קמפיין דיוג של קבוצת התקיפה המדינתית APT42 כנגד אישים באקדמיה

30/09/2024
כ"ז אלול תשפ"ד

[תקציר]

- מערך הסייבר הלאומי איתר לאחרונה קמפיין דיוג (פישינג) ממוקד המכוון נגד אנשי אקדמיה, העוסקים במחקר בזירה האיראנית/מזרח התיכון, ואנשי מערכת הביטחון לשעבר.

פעולות מידיות לביצוע:

- להתרעה זו מצורף קובץ מזהים. מומלץ מאד לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.

[פרטים]

- קמפיין זה משויך לקבוצת התקיפה האיראנית APT42, אשר מקושרת למשמרות המהפכה האיסלאמית באיראן (IRGC), ומתמחה במבצעי ריגול סייבר ואיסוף מודיעין.
- הקבוצה ידועה בשימוש בטכניקות הנדסה חברתית מתוחכמות, ודיוג ממוקד לצורך איסוף מידע רגיש.
- הקמפיין כולל שליחת הודעות דוא"ל מדומיינים המתחזים לארגונים לגיטימיים ומכוני מחקר, כאשר תוכן המיילים כולל לינקים לפגישות "Zoom" ומסמכי PDF עם הזמנה להשתתפות בוועידה, בצירוף רשימות משתתפים לצורך ביסוס אמינות.
- כמו כן, נשלחו הודעות מגורמים המתחזים לחוקרים בתחום המחקר המדיני בדגש על המזרח התיכון, המבקשים להתייעץ בנושא מחקרים אקדמיים.
- ראו בהמשך צילומי מסך של הודעות שנשלחו במסגרת הקמפיין.

⚠

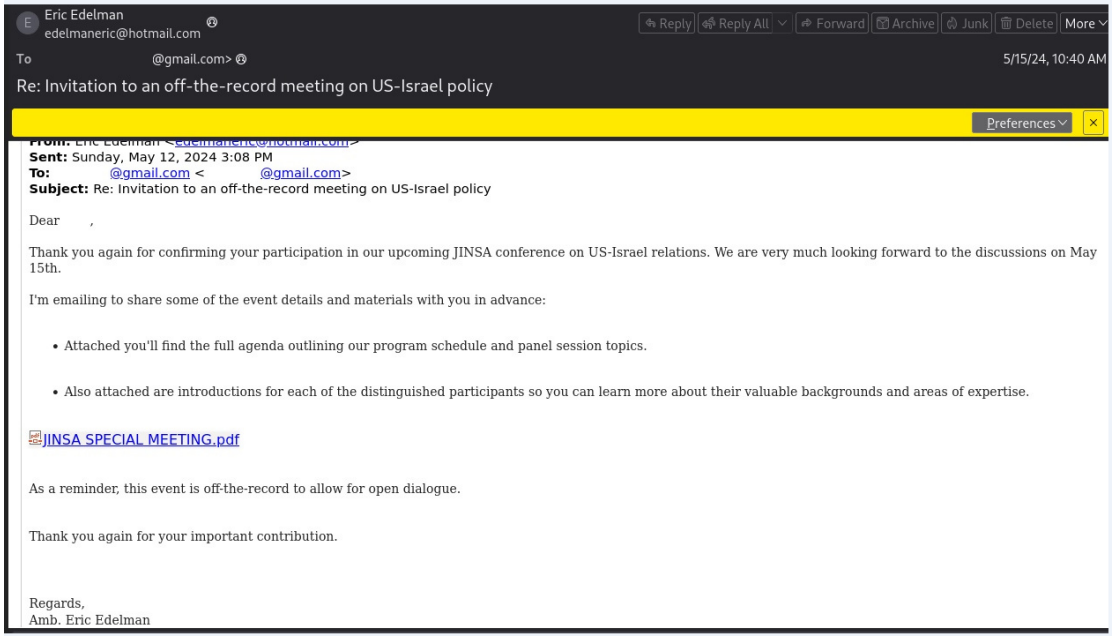
שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.

המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

[דרכי התמודדות]

- להתרעה זו מצורף קובץ מזהים. מומלץ מאד לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.
- מומלץ לנקוט משנה זהירות בפתיחת צרופות או הפעלת קישורים בהודעות דוא"ל, ולוודא מול השולח באמצעות ערוץ תקשורת שונה האם שלח אותן.

צילומי מסך של הודעות מהקמפיין



Eric Edelman
edelmaneric@hotmail.com

Reply | Reply All | Forward | Archive | Junk | Delete | More

To @gmail.com>

5/15/24, 10:40 AM

Re: Invitation to an off-the-record meeting on US-Israel policy

Preferences

From: Eric Edelman <edelmaneric@hotmail.com>
Sent: Sunday, May 12, 2024 3:08 PM
To: @gmail.com < @gmail.com>
Subject: Re: Invitation to an off-the-record meeting on US-Israel policy

Dear ,

Thank you again for confirming your participation in our upcoming JINSA conference on US-Israel relations. We are very much looking forward to the discussions on May 15th.

