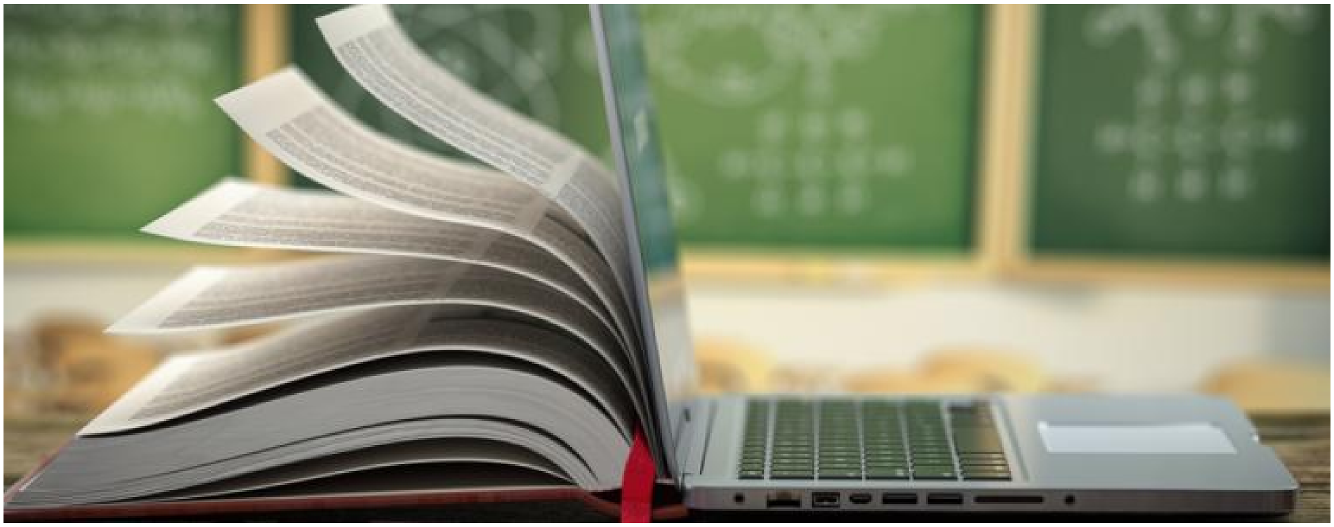
Operation SpoofedScholars: A Conversation with TA453

June 30, 2021

Blog
Threat Insight
Operation SpoofedScholars: A Conversation with TA453



July 13, 2021 Joshua Miller, Crista Giering, & the Threat Research Team

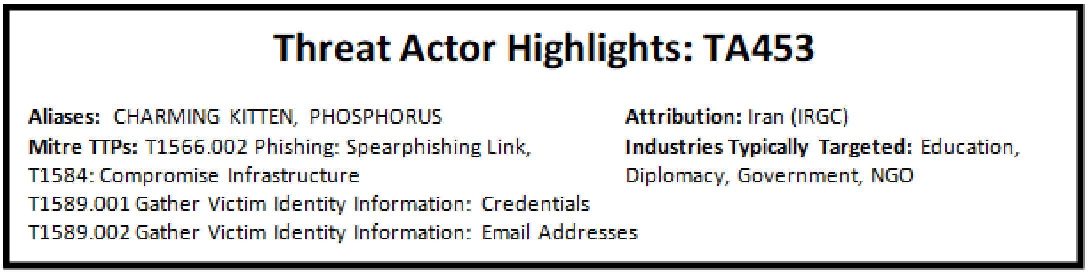
Key Takeaways

- TA453, an Iranian-state aligned actor, masqueraded as British scholars to covertly target individuals of intelligence interest to the Iranian government in what Proofpoint has dubbed Operation SpoofedScholars.
- The email conversations were benign until TA453 provided a link to a compromised website hosting a credential harvesting page.
- The use of a legitimate but actor-compromised website is an increase in sophistication compared to TA453's historical Tactics, Techniques, and Procedures of using actor-controlled credential phishing websites.
- Proofpoint has worked with the appropriate authorities to conduct victim notification.

Overview

Masquerading as UK scholars with the University of London's School of Oriental and African Studies (SOAS), the threat actor TA453 has been covertly approaching individuals since at least January 2021 to solicit sensitive information. The threat actor, an APT who we assess with high confidence supports Islamic Revolutionary Guard Corps (IRGC) intelligence collection efforts, established backstopping for their credential phishing infrastructure by compromising a legitimate site of a highly regarded academic institution to deliver personalized credential harvesting pages disguised as registration links. Identified targets included experts in Middle Eastern affairs from think tanks, senior professors from well-known academic institutions, and journalists specializing in Middle Eastern coverage.

