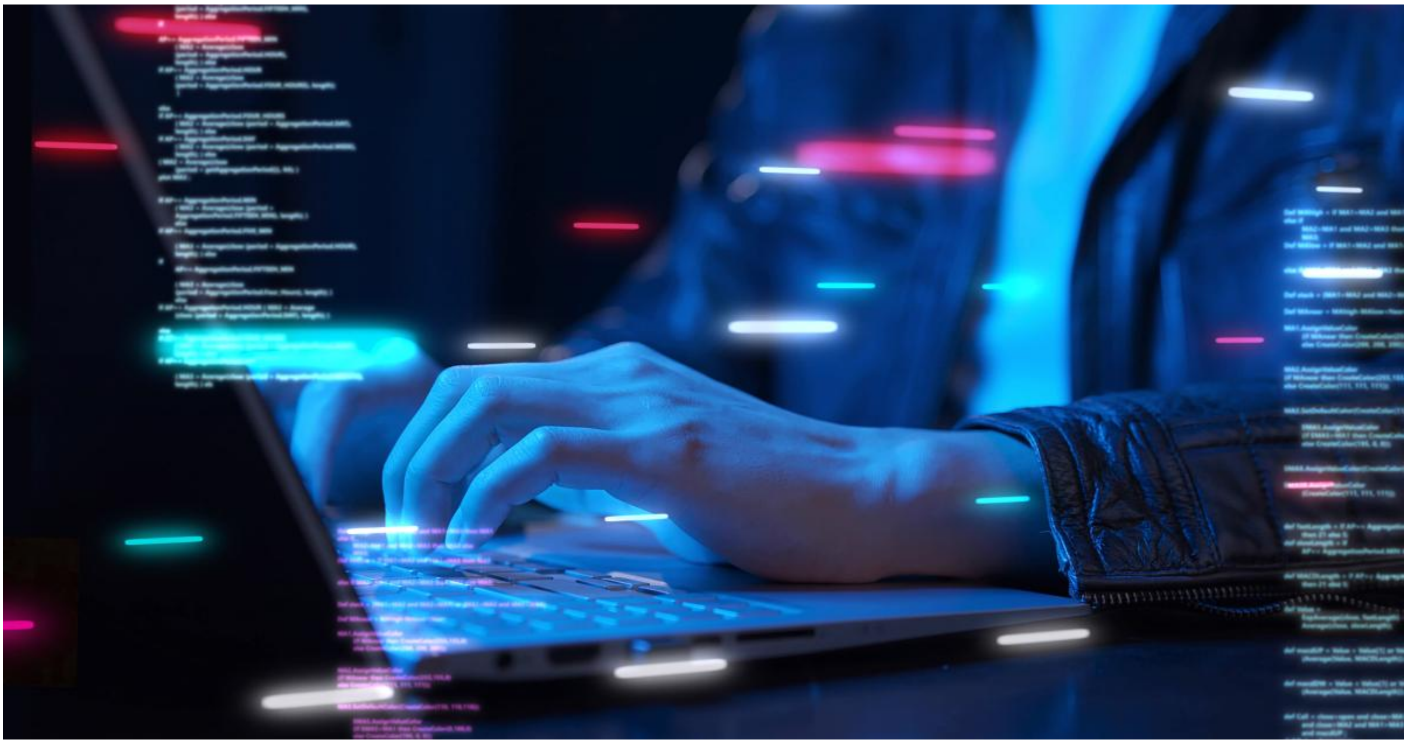
Look What You Made Me Do: TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO

⁝ 9/11/2022



September 13, 2022 Joshua Miller, Kyle Eaton and Alexander Rausch

Key Takeaways

- In mid-2022, TA453 deployed a social engineering impersonation technique informally called Multi-Persona Impersonation in which the threat actor uses at least two actor-controlled personas on a single email thread to convince targets of the legitimacy of the campaign.
- This is an intriguing technique because it requires more resources be used per target—potentially burning more personas—and a coordinated approach among the various personalities in use by TA453.
- This is the latest in TA453's evolution of its techniques and can be mitigated in large part by potential targets, such as those specializing in Middle Eastern affairs or nuclear security, by being cautious when they receive outreach from unexpected sources, even those that appear legitimate.

Overview

As a great songwriter once penned, "everyone needs a friend." No APT this year has been taking this sentiment more to heart than the Iran-aligned espionage threat actor TA453. Throughout late 2021 and through 2022, Proofpoint researchers have observed TA453, which overlaps with activity tracked as Charming Kitten, PHOSPHORUS, and APT42, continually innovating its approach in a quest to fulfill its intelligence priorities. In late June 2022, this evolution resulted in campaigns utilizing what Proofpoint informally calls Multi-Persona Impersonation (MPI), a subset of Impersonation noted in Proofpoint's Email Fraud Taxonomy framework. In MPI, TA453 takes their targeted social engineering to a new level, targeting researchers with not just one actor-controlled persona but multiple. This technique allows TA453 to leverage the psychology principle of social proof to prey upon its targets and increase the authenticity of the threat actor's spear phishing. Proofpoint has previously observed this technique from advanced business email compromise actors such as TA2520 (Cosmic Lynx).

It is important to note that for the purposes of this blog, Proofpoint refers to each of the TA453 personas by the sender name. While Proofpoint has previously observed TA453 using compromised email accounts to send phishing emails, Proofpoint has no specific indication that these spoofed individuals were victimized by TA453. Additionally, Proofpoint regularly sees TA453 pair the same spoofed person with different actor-controlled email addresses.