I'm emailing to share some of the event details and materials with you in advance:

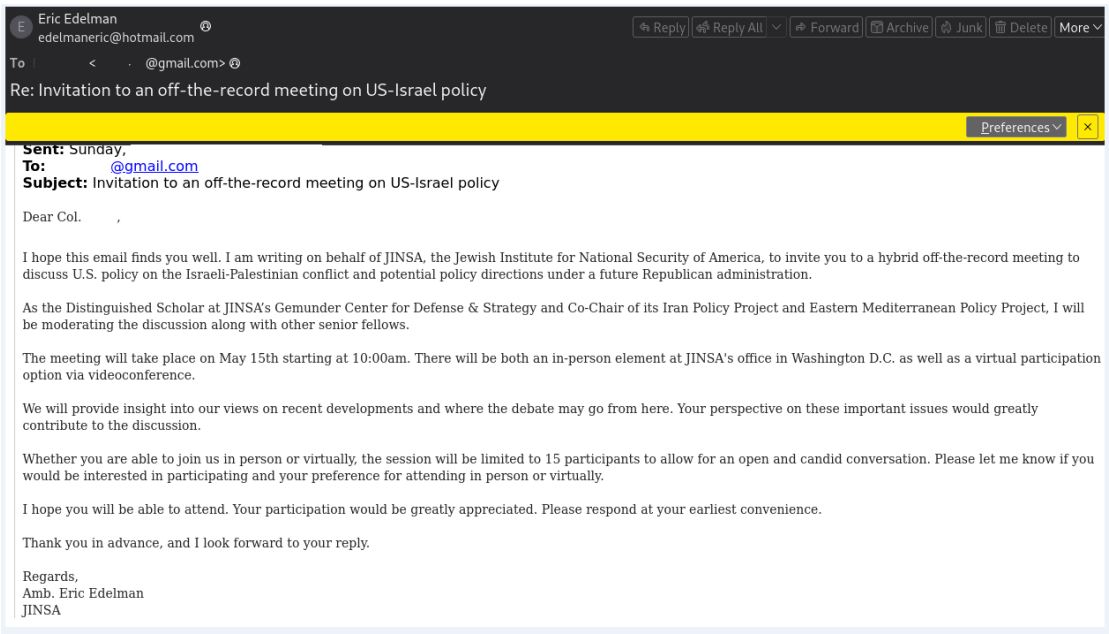
- Attached you'll find the full agenda outlining our program schedule and panel session topics.
- Also attached are introductions for each of the distinguished participants so you can learn more about their valuable backgrounds and areas of expertise.

JINSA SPECIAL MEETING.pdf

As a reminder, this event is off-the-record to allow for open dialogue.

Thank you again for your important contribution.

Regards,
Amb. Eric Edelman



Eric Edelman
edelmaneric@hotmail.com

Reply | Reply All | Forward | Archive | Junk | Delete | More

To < . @gmail.com>

Re: Invitation to an off-the-record meeting on US-Israel policy

Preferences

Sent: Sunday,
To: @gmail.com
Subject: Invitation to an off-the-record meeting on US-Israel policy

Dear Col. ,

I hope this email finds you well. I am writing on behalf of JINSA, the Jewish Institute for National Security of America, to invite you to a hybrid off-the-record meeting to discuss U.S. policy on the Israeli-Palestinian conflict and potential policy directions under a future Republican administration.

As the Distinguished Scholar at JINSA's Gemunder Center for Defense & Strategy and Co-Chair of its Iran Policy Project and Eastern Mediterranean Policy Project, I will be moderating the discussion along with other senior fellows.

The meeting will take place on May 15th starting at 10:00am. There will be both an in-person element at JINSA's office in Washington D.C. as well as a virtual participation option via videoconference.

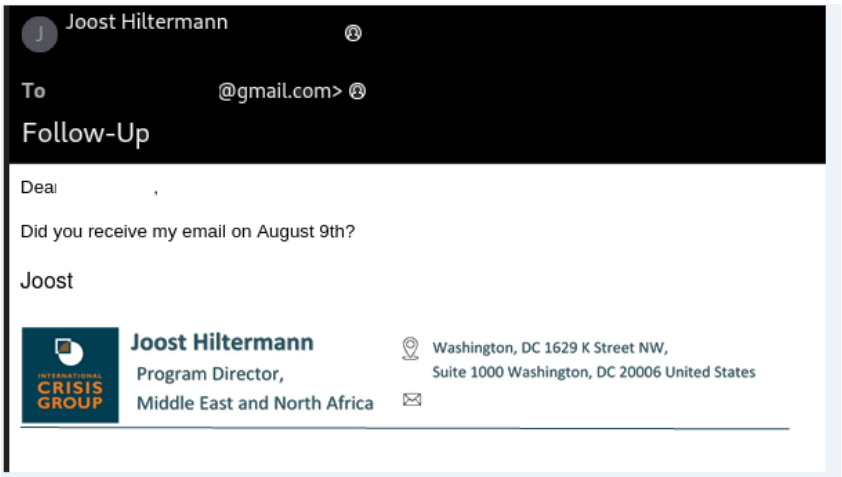
We will provide insight into our views on recent developments and where the debate may go from here. Your perspective on these important issues would greatly contribute to the discussion.