These connection attempts were detailed and extensive, often including lengthy conversations prior to presenting the next stage in the attack chain. Once the conversation was established, TA453 delivered a "registration link" to a legitimate but compromised website belonging to the University of London's SOAS radio. The compromised site was configured to capture a variety of credentials. Of note, TA453 also targeted the personal email accounts of at least one of their targets. In subsequent phishing emails, TA453 shifted their tactics and began delivering the registration link earlier in their engagement with the target without requiring extensive conversation. This operation, dubbed SpoofedScholars, represents one of the more sophisticated TA453 campaigns identified by Proofpoint.



Threat Actor Highlights: TA453

Aliases: CHARMING KITTEN, PHOSPHORUS

Mitre TTPs: T1566.002 Phishing: Spearphishing Link,
T1584: Compromise Infrastructure
T1589.001 Gather Victim Identity Information: Credentials
T1589.002 Gather Victim Identity Information: Email Addresses

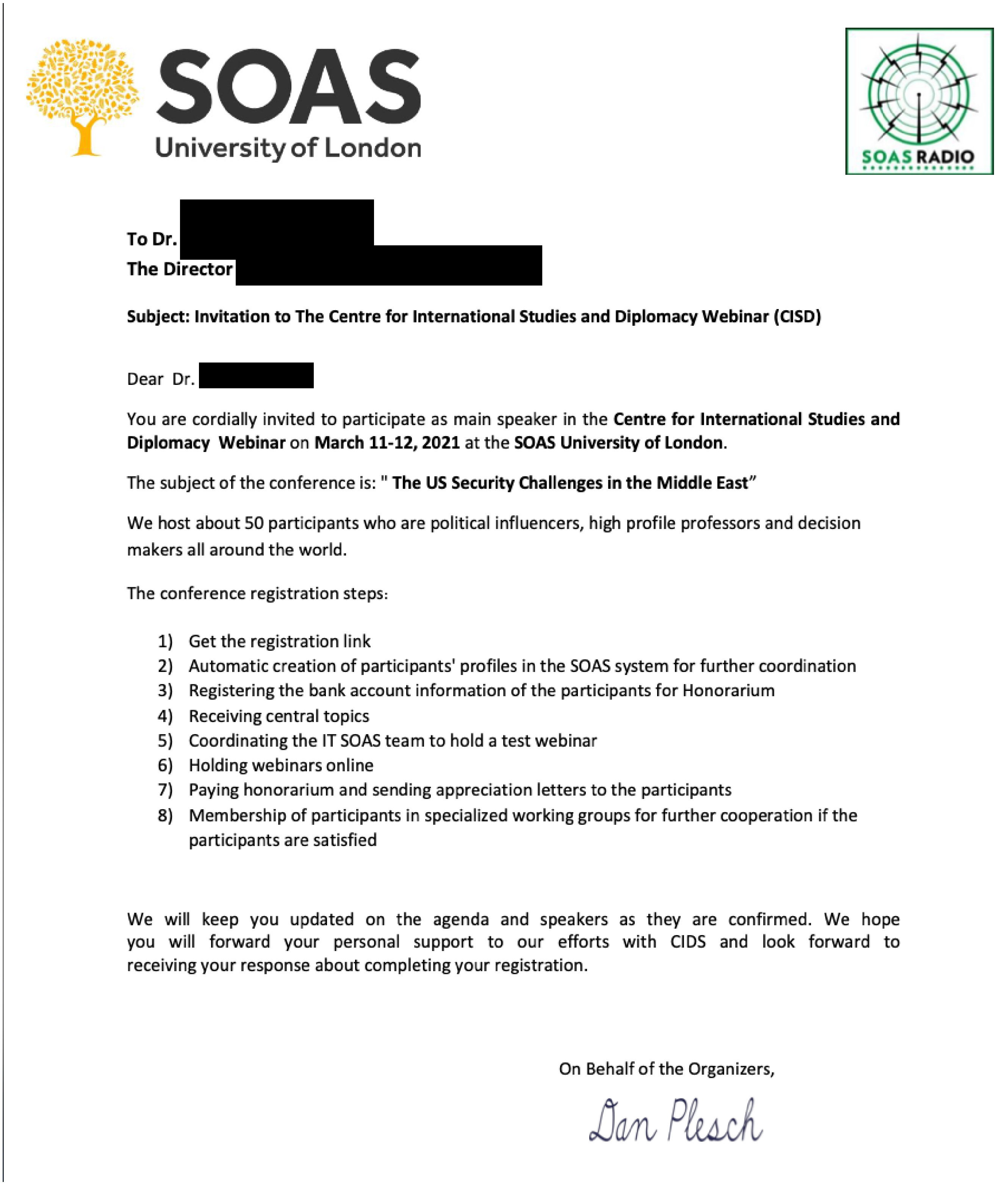
Attribution: Iran (IRGC)

