other subdomains for markaz-royal[.]net have included Al-Qahtani's first name:

[125] https://www.webroot.com/blog/2012/03/08/a-peek-inside-the-darkness-optima-ddos-bot/
[126] https://info.publicintelligence.net/FBI-BlackshadesDomains.txt
[127] https://publicintelligence.net/fbi-blackshades-bulletins/
[128] https://www.exposedbotnets.com/2011/01/nokia2mon2markaz-royalnetshellbooter.html

- Saud.markaz-royal[.]net
- Saud2.markaz-royal[.]net
- Saud4.markaz-royal[.]net
- Saud5.markaz-royal[.]net
- Saud6.markaz-royal[.]net
- Saud9.markaz-royal[.]net

A malicious Windows executable associated with a Russian DDoS bot called Darkness or Optima was observed contacting three hosts: saud4.markaz-royal[.]net, saud5.markaz-royal[.]net and saud6.markaz-royal[.]net.[129]

Two URLs were captured for saud4.markaz-royal[.]net in the Wayback Machine in July 2011 and August 2011: a Russian FAQ page for Optima[130] and the login page for the Optima control panel.[131] The following is an excerpt from the FAQ page machine translated to English:



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 .

[129] https://www.virustotal.com/gui/file/df539e60a2c3c878cc6f0236d0ba7836a1ec1488b9e0320851e9d09d8a55eb3e/ detection

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

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

A malicious executable associated with Nullbot, which al-Qahtani endorsed on Hack Forums, was programmed to contact both saud.markaz-royal[.]net and nokia2mon2.markaz-royal[.]net.[132] Al-Qahtani's first name was also included in the name of at least two files created by the malware when executed by a victim: NullBot_saud[.]exe and NULLBOT_SAUD.EXE-02423B30[.]pf.

Another host, dan.markaz-royal[.]net, was observed[133] as a command and control server for ZeuS malware.[134]

After markaz-royal[.]net's registration expired in August 2012, it was not renewed again until October 2016, when Dave Loftus of Arbor Networks Security Engineering & Response Team in Ann Arbor, Michigan registered the domain and pointed it to a sinkhole[135] at arbor-sinkhole.net for a year.

Two Active Domains Connected To Encrypted Email Service

Al-Qahtani registered two domains — saudq[.]com and jasmn[.]info — that use Hushmail, an end-to-end encrypted email service. Both of the domains are active, though neither has an active website. No historical websites were found for either domain on web page archiving services. Al-Qahtani used the email address saudq@saudq.com in several emails with Hacking Team. Al-Qahtani's jasmn[.]info email address has not been identified.

On November 14, 2014, al-Qahtani posted a thread on Hack Forums offering $100 for a logo for "[his] webmail site" that incorporated the word "JASMN" and resembled the logo of Hushmail.[136] "u can add an idea that shown its secure and encrypted email," he wrote.

HackForum members posted at least a dozen examples, including several that incorporated the generic top-level domain .com, which Qahtani insisted was not necessary: "no need to add .com | its only : jasmn ,, and add something to show its secure and encrypted." The next day, he chose two winners, one of which was this logo:[137]

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

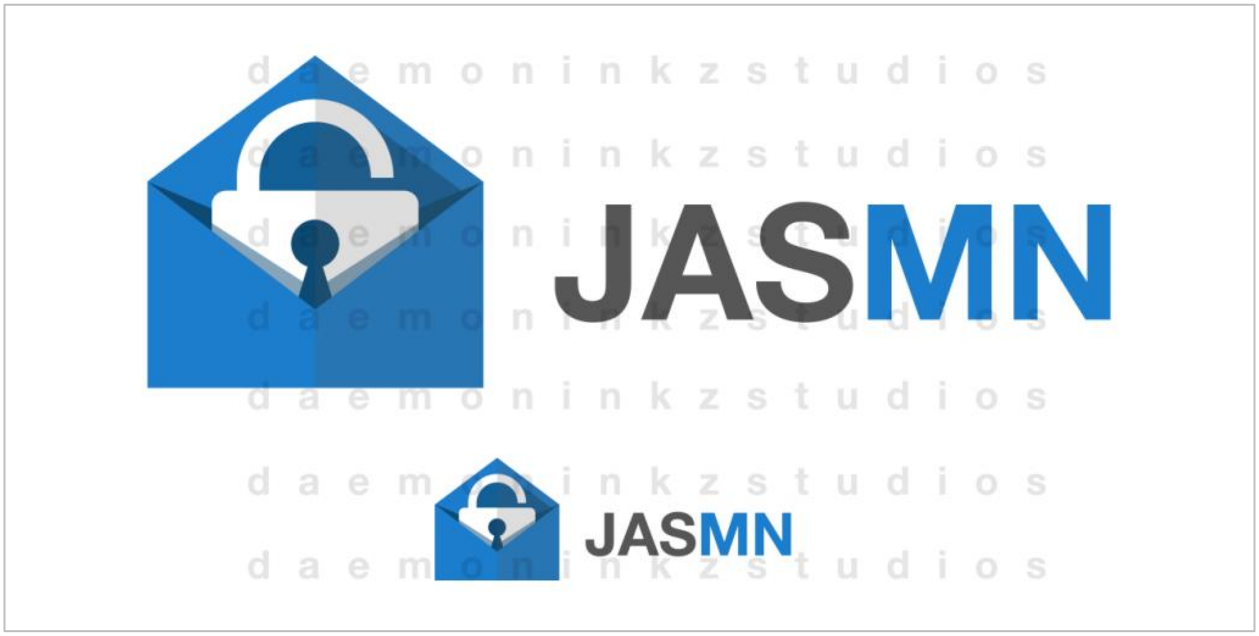
[133] https://zeustracker.abuse.ch/monitor.php?host=dan.markaz-royal.net