Whether you are able to join us in person or virtually, the session will be limited to 15 participants to allow for an open and candid conversation. Please let me know if you would be interested in participating and your preference for attending in person or virtually.

I hope you will be able to attend. Your participation would be greatly appreciated. Please respond at your earliest convenience.

Thank you in advance, and I look forward to your reply.

Regards,
Amb. Eric Edelman
JINSA



Joost Hiltermann

To @gmail.com>

Follow-Up

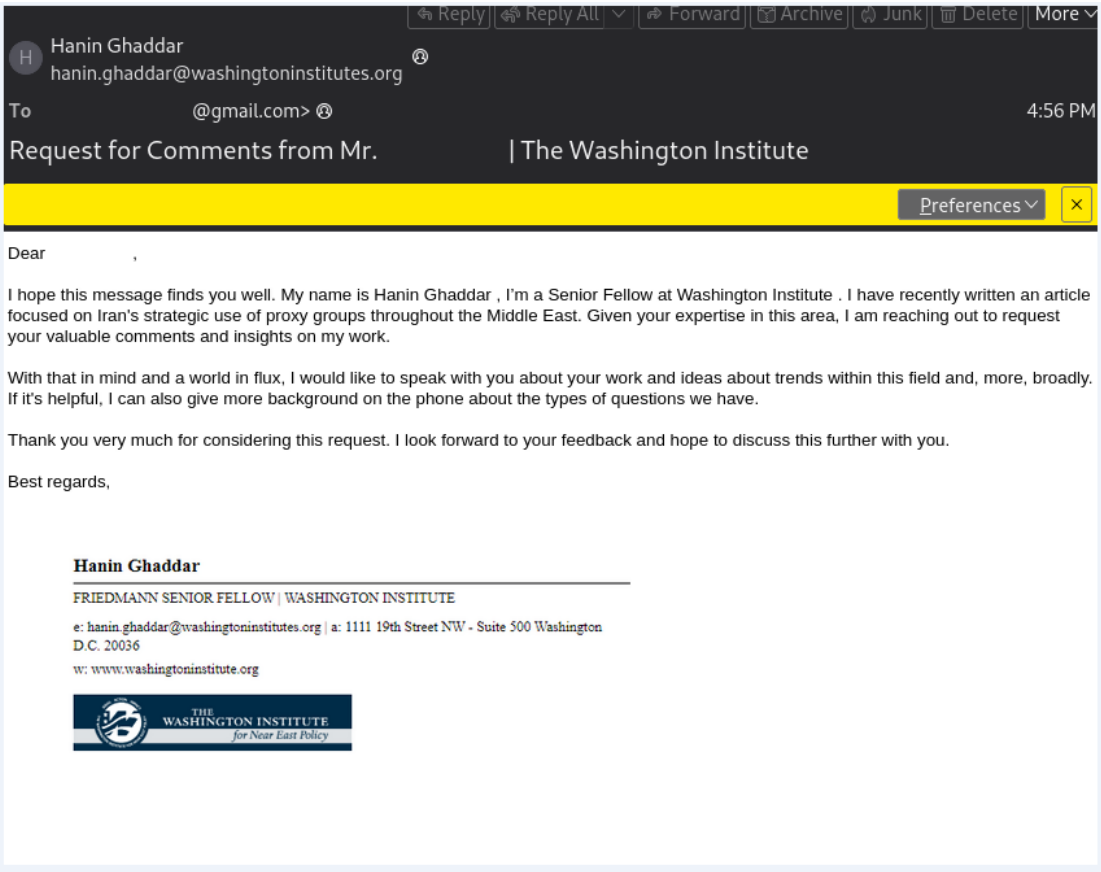
Dea ,

Did you receive my email on August 9th?

Joost

Joost Hiltermann
Program Director,
Middle East and North Africa

Washington, DC 1629 K Street NW,
Suite 1000 Washington, DC 20006 United States



Reply | Reply All | Forward | Archive | Junk | Delete | More

Hanin Ghaddar
hanin.ghaddar@washingtoninstitutes.org

To @gmail.com> 4:56 PM

Request for Comments from Mr. | The Washington Institute

Preferences

Dear ,

I hope this message finds you well. My name is Hanin Ghaddar , I'm a Senior Fellow at Washington Institute . I have recently written an article focused on Iran's strategic use of proxy groups throughout the Middle East. Given your expertise in this area, I am reaching out to request your valuable comments and insights on my work.

With that in mind and a world in flux, I would like to speak with you about your work and ideas about trends within this field and, more, broadly. If it's helpful, I can also give more background on the phone about the types of questions we have.

Thank you very much for considering this request. I look forward to your feedback and hope to discuss this further with you.

Best regards,

Hanin Ghaddar

FRIEDMANN SENIOR FELLOW | WASHINGTON INSTITUTE

e: hanin.ghaddar@washingtoninstitutes.org | a: 1111 19th Street NW - Suite 500 Washington D.C. 20036

w: www.washingtoninstitute.org

THE WASHINGTON INSTITUTE for Near East Policy