Industries Typically Targeted: Education, Diplomacy, Government, NGO

Chatting with TA453

In early 2021, a TA453 persona, “Dr.Hanns Bjoern Kendel, Senior Teaching and Research Fellow at SOAS University in London,” used email address hannse.kendel4[@]gmail.com to solicit conversations with targets. The following is a brief summary of an example conversation observed by Proofpoint Threat Research:

TA453 sent an initial email trying to entice the target with a prospective invitation to an online conference on “The US Security Challenges in the Middle East.” TA453 strived to connect with the individual via phone to discuss the invitation; however, after the target hedged and emphatically stated that they wanted a written proposal with the details, TA453 acquiesced with conference specifics. After a little back and forth that verified the target’s interest, TA453 provided a detailed invitation to the fake conference (Figure 1). The conversation concluded with TA453 attempting to get the target to connect via videoconferencing.



SOAS
University of London
SOAS RADIO

To Dr. [redacted]
The Director [redacted]

Subject: Invitation to The Centre for International Studies and Diplomacy Webinar (CISD)

Dear Dr. [redacted]

You are cordially invited to participate as main speaker in the **Centre for International Studies and Diplomacy Webinar** on **March 11-12, 2021** at the **SOAS University of London**.

The subject of the conference is: " **The US Security Challenges in the Middle East**"

We host about 50 participants who are political influencers, high profile professors and decision makers all around the world.

The conference registration steps:

1) Get the registration link
2) Automatic creation of participants' profiles in the SOAS system for further coordination
3) Registering the bank account information of the participants for Honorarium
4) Receiving central topics
5) Coordinating the IT SOAS team to hold a test webinar
6) Holding webinars online
7) Paying honorarium and sending appreciation letters to the participants
8) Membership of participants in specialized working groups for further cooperation if the participants are satisfied

We will keep you updated on the agenda and speakers as they are confirmed. We hope you will forward your personal support to our efforts with CIDS and look forward to receiving your response about completing your registration.

On Behalf of the Organizers,

Dan Plesch

Figure 1. Fake conference invitation.

Conversation Analysis

Throughout the conversation, Proofpoint identified a few interesting themes:

- TA453 demonstrates passable English skills and is open to voice communication via videoconferencing.
- TA453 demonstrates an interest in mobile phone numbers, possibly for mobile malware or additional phishing.
- TA453 repeatedly demonstrated a desire to connect with the target in real-time.

Personal Targeting

In addition to Hanns' solicitations, at least one target received a credential harvesting email to their personal email account. This attempt did not masquerade as Dr. Kendel but did still attempt to harvest credentials from the target. Currently, Proofpoint does not have more information on this specific kill chain.

Campaign Breakdown

Targets

TA453 targets in Operation SpoofedScholars can be clustered into three main categories that are consistent with the IRGC's historical collection priorities.

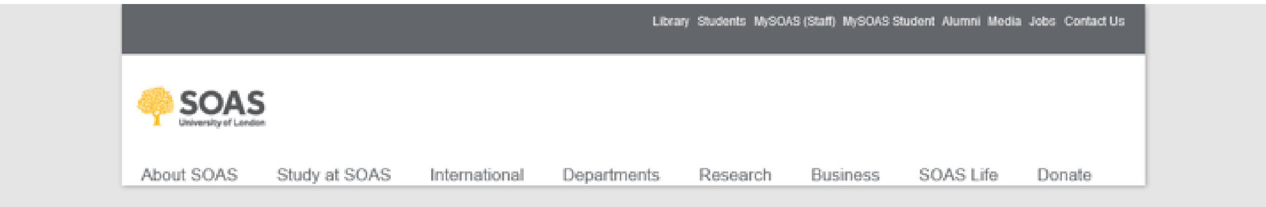
- Senior think tank personnel
- Journalists focused on Middle Eastern affairs
- Professors