[134] https://zeustracker.abuse.ch/faq.php

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

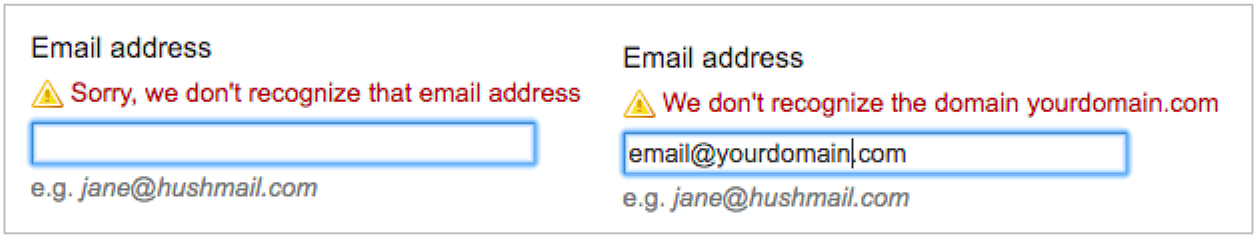
[136] https://hackforums.net/showthread.php?tid=4537112&pid=43323397#pid43323397

[137] https://photobucket.com/gallery/user/demiedealsNegSpace/media/cGF0aDovamFzbG9nb196cHNIZmUwNDFhNS5w bmc



The reason al-Qahtani did not want ".com" incorporated in the logo is because he had registered the domain jasmn[.]info, which was created on November 13, 2014, a day before his logo request on Hack Forums. Jasmn[.]info was identified by reviewing the hosting history of saudq[.]com, which shared an IP address with jasmn[.]info, as detailed below.

Al-Qahtani may use jasmn.info for sending and receiving email. Jasmn.info has two Hushmail servers at plsmtp1.hushmail.com and plsmtp2.hushmail.com. It was possible to confirm that al-Qahtani has a Hushmail account thanks to information leakage from Hushmail's login page. Login attempts with an incorrect email address will return one of the following two messages:



Email address

⚠ Sorry, we don't recognize that email address

e.g. *jane@hushmail.com*

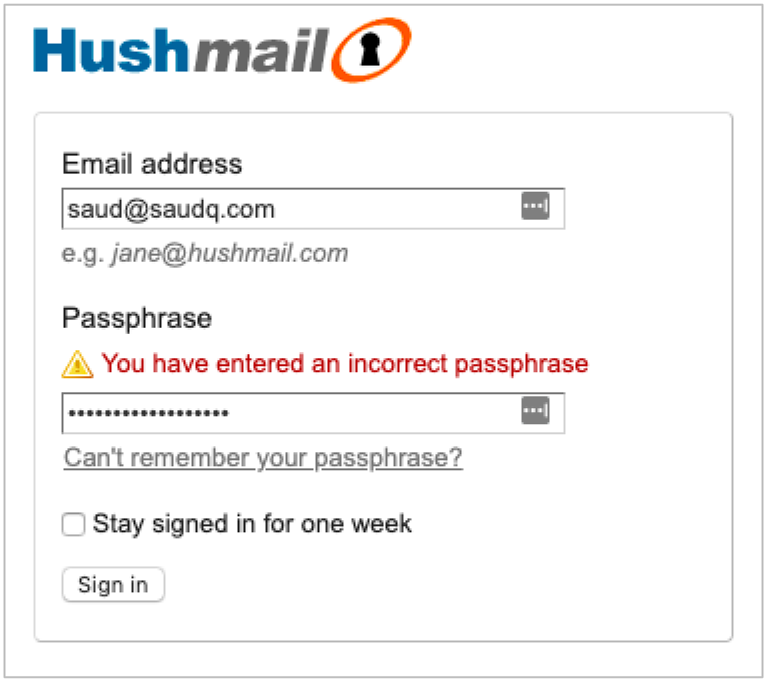
Email address

⚠ We don't recognize the domain yourdomain.com

email@yourdomain.com

e.g. *jane@hushmail.com*

Using al-Qahtani's email address, saud@saudq.com, confirms that the email address and domain have been registered with Hushmail:



Email address

saud@saudq.com

Passphrase

⚠ You have entered an incorrect passphrase

••••••••••••••••••

□ Stay signed in for one week

Throughout the life of the domain, which expires on November 13, 2019, al-Qahtani has used the Whois privacy service provided by Oracle subsidiary Dyn Inc. For approximately a week, the domain was originally hosted at 216.146.39[.]125, a shared server owned by Dyn that currently hosts approximately 3,900 domains. Since November 22, 2014, the domain has been hosted at 148.130.4[.]52, a dedicated server owned by S-MOS Systems, Inc., a defunct San Jose-based company acquired by an Epson Inc. subsidiary in 1998, according to California Secretary of State filings.[138]

The same day that jasmn[.]info was pointed to 148.130.4[.]52, the saudq.com domain — which was created a week before jasmn[.]info — was also hosted on the same server. Saudq.com has since changed hosts twice: in March 2015 to a shared server at 216.146.39[.]125 and in May 2015 to 159.8.206[.]68, which hosts one other domain, saudqq[.]com.

