THE HACKING HOLE WHERE JOHN BOLTON SHOULD BE

Unless DOJ disguised him, the hack of John Bolton described in his indictment didn't show up in the Iranian hack-and-leak indictment. It should have. After listing the 2022 attempt to assassinate Bolton (where he is described as "a former US National Security Advisor," the indictment lists a slew of people that Iran IGRC attempted to hack (starting in 2020) and (starting in 2021) nine people it succeeded in hacking before it hacked Roger Stone and four other Trump flunkies.

Bolton should have, could have, been included along with those nine people.

As the (nifty color-coded) timeline below makes clear, Bolton told the FBI about the hack of him, on July 6, 2021, just as the Iranian hackers were setting up infrastructure to hack a set of people that include those, like Bolton, who played a role in the Qasem Soleimani assassination and Trump's hardline first term approach with Iran.

To be sure, there are potentially good reasons why Bolton is not in there. There's a sealed notice of related case in the Bolton docket (at docket entry 6), which could reflect charges against the people who hacked him, charges that might have been filed shortly after he alerted the FBI about the hack. Prosecutors could have left Bolton out to obscure that he told the FBI about the hack (and that therefore the FBI had been working backwards from that ever since, which is consistent with the timeline). Prosecutors could have left Bolton out because the criminal investigation into him remained open.

All plausible reasons to leave him out.

But when you put the hack and assassination

targeting of Bolton on the same timeline as the hack-and-leak targeting first fellow Iran hawks and then the Trump campaign, as well as the second alleged assassination attempt by Asif Merchant, all presumed to be IGRC, it raises further questions.

First, one reason I was interested in Merchant's disclosure yesterday that he was under surveillance from the moment he arrived in the US in April 2024 is because it suggests US spies were already well aware of the efforts to retaliate for the Soleimani killing. Indeed, the timeline explains how the FBI was magically able to get CHSes in both the Shahram Poursafi and the Asif Merchant attempt to hire hit squads to target Bolton and others: the FBI identified those people via those intercepts and flipped them early on in the plot.

It does raise questions about whether the FBI also knew of the hack-and-leak targeting Bolton in advance. The FBI would have been tracking the IGRC closely after their 2020 effort to attack Democrats under the guise of the Proud Boys (an earlier plot that makes the targeting of Proud Boy ally Roger Stone more interesting).

There is some separation between these two plots. While Poursafi eventually had access to non-public intelligence targeting Bolton, he didn't even know Bolton's home address at first, which he would have known if he had the emails stolen from Bolton available to him. But the hack-and-leak indictment, at least, lists as one of the goals of the hacking campaign, "to advance the IRGC's malign activities, including ongoing efforts to avenge the death of Qasem Soleimani," and the first hack included, of someone at State who led the Abraham Accords, implies that's how they used, "travel, lodging and other information" from someone who was "a senior U.S. Department of State official at the time of Qasem Soleimani's death and therefore of interest to the IRGC." Near the tail end of the Poursafi complaint, so just weeks before the hack of that victim, Poursafi turned to another

target.

But that's the other reason this timeline is of such interest. The progression with Bolton went Hack > Extortion > Assassination Attempt. Bolton could simply have cooperated with the IGRC, but instead he went to the FBI (which has now led to his prosecution).

Trump, however did not.

It was over two months between the time hackers got into Roger Stone's Hotmail account in May 2024 and the time the hack became public. In July, when they first became aware of the hack, the campaign affirmatively decided not to report it to the FBI.

> Trump's mistrust of federal agencies has complicated the investigation into Iran's cyberattack on his campaign. When a technology firm first discovered the breach, campaign aides huddled to discuss what they should do. After hours of discussions in July, they decided they trusted the software experts to handle the matter and did not call the FBI. Co-campaign manager Susie Wiles, whose email account was targeted, was among those who questioned whether they could trust the Justice Department. The fears centered on giving federal officials access to campaign email servers and whether they would leak information out publicly.

As I noted at the time, Trump made that decision after relentlessly (and falsely) accusing the FBI of failing to get the server from the DNC hack. The decision was understandable (once you account for Trump's venality and paranoia), because according to the initial reports, the hackers claim to have gotten information on Trump's legal cases, not just his campaign.

> The sender would not speak on the telephone with a Post reporter but indicated they had access to additional

> information, including internal campaign emails and documents related to Trump's court cases.

And one reason that's interesting is because — as Reuters disclosed only this summer — the lawyer targeted in the attack was Lindsey Halligan, who had no public role on the campaign but who did represent Trump on the stolen documents case.