Typical TA453 Activity

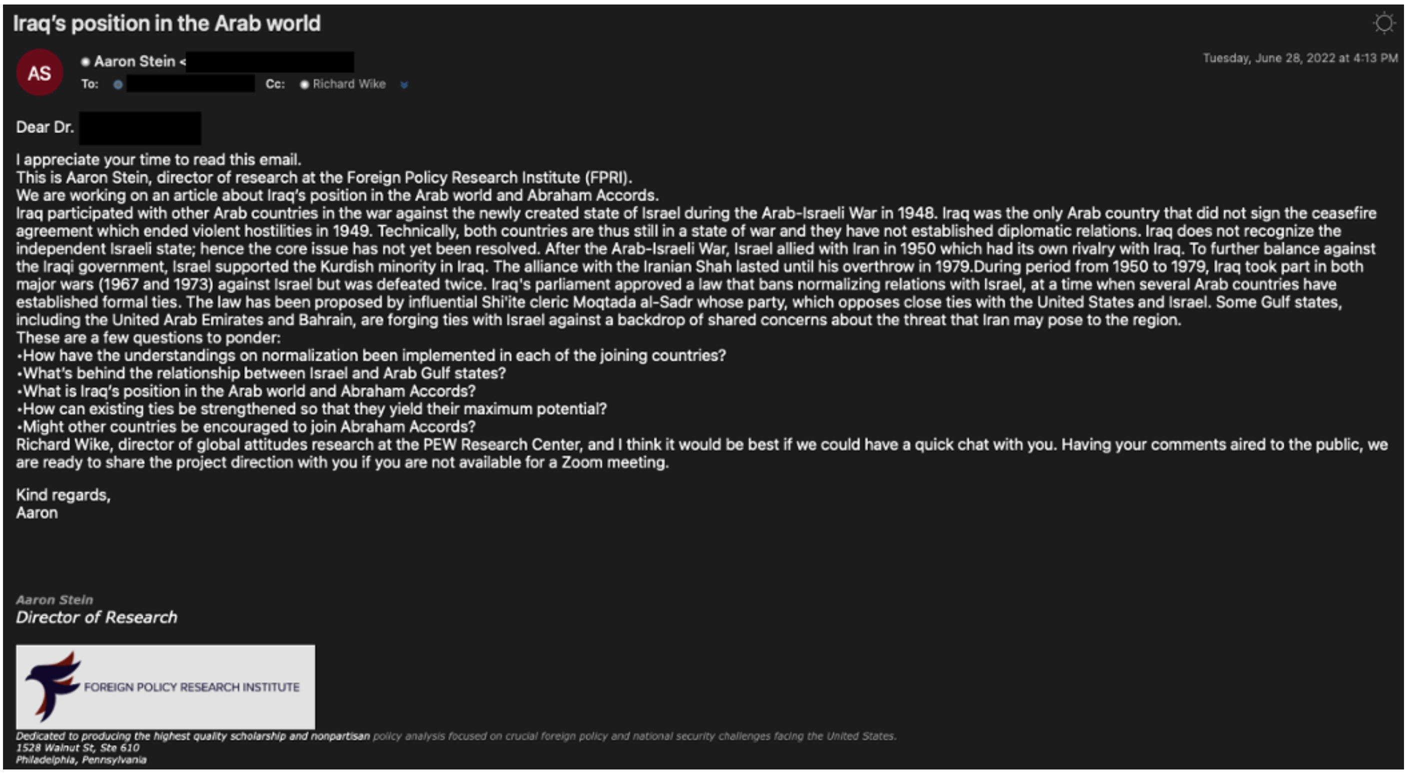
In what Proofpoint researchers consider a standard TA453 campaign, the threat actor masquerades as an individual, such as a journalist or policy adjacent individual, working to collaborate with the intended target. Historically, TA453 has targeted academics, policymakers, diplomats, journalists, and human rights workers. Benign conversations that eventually lead credential harvesting links are hallmarks of TA453 activity. Proofpoint has observed limited instances of TA453 deploying malware.

In almost all cases, TA453 would engage in one-to-one conversations with their targets but this changed in mid-2022.

Times are Changing: TA453's Multiple Personalities

Proofpoint researchers observed a shift in TA453's approach starting in June 2022. In this first campaign (Figure 1), TA453 started the conversation masquerading as "Aaron Stein, Director of Research at FRPI." The actor included a variety of questions intended to generate a dialogue about Israel, the Gulf States, and the Abraham Accords. While these questions are generally meant to establish a pretext for sending a follow-up credential harvesting link or to deliver a malicious document, it is also possible they represent intelligence questions tasked to TA453.

In the email, TA453's "Aaron Stein" launched the threat actor's use of Multi-Persona Impersonation (MPI) by referring to and including a "Richard Wike, director of global attitudes research at PEW Research Center" on the CC line.