As with jasmn[.]info, Al-Qahtani registered saudq[.]com with Dyn's Whois privacy service, and it is currently active, expiring on November 7, 2019.

Saudqq Domain Used As Malware C2 Server

Saudqq[.]com, which was created in April 2015, has had at least 22 subdomains, including some with strings referencing social media and messaging platforms, such as Facebook, Instagram and Telegram:

- bot.saudqq[.]com
- botman.saudqq[.]com
- cpanel.saudqq[.]com
- am.saudqq[.]com
- quiz.saudqq[.]com

[138] https://businesssearch.sos.ca.gov/Document/RetrievePDF?Id=01210852-6967276

- codequiz.saudqq[.]com
- rsd.saudqq[.]com
- demo.saudqq[.]com
- [redacted].saudqq[.]com[139]
- 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

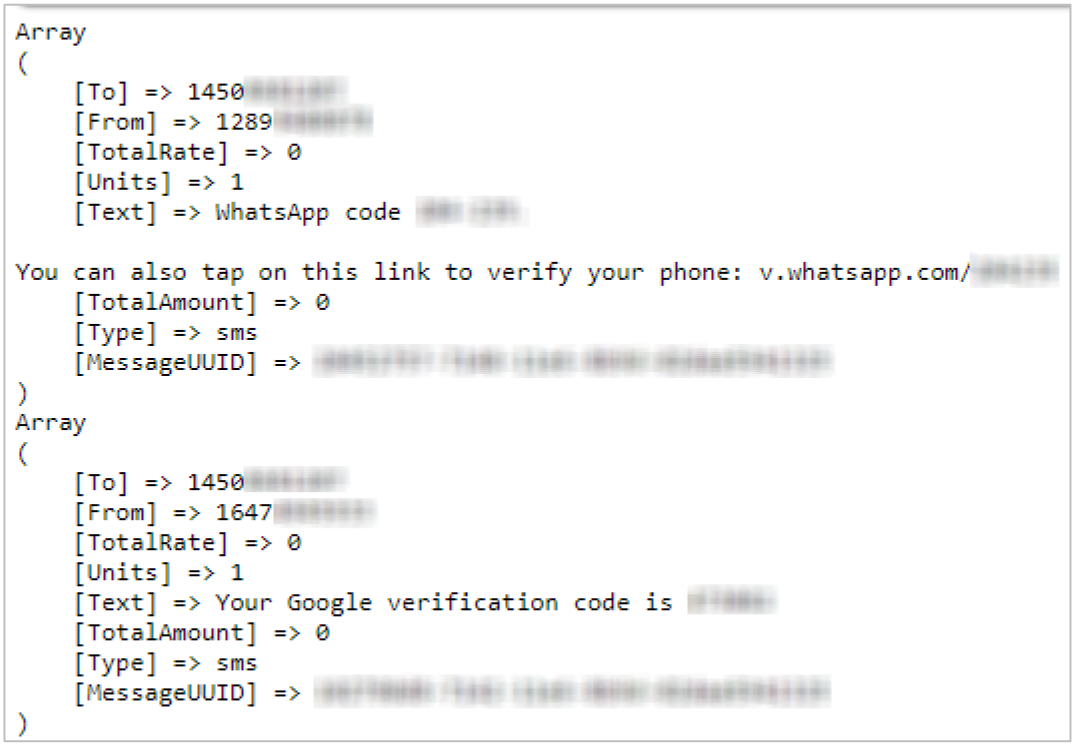
Research into these subdomains is ongoing.

SMS Logs Hosted On Archived Subdomain

In September 2016 and October 2016, two iterations of a text file hosted on [redacted].saudqq[.]com were preserved by the Wayback Machine and include what appear to be SMS logs of two-factor authentication codes, login notifications and other communications sent to approximately one dozen phone numbers across Canada.

The September 2016 capture shows logs for 12 SMS messages to Canadian numbers with area codes for Quebec (450) and Manitoba (204). The messages were sent from Canadian numbers with area codes for Ontario (289, 705), Toronto (647), Montreal (438) and Alberta (403). All of the messages are WhatsApp verification codes, except for one Google verification code:

[139] Some of the information in this section has been redacted to preserve the privacy of individuals who appear to have been targeted by al-Qahtani.



```
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]
)
```

The October 2016 capture contains 142 SMS messages, all of which were sent to Canadian numbers with the Quebecois area code 450. Only five numbers were targeted — two were messaged once each; one was messaged 17 times; another was messaged 47 times; and another still was messaged 76 times. The content of the messages varied widely. Messages appearing to be security or confirmation codes were sent for Coinbase, WeChat, Instagram, Microsoft, VK, WhatsApp, Steam, AirBnB, Viber and AOL.