> In online chats with Reuters on Sunday and Monday, the hackers, who go by the pseudonym Robert, said they had roughly 100 gigabytes of emails from the accounts of White House Chief of Staff Susie Wiles, Trump lawyer Lindsey Halligan, Trump adviser Roger Stone and porn star-turned-Trump antagonist Stormy Daniels.

Which brings me back to Merchant, to the delay in turning over his own conversations until October 28.

Two public things might explain that delay (there are no doubt a bunch of secret things that could to0): The conviction of Ryan Routh, who did have Iranian ties, though no Iranian role in his assassination attempt was publicly disclosed, and the indictment of Bolton, which disclosed that Bolton alerted the FBI to this hack back in 2021, just months before the FBI would preempt an assassination effort targeting Bolton as well.

The FBI took far greater efforts to rein in any publication of the materials stolen from Trump's people than they ever have on another leak save WikiLeaks' biggest document dumps. I can't help but wonder whether there's more about the Trump hack we weren't told.

Timeline

December 19, 2018: Hackers establish account using Israeli politician's name.

April 15, 2019: IRGC designated as FTO.

January 3, 2020: Trump kills Qasem Soleimani.

April 11, 2020: Hackers get an account in the name of a SCOTUS spouse.

October 22, 2020: Treasury sanctions IRGC for tampering in 2020 election.

June 16, 2021: Bolton and DOJ enter settlement on book.

July 6, 2021: Bolton representative tells FBI Iran has hacked Bolton.

July 7, 2021: Hackers register fake domain mailerdaemon.online.

July 25, 2021: Hacker threatens to release Bolton materials.

> I do not think you would be interested in the FBI being aware of the leaked content of John's email (some of which have been attached), especially after the recent acquittal.
>
> This could be the biggest scandal since Hillary's emails were leaked, but this time on the GOP side!
>
> Contact me before it's too late…

July 28, 2021: Bolton representative tells FBI about threat.

July 29, 2021: Bolton rep tells FBI he would delete account.

August 5, 2021: Iran threatens Bolton again.

> OK John … As you want (apparently), we'll disseminate the expurgated sections of your book by reference to your leaked email…

October 22, 2021: Shahram Poursafi asks Individual A to photograph Bolton. Individual A suggests CHS.

November 9, 2021: Hackers register fake domain mailer-daemon.live. CHS contacts Poursafi; Poursafi asks if he could hire someone to "eliminate someone."

November 14: Poursafi tells CHS he doesn't need pictures anymore. After searching for it online, Poursafi provides Bolton's DC office address with name of scheduling assistant.

November 18: Poursafi note with Bolton's name, website, social media handle, and former title.

November 19: CHS asks for home address and asks how to do it.

November 21: Poursafi ups the payment to $300,000.

November 23: CHS tells Poursafi he traveled from Texas to DC; Poursafi still did not have home address, but that Bolton walked or was driven to work.

December 7, 2021: Poursafi says because of a recent failed operation, Iran did not approve payment.

December 10, 2021: Poursafi told the CHS that Bolton didn't go outside often.

December 12, 2021: Hackers register tinyurl.ink.

December 14, 2021: Hackers create persona based on DC think tank employee and phish State employee (Victim 1).

December 16, 2021: Poursafi asked CHS to refer to Bolton by name "Benham."

December 20, 2021: With Bolton's consent, CHS sent pictures of Bolton leaving his office.

December 22, 2021: Poursafi sends picture of cash he claims is for CHS.

January 3, 2022: Iranian President Ebrahim Raisi says Trump and other high ranking Trump

officials need to face trial for Soleimani killing. Poursafi tells CHS the murder was not timed to coincide with anniversary of Soleimani death. Poursafi says he has a source who says Bolton is at home.

January 5, 2022: CHS tells Poursafi he would do the job on January 16 or 17.

January 7, 2022: IGRC head Esmail Ghani promises revenge.

January 10, 2022: CHS asks if Ghani's speech was a reference to this job.

January 15, 2022: CHS claims to have three vans. Poursafi warns not to talk operational details on phone, instructs CHS to crush phone and/or change Poursafi contact to "Mark" in it.

January 18, 2022: CHS sent Poursafi public information stating that Bolton might be traveling; Poursafi said that Bolton was not. "The information does not appear to have been publicly available. POURSAFI did not specify whether his source was a person conducting surveillance, a cyber intrusion, or another type of source."