Iraq's position in the Arab world

● Aaron Stein < [redacted]

To: ● [redacted] Cc: ● Richard Wike

Tuesday, June 28, 2022 at 4:13 PM

Dear Dr. [redacted]

I appreciate your time to read this email.
This is Aaron Stein, director of research at the Foreign Policy Research Institute (FPRI).
We are working on an article about Iraq's position in the Arab world and Abraham Accords.
Iraq participated with other Arab countries in the war against the newly created state of Israel during the Arab-Israeli War in 1948. Iraq was the only Arab country that did not sign the ceasefire agreement which ended violent hostilities in 1949. Technically, both countries are thus still in a state of war and they have not established diplomatic relations. Iraq does not recognize the independent Israeli state; hence the core issue has not yet been resolved. After the Arab-Israeli War, Israel allied with Iran in 1950 which had its own rivalry with Iraq. To further balance against the Iraqi government, Israel supported the Kurdish minority in Iraq. The alliance with the Iranian Shah lasted until his overthrow in 1979.During period from 1950 to 1979, Iraq took part in both major wars (1967 and 1973) against Israel but was defeated twice. Iraq's parliament approved a law that bans normalizing relations with Israel, at a time when several Arab countries have established formal ties. The law has been proposed by influential Shi'ite cleric Moqtada al-Sadr whose party, which opposes close ties with the United States and Israel. Some Gulf states, including the United Arab Emirates and Bahrain, are forging ties with Israel against a backdrop of shared concerns about the threat that Iran may pose to the region.
These are a few questions to ponder:
•How have the understandings on normalization been implemented in each of the joining countries?
•What's behind the relationship between Israel and Arab Gulf states?
•What is Iraq's position in the Arab world and Abraham Accords?
•How can existing ties be strengthened so that they yield their maximum potential?
•Might other countries be encouraged to join Abraham Accords?
Richard Wike, director of global attitudes research at the PEW Research Center, and I think it would be best if we could have a quick chat with you. Having your comments aired to the public, we are ready to share the project direction with you if you are not available for a Zoom meeting.

Kind regards,
Aaron

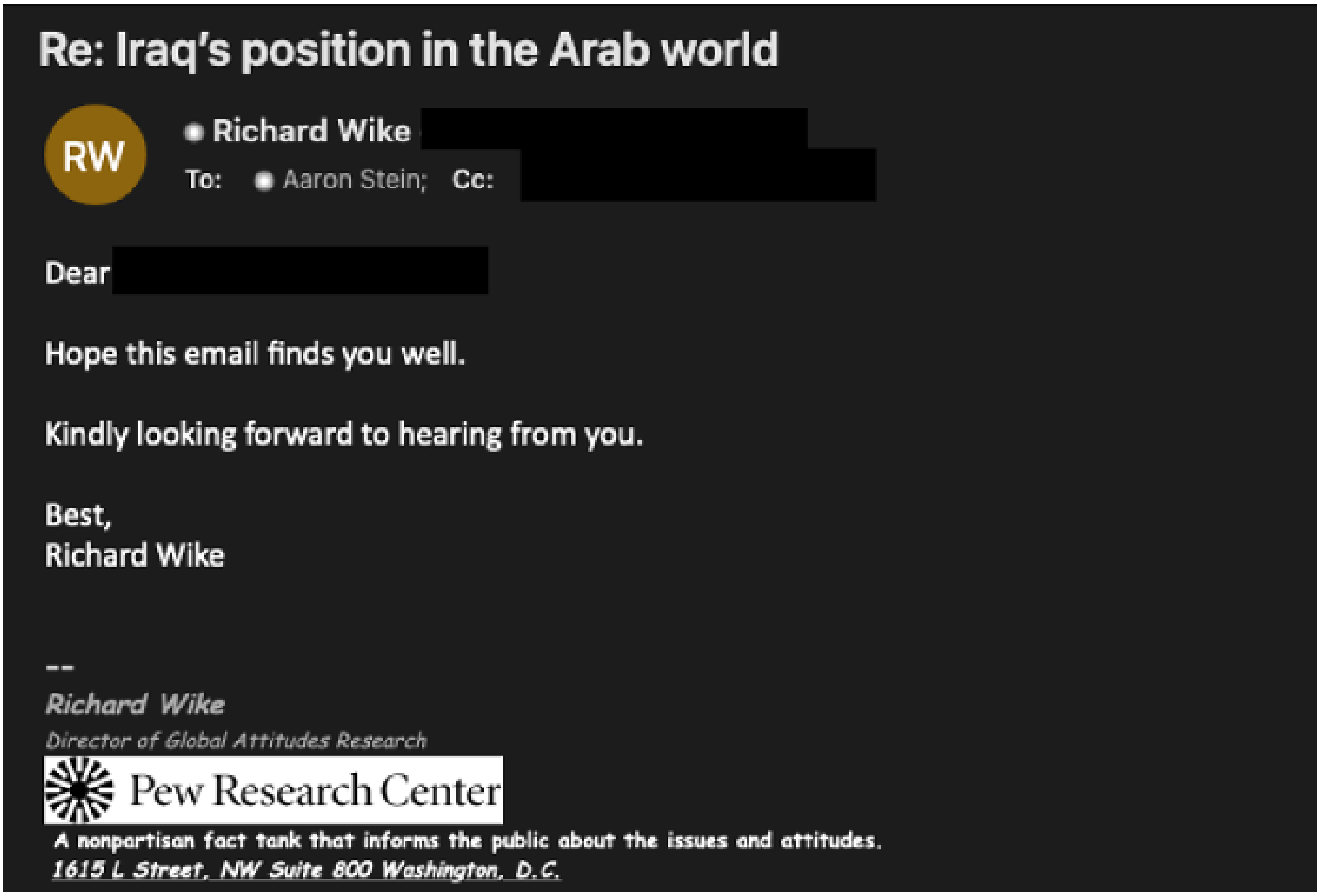
Aaron Stein
Director of Research

FOREIGN POLICY RESEARCH INSTITUTE

Dedicated to producing the highest quality scholarship and nonpartisan policy analysis focused on crucial foreign policy and national security challenges facing the United States.
1528 Walnut St, Ste 610
Philadelphia, Pennsylvania

Figure 1. TA453 email posing as an "Aaron Stein, Director of Research at FRPI."