Some messages included security warnings:

- “Someone is replacing the security info for Microsoft account [redacted]@gmail.com. Not you? https://account.live[.]com/Proofs/Manage”
- “Verification code: [redacted]. The code is only used for removing WeChat restrictions. Do not share it with anyone.”
- “Unusual sign-in for Microsoft account [redacted]. Review at https://account.live.com/a”

Other messages referenced Uber profiles:

- “UBER: Do you need help finishing your Uber profile? Come visit us during our office hours (t.uber[.]com/indy-help) or RSVP for an information session tonight: t.uber[.]com/uber101indy”
- “UBER: Chat live 1-on-1 with an Indianapolis Uber expert now until 10:30AM! We will answer all of your questions and get you on the road as soon as possible: t.uber[.]com/chatlive6”
- “UBER: [redacted], weekends are the best time to earn big driving with Uber! Have questions? Come visit us tomorrow @ 99 E Carmel Dr, Suite 150 - Carmel, IN from 12p-5p!”
- “Uber: Continue the process to partner with Uber by consenting to our driver screening process at https://partners.uber.com. Questions? Visit help.uber.com”

The messages also included spam from the lunch delivery company peachd.com, friend-renting service rentafriend.com and gaming company leovegas.com. Other spam messages for other companies, services and offers did not include links.

The messages were in six different languages in addition to English:

- Arabic (“رمز التفعيل لحسابك في شابك هو”)
- Chinese (“**您申请的手机验证码是：** [redacted]**，请输入后进行验证，谢谢 ！**“)
- Thai (“**ใช้** [redacted] **เพื่อตรวจสอบยืนยันบัญชีผู้ใช้** Instagram **ของคุณ**”)
- Russian (“VK: **Код подтверждения для входа на Вашу страницу ВКонтакте**: [redacted]”
- French (“Collectionnez 6 bonus & vos 90% de l'offre du jour chez JackpotCity. RDV sur www.jpcw[.]in avec sugarmine. Contactez-nous pour desinscription”)
- Spanish (“Usa el código [redacted] para quitar este teléfono de tu cuenta”)

Two shortened URLs were sent in two messages. One, goo[.]gl/sUAPbz, was sent with the message, “Deposit $25 and get up to $5,000 Cashback! Login to your Trade360 account now.” The URL expands to https://www.trade360[.]com/en-gb/trading/?af_chrome_lp=true&af_sub1=English&c=PVnodeposit_Oct10&pid=SMS&af_channel=Email+Marketing&af_keywords=Conversion&view=trading.cashier. None of the dozens of files identified by VirusTotal as referencing trade360[.]com have been detected as being malicious.[140]

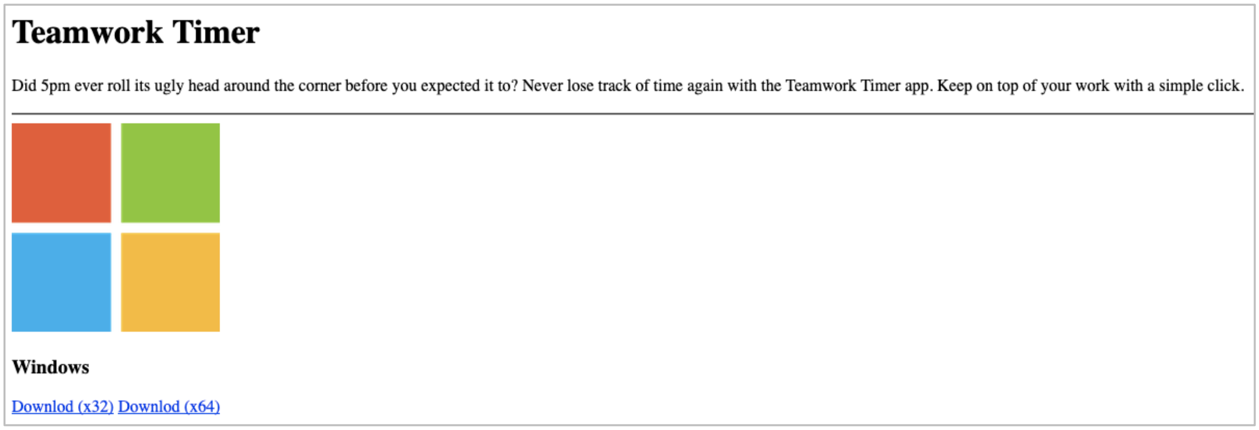
The other shortened URL, goo[.]gl/T6ajlO was sent with the message, “Earn more PeNNeY to make international calls by updating your PeN app in Google Play.” The URL expands to https://play.google[.]com/store/apps/details?id=net.penchat.android, a defunct link for an Android app called PeN Chat. PeN Chat is an “app for everything,” including messaging, voice, social media and e-commerce, according to the app’s website, which indicates that it was created by Dark Matter AB in Sweden.[141] Dark Matter, which does not appear to be related to the UAE hacking firm[142] by the same name, filed for bankruptcy in 2018.[143]

App By “SaudQ” Available For Download

The [redacted].saudqq[.]com subdomain also hosted a download page for “Teamwork Timer,” ostensibly an application for tracking your time while you work, according to an August 2017 snapshot of the page captured by the Wayback Machine.