January 20, 2022: Poursafi told CHS Bolton did not have a body guard, had not yet left town.

January 28, 2022: Poursafi instructs CHS to get surveillance cameras for Bolton's home and office.

January 29, 2022: Poursafi instructs CHS to restore social media account.

February 1, 2022: Poursafi told CHS the area around Bolton's home was clear.

April 13, 2022: Poursafi pushes CHS to do a second job.

April 28, 2022: Poursafi told CHS to finish the second job in six days.

April 30, 2022: Hackers create another persona, persona 3.

May 9, 2022: Jalili accesses persona 3 account, other hackers arrive in office, send test message to book author.

May 31, 2022: Hackers register mailer-daemon.me.

June 18, 2022: Hackers create persona 4, phish victim 1.

August 2, 2022: Hackers create spoof of think tank, with two more personas.

August 5, 2022: Shahram Poursafi complaint.

August 6, 2022: Hackers start stealing from victim 1, including his passport.

Early August 2022: Hackers create persona based on DC journalist/think tanker (victim 4).

August 23, 2022: Victim 4 responds to phish.

August 29, 2022 through October 5, 2022: Hackers hack former Homeland Security Advisor (Victim 5).

October 4, 2022: Hackers pose as assistant to Victim 1 to contact peace organization employee (Victim 2), using stolen passport and get Victim 2 to buy business class ticket for Victim 1.

October 26, 2022: Hackers used Victim 1 passport to query about UAE conference.

November 23, 2022: Hackers create persona based on UAE embassy employee in DC, then use account to invite Victim 1, a former senior CIA person (Victim 6), a former US Ambassador to Israel (Victim 7), and a former Deputy CIA Director (Victim 8) as well as other targeted persons to a party at UAE embassy.

December 20, 2022 to January 23, 2022: Hackers compromise Victim 6’s personal email.

January 16, 2023: Hackers create encrypted app account in the name of DC think tank employee and phish Iranian Human Rights worker (Victim 9).

April 2024: Hackers try to phish Victim 5.

April 13, 2024: Merchant arrives in Houston.

April 22, 2024: Merchant pitches CHS on business.

May 23, 2024: Hackers attempt to log into Roger Stone's account.

May 24 ,2024: Hackers use recovery code to access Stone's account.

June 3-4, 2024: Merchant presents plan.

June 10, 2024: Merchant and CHS meet fake hitmen.

June 12, 2024: Hackers access Stone's account and access campaign official (Victim 11).

June 13, 2024: Merchant establishes code.

June 15, 2024: Hackers use Stone's account to attempt to phish Victim 13 (Susie Wiles?).

June 18, 2024: Merchant arranges payment with US-based associate.

June 20, 2024: Hackers hack a second Stone account.

June 21, 2024: Via WhatsApp Merchant's cousin arranges payment.

June 27, 2024: Hackers send Trump debate prep to two people on Biden's campaign; neither responded.

July 3, 2024: Hackers send Trump info to another Biden associate; that person did not respond.

July 12, 2024: Merchant arrest.

July 20, 2024: Hackers use 2FA hack to access Trump lawyer [Lindsey Halligan?], Victim 12.

July 22, 2024: Hackers started pitching content to journalists, including by pitching one journalist on things campaign official said to Susie Wiles about that journalist's reporting.

August 9, 2024: Microsoft report on Iran hack.

August 10, 2024: Politico reports hack; WaPo

follows.

August 13, 2024: Hackers ousted from Victim 11 account and Victim 12 account.

August 14, 2024: Google report on Iran hack.

August 31, 2024: Hackers pitch more journalists (including me).

September 24, 2024: Iran hack-and-leak indictment.

October 2, 2024: FISA notice in Merchant prosecution.

December 20, 2024: Initial CIPA request in Merchant prosecution.

July 1, 2025: Hackers attempt to sell Susie Wiles, Lindsey Halligan, Stone, and Stormy Daniel emails.

July 11, 2025: CIPA filing in Merchant prosecution.

August 11, 2025: CIPA meeting in Merchant prosecution.

September 23, 2025: Ryan Routh guilty verdict.

October 18, 2025: Bolton indicted.

October 28, 2025: Delayed discovery provided in Merchant prosecution.

November 12, 2025: Ex parte communication in Merchant prosecution.

Purple: Shahram Poursafi complaint

Blue: Iran hack-and-leak indictment

Pink: Asif Merchant complaint

Green: Bolton prosecution