A day after the initial email, "Richard Wike" responded (Figure 2) to the email thread likely in an attempt to establish the veracity of the request and solicit a response from the target. In this case, no malicious documents or links were observed.



Re: Iraq's position in the Arab world

● Richard Wike [redacted]

To: ● Aaron Stein; Cc: [redacted]

Dear [redacted]

Hope this email finds you well.

Kindly looking forward to hearing from you.

Best,
Richard Wike

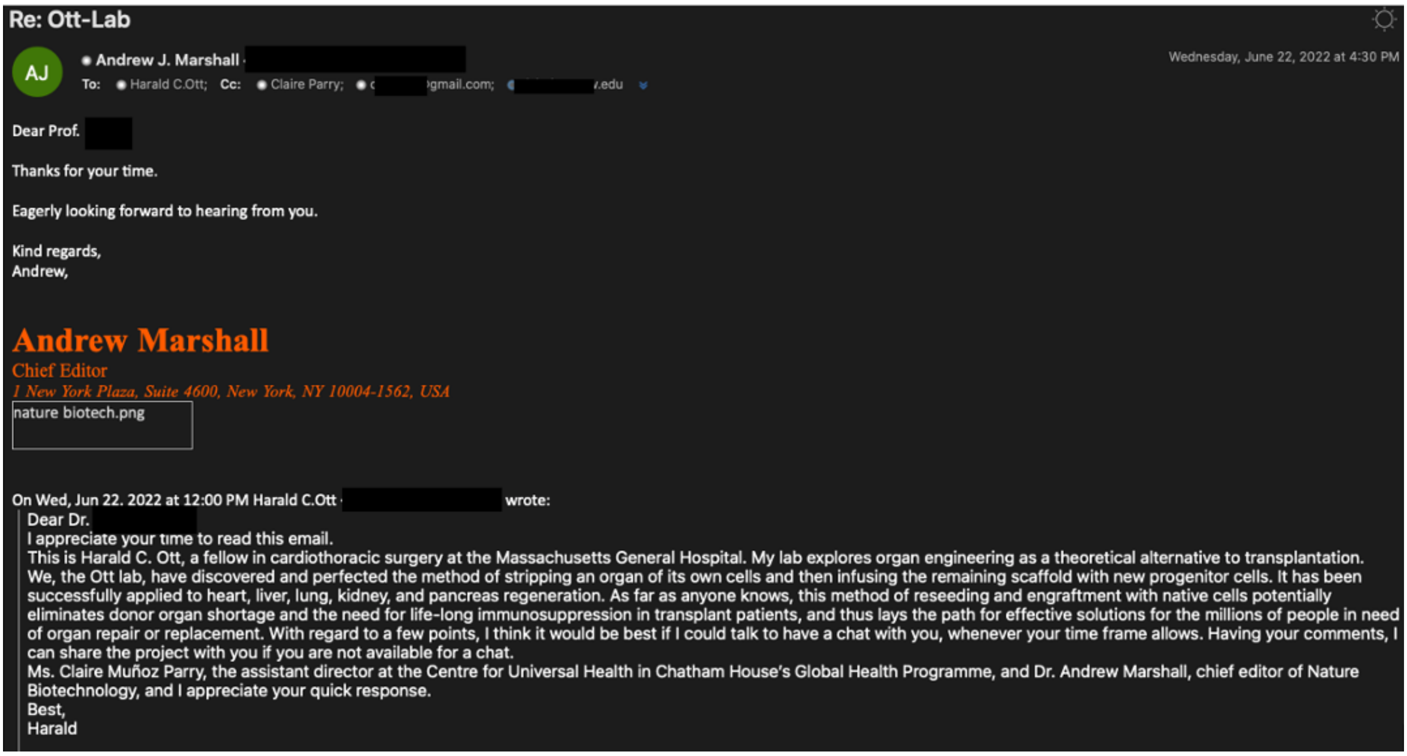
--
Richard Wike
Director of Global Attitudes Research

Pew Research Center

A nonpartisan fact tank that informs the public about the issues and attitudes.
1615 L Street, NW Suite 800 Washington, D.C.

Figure 2. TA453 follow-up email using another persona.

Bringing Up BadBlood: In late June 2022, TA453 reached out to a target specializing in genome research as "Harald Ott" and cc'd two other actor-controlled accounts, "Claire Parry, Assistant Director at the Centre for Universal Health in Chatham House's Global Health Programme" and "Dr. Andrew Marshall, chief editor of Nature Biotechnology," which made this impersonation attempt a three to one MPI using organ regeneration as a lure. When the target replied to the initial email, "Harald" delivered a OneDrive link that downloaded a malicious Word doc named Ott-Lab 371.docx. The SHA256 for the file is f6456454be8cb77858d24147b1529890cd06d314aed70c07fc0b5725ac84542b. Proofpoint assesses this document represents the latest iteration of TA453's exploitation of Remote Template Injection previously reported by PwC. The template and its macros, dubbed *Korg* by Proofpoint, will be discussed later in this report.