“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.” The page, which features a “SaudQ 2017” copyright mark, includes defunct links to downloads for Windows, Linux and Mac.

[140] https://www.virustotal.com/#/domain/trade360.com
[141] http://www.penchat.net/about/
[142] https://www.reuters.com/article/us-usa-spying-raven-specialreport/special-report-inside-the-uaes-secret-hacking-team-of-u-s-mercenaries-idUSKCN1PO19O
[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.

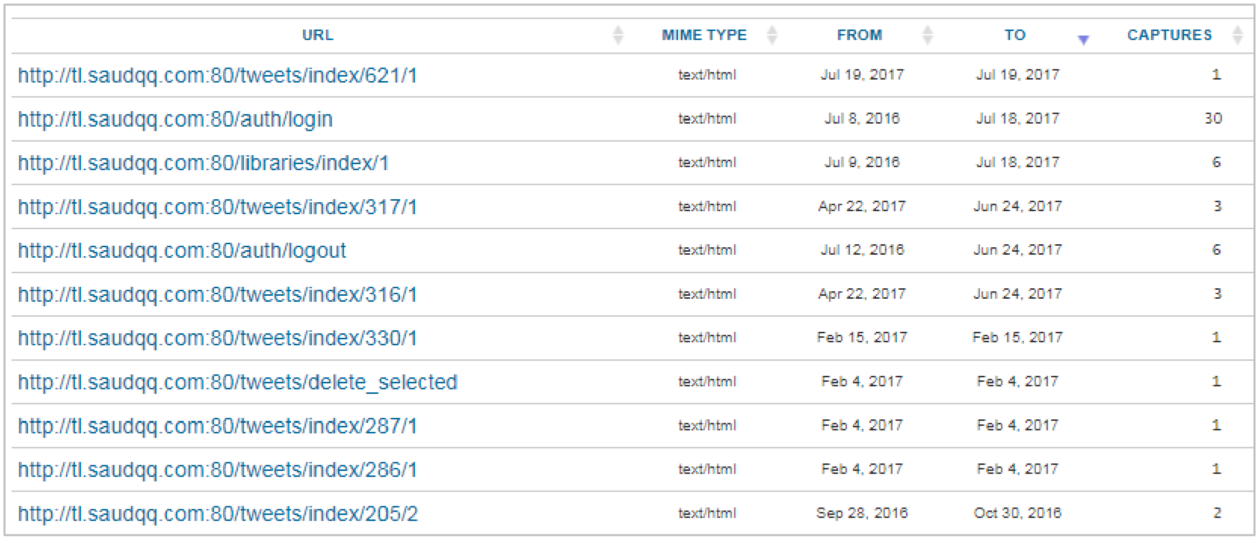
Windows

Downlod (x32) Downlod (x64)

Two Subdomains Used For Twitter

The subdomains tl.saudqq[.]com and tam.saudqq[.]com were used for Twitter, based on archived snapshots of the hosts captured by the Wayback Machine.

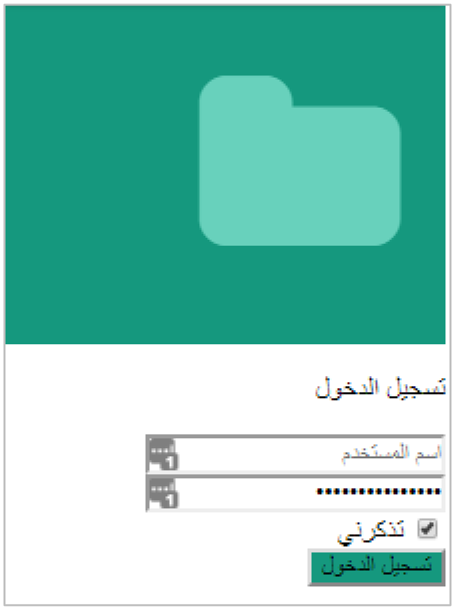
The tl.saudqq[.]com subdomain has dozens of directories referring to tweets, as captured by Wayback Machine, including:



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

All of the captured URLs redirect to a barebones login page:[144]

[144] https://web.archive.org/web/20160709181523/http:/tl.saudqq.com/auth/login



The tam.saudqq[.]com subdomain hosted a “Twitter Account Manager” (TAM) control panel, according to an archived copy of the website from February 2017.[145] In March 2016, a chat log was published on Pastebin that appears to originate from a team working on the Twitter Account Manager. Six individuals are participants in or mentioned in the chat, including a freelance software developer based in Istanbul, Turkey, according to his LinkedIn profile.[146]

The chat referenced using a Mongo database for tweet libraries and included several dead links that are now dead, such as http://tam.saudqq.com/TweetLibraries. One of the chat members also addressed “WhatsApp project developers,” but no details on the WhatsApp project were mentioned.

Demo Subdomain Used For Translation Management

An archived copy of the subdomain demo.saudqq[.]com resolved to a barebones login page in July 2017 and August 2017 that included the phrase “translation management” (“ادارة الترجمة”).[147] The Wayback Machine also captured 54 URLs for the subdomain, which included directories such as /reports, /statistics and /sources/create.[148] All of the URLs reviewed redirected to an archived copy of the aforementioned login page except demo.saudqq[.]com:80/cgi-sys/suspendedpage.cgi, which resolved to an archived “account suspended” page.