Re: Ott-Lab

AJ ● Andrew J. Marshall [redacted]

Wednesday, June 22, 2022 at 4:30 PM

To: ● Harald C.Ott; Cc: ● Claire Parry; ● c[redacted]gmail.com; [redacted].edu

Dear Prof. [redacted]

Thanks for your time.

Eagerly looking forward to hearing from you.

Kind regards,
Andrew,

Andrew Marshall
Chief Editor
1 New York Plaza, Suite 4600, New York, NY 10004-1562, USA
nature biotech.png

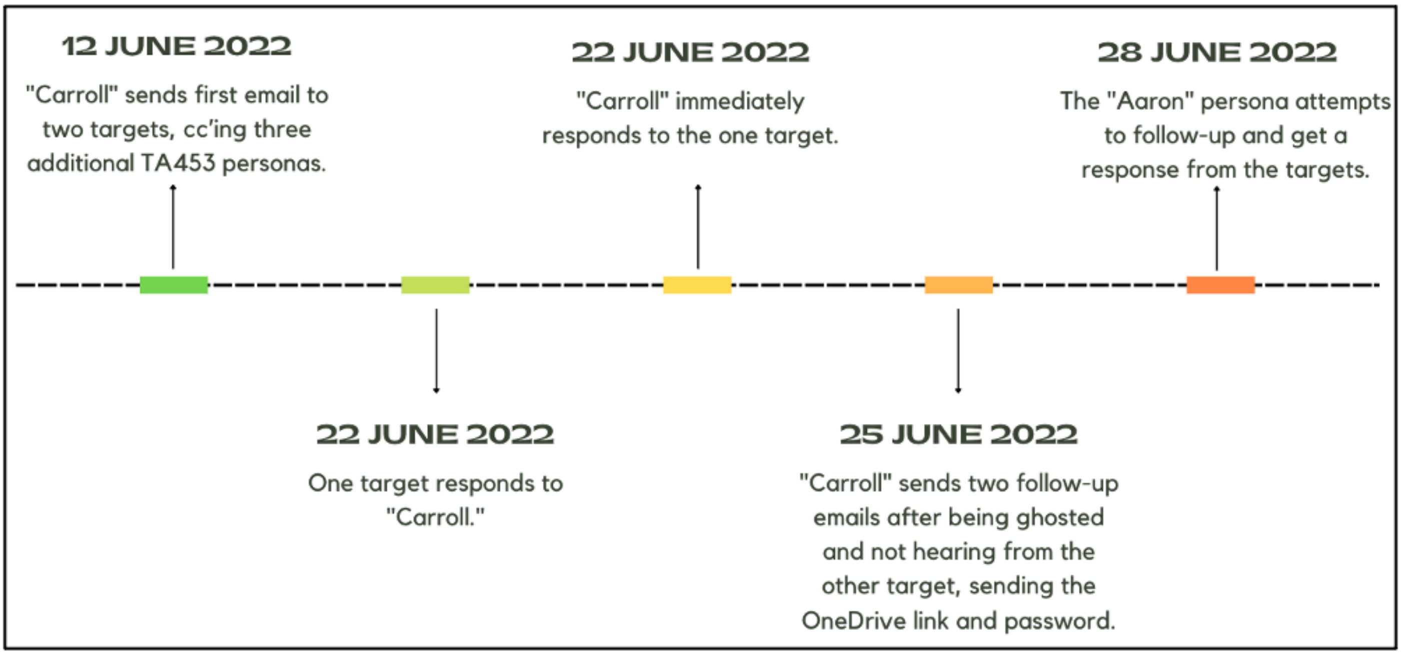
On Wed, Jun 22. 2022 at 12:00 PM Harald C.Ott [redacted] wrote:

> Dear Dr. [redacted]
> I appreciate your time to read this email.
> This is Harald C. Ott, a fellow in cardiothoracic surgery at the Massachusetts General Hospital. My lab explores organ engineering as a theoretical alternative to transplantation. We, the Ott lab, have discovered and perfected the method of stripping an organ of its own cells and then infusing the remaining scaffold with new progenitor cells. It has been successfully applied to heart, liver, lung, kidney, and pancreas regeneration. As far as anyone knows, this method of reseeding and engraftment with native cells potentially eliminates donor organ shortage and the need for life-long immunosuppression in transplant patients, and thus lays the path for effective solutions for the millions of people in need of organ repair or replacement. With regard to a few points, I think it would be best if I could talk to have a chat with you, whenever your time frame allows. Having your comments, I can share the project with you if you are not available for a chat.
> Ms. Claire Muñoz Parry, the assistant director at the Centre for Universal Health in Chatham House's Global Health Programme, and Dr. Andrew Marshall, chief editor of Nature Biotechnology, and I appreciate your quick response.
> Best,
> Harald

Figure 3. Screenshot of TA453 using one of its cc'd personas to further the ruse targeting a medical researcher.

While the targeting of medical personnel, specifically those involved in genome research, is not a frequent area of focus for TA453, it is not the first time this actor has demonstrated an interest in this type of research. In December 2020, TA453 conducted a phishing campaign targeting medical researchers, as detailed in Proofpoint's BadBlood blog.

Group Project: In June 2022, TA453's "Carroll Doherty" persona reached out to a prominent academic involved in nuclear arms control about a possible US versus Russia clash. This campaign ended up representing an evolution of TA453's MPI technique as the persona did not stop at reaching out to just one target but reached out to two targets at the same university. "Carroll" also cc'd three other TA453 personas on the email: "Daniel Krcmaric," "Aaron Stein," and "Sharan Grewal."



12 JUNE 2022

"Carroll" sends first email to two targets, cc'ing three additional TA453 personas.

22 JUNE 2022

One target responds to "Carroll."

22 JUNE 2022

"Carroll" immediately responds to the one target.

25 JUNE 2022

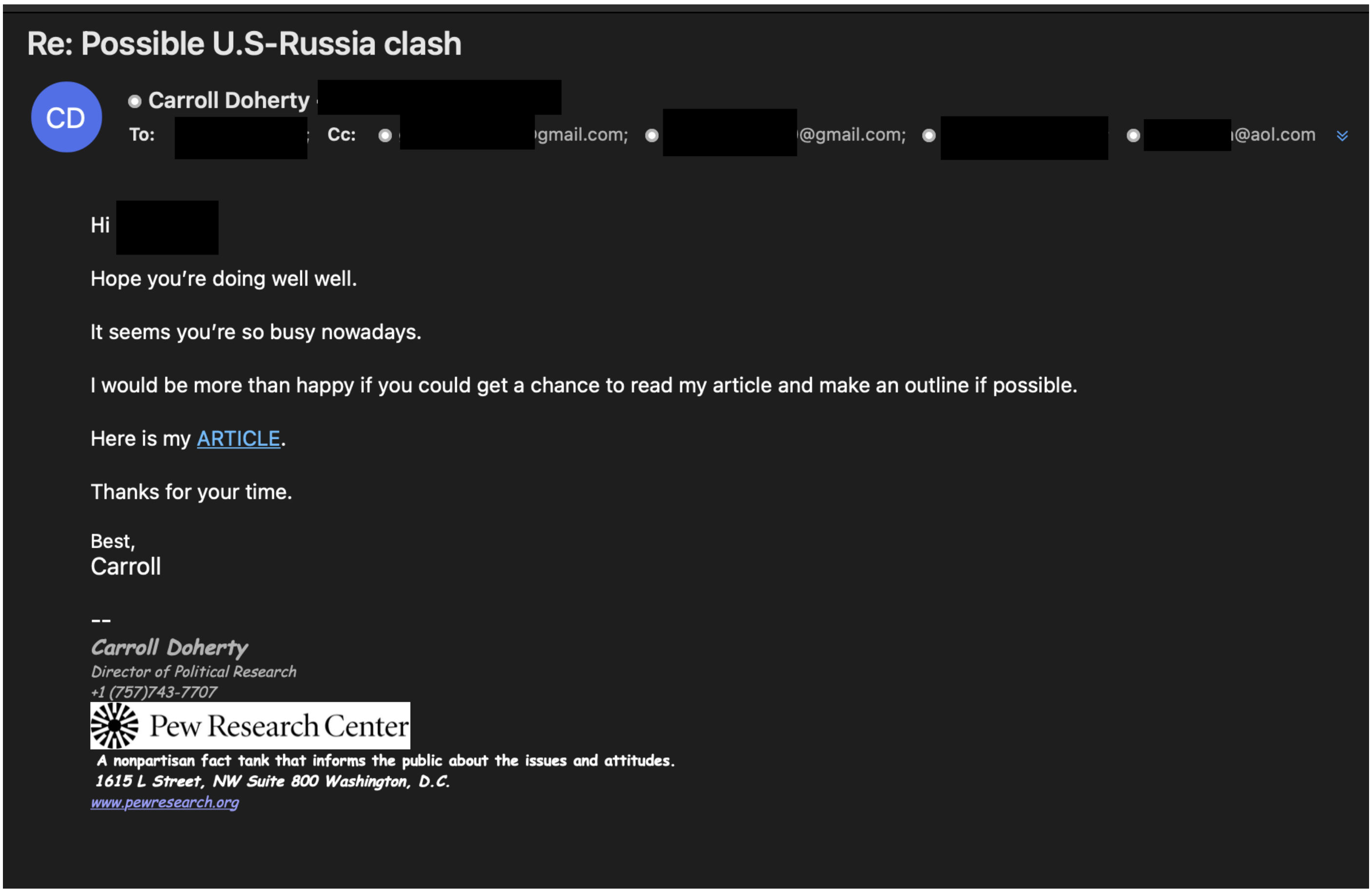
"Carroll" sends two follow-up emails after being ghosted and not hearing from the other target, sending the OneDrive link and password.

28 JUNE 2022

The "Aaron" persona attempts to follow-up and get a response from the targets.

Figure 4. Timeline of TA453's Group Project email campaign.

One of the targets responded initially to the outreach email but then ghosted "Carroll." After the target failed to respond for a little over a week, "Carroll" kindly provided a OneDrive link to the article referenced in the original email (Figure 5). The link downloaded a document titled “The possible US-Russia clash.docx" SHA256: 16a961475a88313478bc2406d6b442be9809e64ea9e2a4754debcce9200cf36b.



Re: Possible U.S-Russia clash

CD ● Carroll Doherty [redacted]

To: [redacted] Cc: ● [redacted]gmail.com; ● [redacted]@gmail.com; ● [redacted] ● [redacted]@aol.com

Hi [redacted]

Hope you’re doing well well.

It seems you’re so busy nowadays.