Tabeta Subdomain Included In Twitter Spam Analysis

The subdomains codequiz.saudqq[.]com and tabeta.saudqq[.]com were not archived in the Wayback Machine, but they appeared in pastes and an analysis of spam on Twitter, respectively. A URL featuring the host codequiz.saudqq[.]com was included in two scripts posted to Pastebin in March 2016 and August

[145] https://web.archive.org/web/20170212205754/http:/tam.saudqq.com:80/
[146] The link to the chat log, which is still available on Pastebin as of this writing, has been withheld to protect the chat members’ privacy, as the nature of their work and relationship to al-Qahtani and the Saudi government was not clear.
[147] https://web.archive.org/web/20170718214736/http:/demo.saudqq.com:80/login
[148] https://web.archive.org/web/*/demo.saudqq.com/*

2016. The first paste, titled "CURL test code," included the URL http://codequiz.saudqq[.]com/quiz1/login.php.[149] The second paste[150] was untitled and included the same URL. the subdomain, tabeta.saudqq[.]com was included in an analysis of shortened URL spam on Twitter[151] — the host received four clicks, according to the research.[152]

Domain Recently Expired

When saudqq[.]com was created in April 2015, it was hosted at 159.8.206[.]68, the current dedicated server of saudq[.]com, as described above. That IP address is owned by Softlayer Technologies Inc., a hosting provider acquired by IBM in 2011 that, like ThePlanet.com, which merged with Softlayer in 2010, had a reputation for not doing enough to keep bad actors off their networks.[153] Since March 2016, saudqq[.]com has been hosted at 93.168.220[.]54, which is owned by Saudi Telecom Co. in Riyadh, according to Whois records.

Dyn's Whois privacy service was used throughout the life of the domain, which expired at the end of April 2019. It has not been re-registered as of this writing.

[149] https://pastebin.com/iQDek6Ya
[150] https://pastebin.com/jvrCBykY
[151] https://github.com/HarshShah1997/Spam-Classification
[152] https://github.com/HarshShah1997/Spam-Classification/blob/master/Result/ClicksByDomains.txt
[153] https://krebsonsecurity.com/tag/softlayer/

VI. Other Accounts

Using the contact information shown to belong to al-Qahtani in Section III of this report, it was possible to identify additional contact information for him and identify numerous accounts linked to these email addresses and phone numbers.

"Headhunter" On LinkedIn

Al-Qahtani has a LinkedIn Premium account under the name "saud a" where he describes himself as a "headhunter" based in Saudi Arabia.[154] "i'm very interesting in security information and looking to build a good team on my company," his bio reads.

The employment and educational history listed on the profile do not correspond with al-Qahtani's actual biography. The LinkedIn profile indicates that he has been CEO of "SAUD SALIM" since May 2009 and that he had previously been a general manager at "dar security info" from 2008 to 2009 in Riyadh. Al-Qahtani's profile also indicates that he attended King Saud University from 1998 to 2003 and received a bachelor's degree in "Computer and Information Systems Security/Information Assurance."

Al-Qahtani did attend King Saud University, but he earned a bachelor's degree in law from the school before joining the Royal Saudi Air Force's officer training course.[155]

Al-Qahtani used saudq1978@gmail.com to register the profile.

Pro-Mubarak Persona On Facebook

Al-Qahtani also has a fake Facebook profile under the name احمد محمد مصطفى (Ahmed Mohammed Mustafa), where he published pro-Mubarak content in 2011.[156] There is minimal public content on the profile. The only public details about "Ahmed" in the About section of the profile are that he studied in Cairo and was in the class of 1967.

As Ahmed, an "Egyptian citizen at the end of his life," al-Qahtani published a 700-word note in Arabic in September 2011 comparing the treatment of former Egyptian president Hosni Mubarak, who was standing trial at the time after resigning, with King Farouq, who was overthrown in 1952. He argued that, unlike, say, Qaddafi, who bombed his own people and hung onto power, Mubarak gracefully stepped aside but was nonetheless treated unfairly. (This is, to say the least, an ahistorical interpretation of the Egyptian government's response to the 2011 Egyptian revolution, which was marked by hundreds of deaths and thousands of injuries.)[157]

[154] https://www.linkedin.com/in/saud-a-15821bbb/
[155] http://www.arabnews.com/node/1326371/saudi-arabia
[156] https://www.facebook.com/profile.php?id=100002908691104
[157] https://en.wikipedia.org/wiki/Egyptian_revolution_of_2011#Deaths

The Ahmed profile likes one page, called "أنا أسف ياريس" ("I am sorry, president"),[158] which is dedicated to defending Mubarak. Al-Qahtani follows the Facebook page's Twitter profile (@AseFYaryes), but the account does not follow al-Qahtani back.[159]

The only other public content associated with al-Qahtani's Ahmed profile is a comment on a post by pro-Mubarak page with the same 700-word note.[160]

The Facebook profile is connected to the email address nokia2mon2@gmail.com, which, in turn, is connected to al-Qahtani's mobile number, +966 55 548 9750, and primary Gmail address, saudq1978@gmail.com, according to information leakage from Google's password recovery feature.

Al-Qahtani likely used nokia2mon2@gmail.com to create an account with the free web hosting service 000webhost, as the email address was among 15 million customer records stolen in a March 2015 hack. The username associated with the 000webhost account was "nokia2mon2," and the IP address was 94.98.168.57, another dynamic home subscriber IP address owned by Saudi Telecom Co. in Riyadh, according to Whois records.

The nokia2mon2@gmail.com email address is also connected to a Twitter account, based on information leakage from Twitter's password recovery page, but the particular account has not been determined.

Mobile Number Connected To Snapchat, WhatsApp, Signal

In addition to being connected to his Twitter profile and several email accounts, Al-Qahtani's mobile phone number, +966 55 548 9750, is connected to accounts on Snapchat, WhatsApp and Signal. There is no public information associated with al-Qahtani's WhatsApp or Signal accounts, such as a bio or profile photo. His Snapchat profile is similarly bare, though his username can be seen: "saudq197" — *not* saudq1978.

Al-Qahtani's phone number is also connected to a Facebook profile that has not been identified.

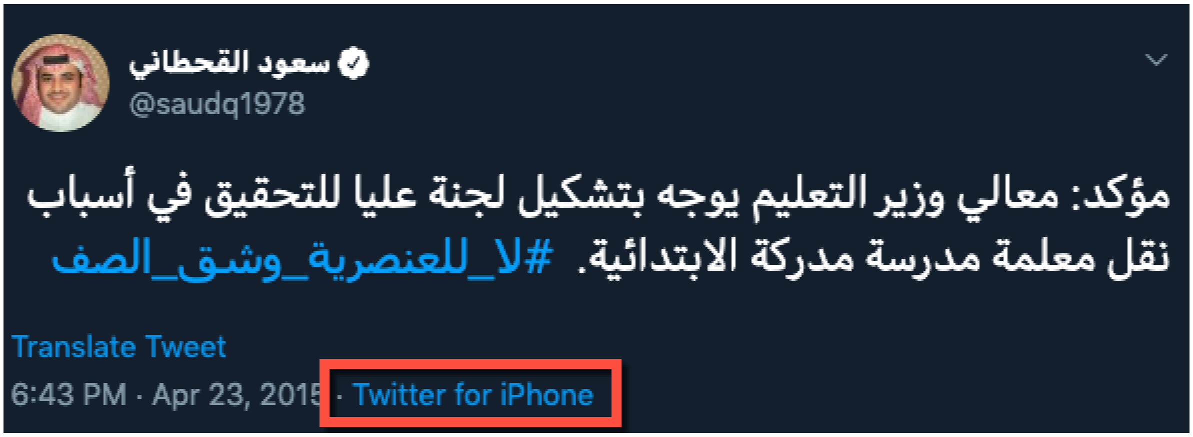
Used Nokia2mon2 Handle On Several Forums

Al-Qahtani likely used the username "nokia2mon2" on at least a half a dozen tech and hacking forums. The posts on these forums resemble al-Qahtani's posts on Hack Forums in form and substance: they are written in broken English, some feature his oft-used sign off, "Best Regards" and they largely involve similar subject matter, namely, failed hacking attempts and offers of larger than ordinary sums of money for assistance.

[158] https://www.facebook.com/pg/AseF.Yarayes
[159] https://twitter.com/AseFYaryes
[160] https://www.facebook.com/AseF.Yarayes/photos/a.127012047369717/194016860669235

In April 2012, a user called nokia2mon2 posted a thread[161] in a subform dedicated to FaceNiff,[162] an Android application that allows users to steal credentials from Facebook, Twitter, YouTube and Amazon accounts or hijack sessions over Wi-Fi. "its catch facebook and youtube but it didnt catch emails and twitter," nokia2mon2 wrote. The user also requested that vBulletin be added to the tool's capabilities. Al-Qahtani posted about vBulletin four times on Hack Forums, including in April 2012, a week before the FaceNiff post, when he complained that his man-in-the-middle attack on three vBulletin boards was unsuccessful.[163]

Three years later, in April 2015, a nokia2mon2 posted a thread on the xda-developers.com forum offering to pay up to $2,000 to anyone who could help him root an Android-based Vertu Aster phone.[164] When asked why he did not just buy a second phone, he responded, "i need to root this device for very personal reasons." Four photos of the Vertu phone were attached to the post. Metadata from the photos indicated that they were taken with an iPhone 6 Plus. Al-Qahtani has used both iOS and Android devices to post on Twitter, but in the days surrounding the xda-developers.com post, he used an iPhone:



سعود القحطاني ✓
@saudq1978

مؤكد: معالي وزير التعليم يوجه بتشكيل لجنة عليا للتحقيق في أسباب
نقل معلمة مدرسة مدركة الابتدائية. #لا_للعنصرية_وشق_الصف

Translate Tweet
6:43 PM · Apr 23, 2015 · Twitter for iPhone

Al-Qahtani is also likely behind the nokia2mon2 accounts on LinuxQuestions.org,[165] UbuntuForums.org,[166] Hashcat.net[167] and BlackHatWorld.com.[168] The IP address associated with the nokia2mon2 BlackHatWorld account in breach data — 2.90.233.17 — is owned by Saudi Telecom Co. in Riyadh, according to Whois records.