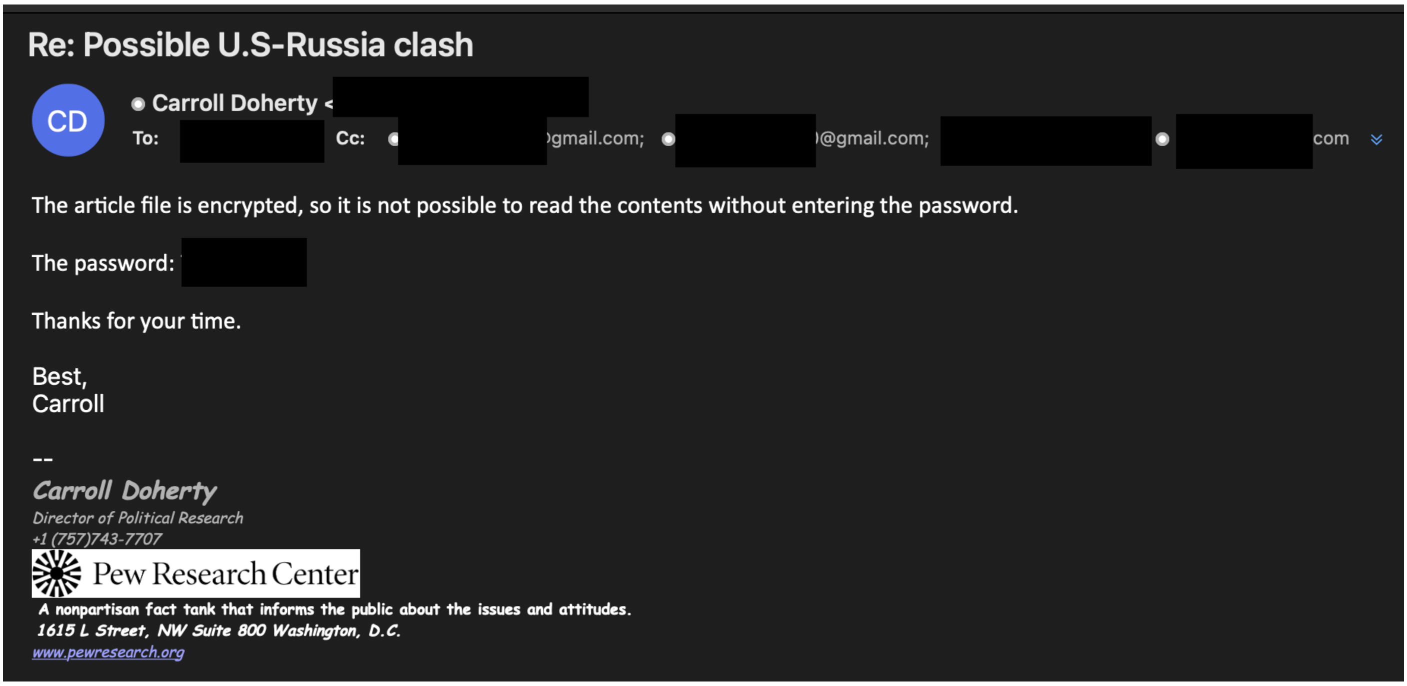
I would be more than happy if you could get a chance to read my article and make an outline if possible.

Here is my ARTICLE.

Thanks for your time.

Best,
Carroll

--
Carroll Doherty
Director of Political Research
+1 (757)743-7707
Pew Research Center
A nonpartisan fact tank that informs the public about the issues and attitudes.
1615 L Street, NW Suite 800 Washington, D.C.
www.pewresearch.org



Re: Possible U.S-Russia clash

CD ● Carroll Doherty <[redacted]

To: [redacted] Cc: ● [redacted]gmail.com; ● [redacted]@gmail.com; [redacted] ● [redacted] com

The article file is encrypted, so it is not possible to read the contents without entering the password.

The password: [redacted]

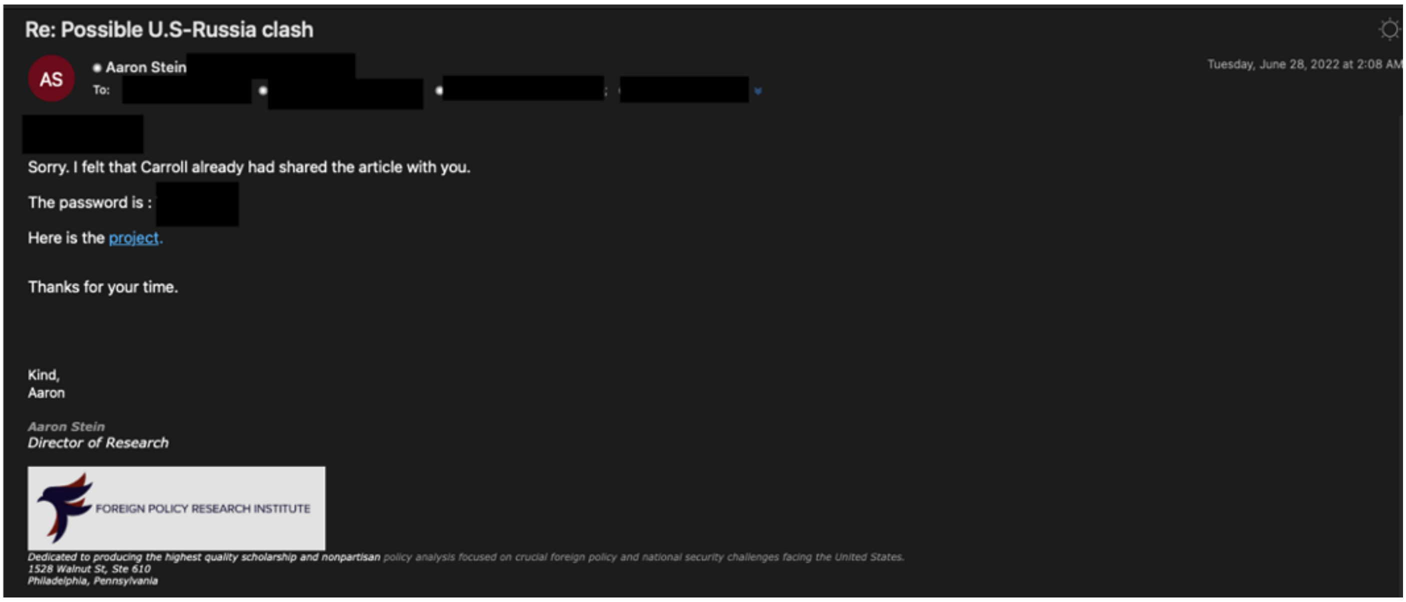
Thanks for your time.