[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] https://forum.xda-developers.com/android/help/help-rooting-vertu-aster-payprice-2000-t3091843
[165] https://www.linuxquestions.org/questions/linux-newbie-8/places-not-open-desktop-blank-after-i-installed-the-second-radeon-6990-pls-help-913004/
[166] https://ubuntuforums.org/showthread.php?t=1878282
[167] https://hashcat.net/forum/user-1671.html
[168] https://www.blackhatworld.com/members/nokia2mon2.263630/

VII. Conclusion

MBS's repression machine is alive and well thanks in no small part to the Trump administration's refusal to hold the Saudi strongman and his regime to account.[169]

Since Khashoggi was murdered last October, the CIA has observed its "duty to warn"[170] on three separate occasions, sharing intelligence to alert dissidents based in the U.S., Canada and Norway to threats originating from Saudi Arabia.[171]

The extent to which the crown prince's right-hand man, Saud al-Qahtani, is continuing to play a role in Saudi Arabia's campaign of intimidation is unclear.

The Saudi government has not publicly discussed his whereabouts, though in private, Saudis officials claim that he is under house arrest.[172]

However, multiple media outlets have cited sources saying that he is still in MBS's good graces and continuing to work in a similar capacity as before he was officially ousted from the royal court. In January 2019, the Washington Post reported that al-Qahtani had been seen in the offices of the royal court in Riyadh.[173] That same month, Washington Post columnist David Ignatius reported that MBS is in regular contact with al-Qahtani, who had recently met with his senior deputies from the Center, citing U.S. and Saudi sources.[174] In April 2019, a source told the Guardian that MBS remains loyal to al-Qahtani, who is "actively engaged" in a role similar to the one he held as head of the Center, though now within MBS's private office.[175]

The best open-source indication to date that al-Qahtani is continuing his hacking work comes from the Guardian, which reported in June 2019, that it was targeted by a Saudi hacking team at the order of al-Qahtani.[176] The newspaper was initially warned of the order by a source in Riyadh earlier this year, and the threat was subsequently corroborated by a confidential internal order signed by al-Qahtani, which the Guardian reviewed. The document, dated March 7, 2019, was written in Arabic and instructed "heads of technological and technical departments" run from the cybersecurity directorate within the private office of the MBS to "carry out the penetration of the servers of the Guardian newspaper and those who worked on

[169] https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-standing-saudi-arabia/
[170] https://fas.org/blogs/secrecy/2015/08/duty-to-warn/
[171] https://www.cbsnews.com/news/activist-iyad-el-baghdadi-says-cia-warned-saudi-arabia-threat-colleagues-jamal-khashoggi/
[172] https://www.nytimes.com/2019/04/08/us/politics/saudi-sanctions-khashoggi.html
[173] https://www.washingtonpost.com/world/named-as-a-key-saudi-suspect-in-khashoggi-killing-top-royal-adviser-drops-out-of-sight/2019/01/06/2aed0cae-0790-11e9-8942-0ef442e59094_story.html
[174] https://www.washingtonpost.com/opinions/global-opinions/the-saudi-engine-of-repression-continues-to-run-at-full-speed/2019/01/10/d5a5f68a-1521-11e9-803c-4ef28312c8b9_story.html?utm_term=.2a0ff68c821a
[175] https://www.theguardian.com/world/2019/apr/12/us-urges-saudi-prince-to-ditch-aide-linked-to-khashoggi-killing
[176] https://www.theguardian.com/world/2019/jun/19/guardian-told-it-was-target-of-saudi-hacking-unit-after-khashoggi-killing

the report that was published, and deal with the issue with complete secrecy, then send us all the data as soon as possible."

Al-Qahtani is not among the 11 suspects facing trial in Saudi Arabia for the murder of Khashoggi.[177]

On June 19, 2019, Agnes Callamard, the United Nations (UN) Special Rapporteur on extrajudicial, summary or arbitrary killings, published a report on Khashoggi's death, calling it a "premeditated extrajudicial execution" at the hands of the Saudi state.[178] "His killing was the result of elaborate planning involving extensive coordination and significant human and financial resources. It was overseen, planned and endorsed by high-level officials. It was premeditated."

The report specifically names al-Qahtani and MBS as two high-level officials who have not been criminally charged but for whom there is "credible evidence meriting further investigation."

Callamard is scheduled to present the findings of her investigation to the UN Human Rights Council on June 27, 2019.[179] Khashoggi's fiancée, Hatice Cengiz, will also address the Council.

The findings included in this report are not exhaustive, and research into al-Qahtani's web infrastructure is ongoing. In addition to the 22 domains analyzed in Section V, this investigation identified several other domains that are likely linked to al-Qahtani but require further research and analysis. Any additional findings will be published in a follow-up report.

#وش_تعرف_عن_النحل

[177] https://www.aljazeera.com/news/2019/04/saudi-royal-advisor-missing-khashoggi-trial-officials-190428065139559.html
[178] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24713
[179] https://twitter.com/RobertMMahoney/status/1142400309223817216/photo/1