Best,
Carroll

--
Carroll Doherty
Director of Political Research
+1 (757)743-7707
Pew Research Center
A nonpartisan fact tank that informs the public about the issues and attitudes.
1615 L Street, NW Suite 800 Washington, D.C.
www.pewresearch.org

Figure 5. Screenshots of "Carroll" persona sending the target a malicious OneDrive link and password.

"Carroll" sent the password separately and followed up with the target to let them know the document is secure because it cannot be read without the password. Four days later, one of the cc'd TA453 personas, "Aaron Stein," dropped "Carroll" from the email thread, apologized to the target, and resent the same OneDrive link and password (Figure 6).



Re: Possible U.S-Russia clash

AS ● Aaron Stein [redacted]

Tuesday, June 28, 2022 at 2:08 AM

To: [redacted] ● [redacted] ● [redacted] ; [redacted]

[redacted]

Sorry. I felt that Carroll already had shared the article with you.

The password is : [redacted]

Here is the project.

Thanks for your time.

Kind,
Aaron

Aaron Stein
Director of Research

FOREIGN POLICY RESEARCH INSTITUTE

Dedicated to producing the highest quality scholarship and nonpartisan policy analysis focused on crucial foreign policy and national security challenges facing the United States.
1528 Walnut St, Ste 610
Philadelphia, Pennsylvania

Figure 6. A cc'd TA453 persona attempting to convince a target of the legitimacy of the campaign.

Similar to the document sent by "Harald," this document also used remote template injection to download *Korg*.

Korg—TA453's Latest Remote Template Injection

As noted above, some of TA453's campaigns delivered OneDrive links that hosted malicious documents. The documents are the latest version of the TA453 remote template injection documents discussed by

PwC in July 2022. The password protected documents downloaded the macro enabled template documents from 354pstw4a5f8.filecloudonline[.]com. Proofpoint observed multiple campaigns reusing that specific filecloudonline[.]com host. The downloaded template, dubbed *Korg* by Proofpoint, has three macros: Module1.bas, Module2.bas, and ThisDocument.cls. The macros collect information such as username, list of running processes along with the user's public IP from my-ip.io and then exfiltrates that information using the Telegram API.

At this time, Proofpoint has only observed the beaconing information and has not observed any follow-on exploitation capabilities. The lack of code execution or command and control capabilities within the TA453 macros is abnormal. Proofpoint judges that infected users may be subject to additional exploitation based on the software identified on their machines.

Attribution

Proofpoint continues to assess that TA453 operates in support of the Islamic Revolutionary Guard Corps (IRGC). This assessment is based on a variety of evidence, including overlaps in unit numbering between Charming Kitten reports and IRGC units as identified by PwC, the US Department of Justice indictment of Monica Witt and IRGC-affiliated actors, and analysis of TA453 targeting compared to reported IRGC-IO priorities.

Proofpoint tracks multiple subgroups of TA453 differentiated primarily by victimology, techniques, and infrastructure. Some subgroups in their typical campaigns will engage in benign conversations with targets for weeks before delivering malicious links. Conversely, another subgroup tends to immediately send a malicious link in the initial email.

While the mere presence of specific indicators does not definitively condemn an email as TA453, indicators of a possible TA453-linked persona include:

- Use of Gmail, Outlook, Hotmail, or AOL email address instead of institutional email
- Including other "personal email accounts" in the conversation
- Replying to blank email
- Asking to collaborate on research about issues relating to the Middle East
- Offering a Zoom call (often resulting in a credential harvesting link)
- Sending unsolicited collaboration "draft" attachments

Conclusion

All threat actors are in constant states of iterating their tools, tactics, and techniques (TTPs), advancing some while deprecating others. The use of MPI by TA453, while the group's latest technique, is likely to continue to evolve and morph as this group hunts for intelligence in support of the IRGC. Proofpoint researchers have already started to observe this potential next step with TA453 attempting to send a blank email, then respond to the blank email all while including all their "friends" on the CC line. This is likely the threat actor's attempt at bypassing security detection.

Researchers involved in international security, particularly those specializing in Middle Eastern studies or nuclear security, should maintain a heightened sense of awareness when receiving unsolicited emails.For example, experts that are approached by journalists should check the journalist’s or their publication’s website to see if the email address belongs to them.