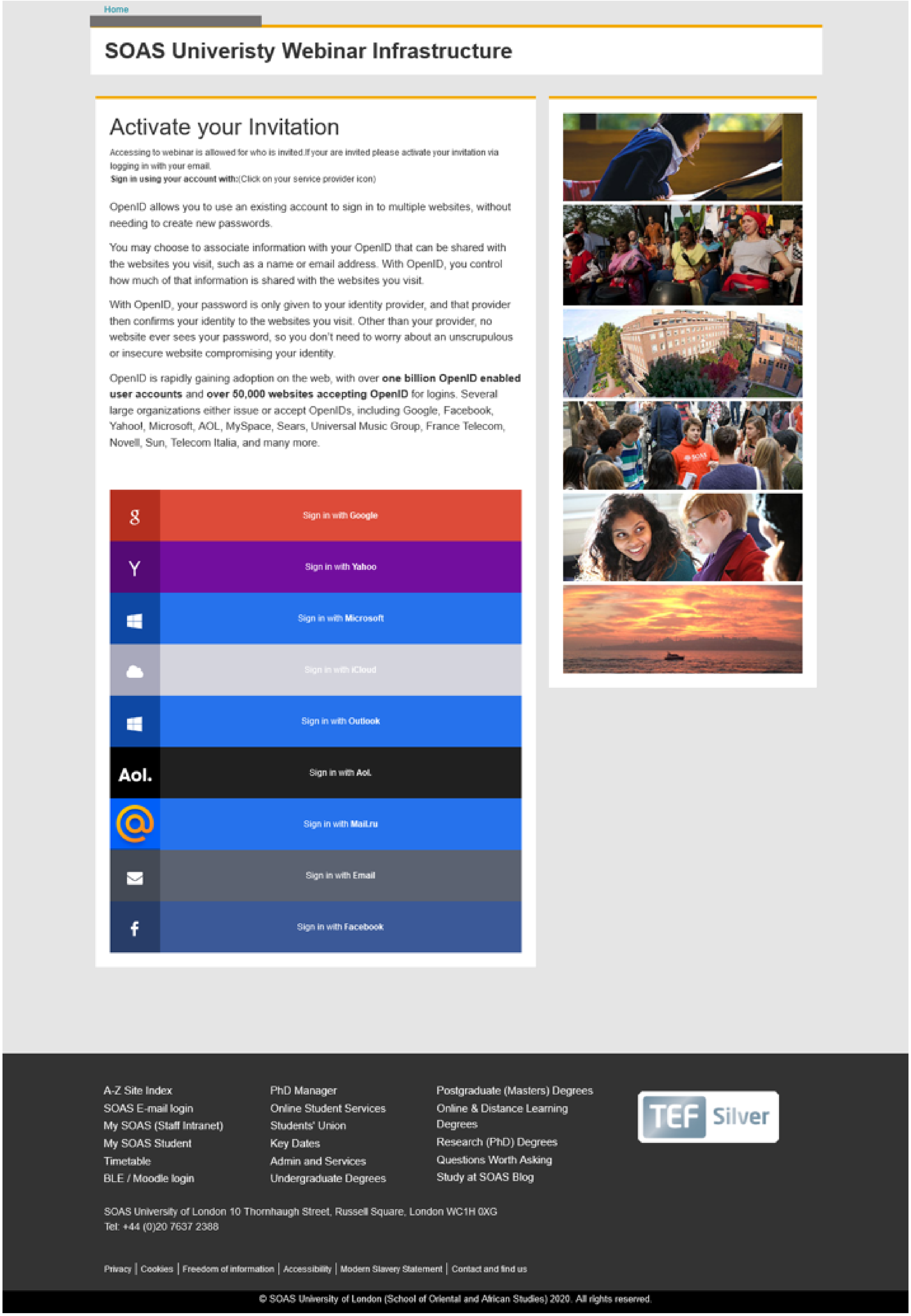
These groupings consistently have information of interest to the Iranian government, including, but not limited to, information about foreign policy, insights into Iranian dissident movements, and understanding of U.S. nuclear negotiations, and most of the identified targets have been previously targeted by TA453. Targeting appeared to be highly selective, with less than ten organizations targeted, according to Proofpoint data.

Infrastructure

Once TA453 established a time for the target to activate their invitation, the TA453 persona provided the personalized link to the intended victim. The link led to a "Webinar Control Panel" on a legitimate but compromised website belonging to University of London's SOAS, a research institution. According to Proofpoint research, while TA453 does appear to have elevated privileges allowing them to create credential harvesting pages at soasradio[.]org, other pages on the site continue to host legitimate SOAS-affiliated content.

TA453 strengthened the credibility of the attempted credential harvest by utilizing personas masquerading as legitimate affiliates of SOAS to deliver the malicious links. The displayed webpage (Figure 2) offers users the ability to use "OpenID" to log in with the following mail providers; Google, Yahoo, Microsoft, iCloud, Outlook, AOL, mail.ru, Email, and Facebook. The website URI was hxxps://soasradio[.]org/connect/?memberemailid= [RedactedInitials of Target]-[String of alphanumeric characters].





SOAS Univeristy Webinar Infrastructure

Activate your Invitation

Accessing to webinar is allowed for who is invited.If your are invited please activate your invitation via logging in with your email.
Sign in using your account with:(Click on your service provider icon)

OpenID allows you to use an existing account to sign in to multiple websites, without needing to create new passwords.

You may choose to associate information with your OpenID that can be shared with the websites you visit, such as a name or email address. With OpenID, you control how much of that information is shared with the websites you visit.

With OpenID, your password is only given to your identity provider, and that provider then confirms your identity to the websites you visit. Other than your provider, no website ever sees your password, so you don't need to worry about an unscrupulous or insecure website compromising your identity.

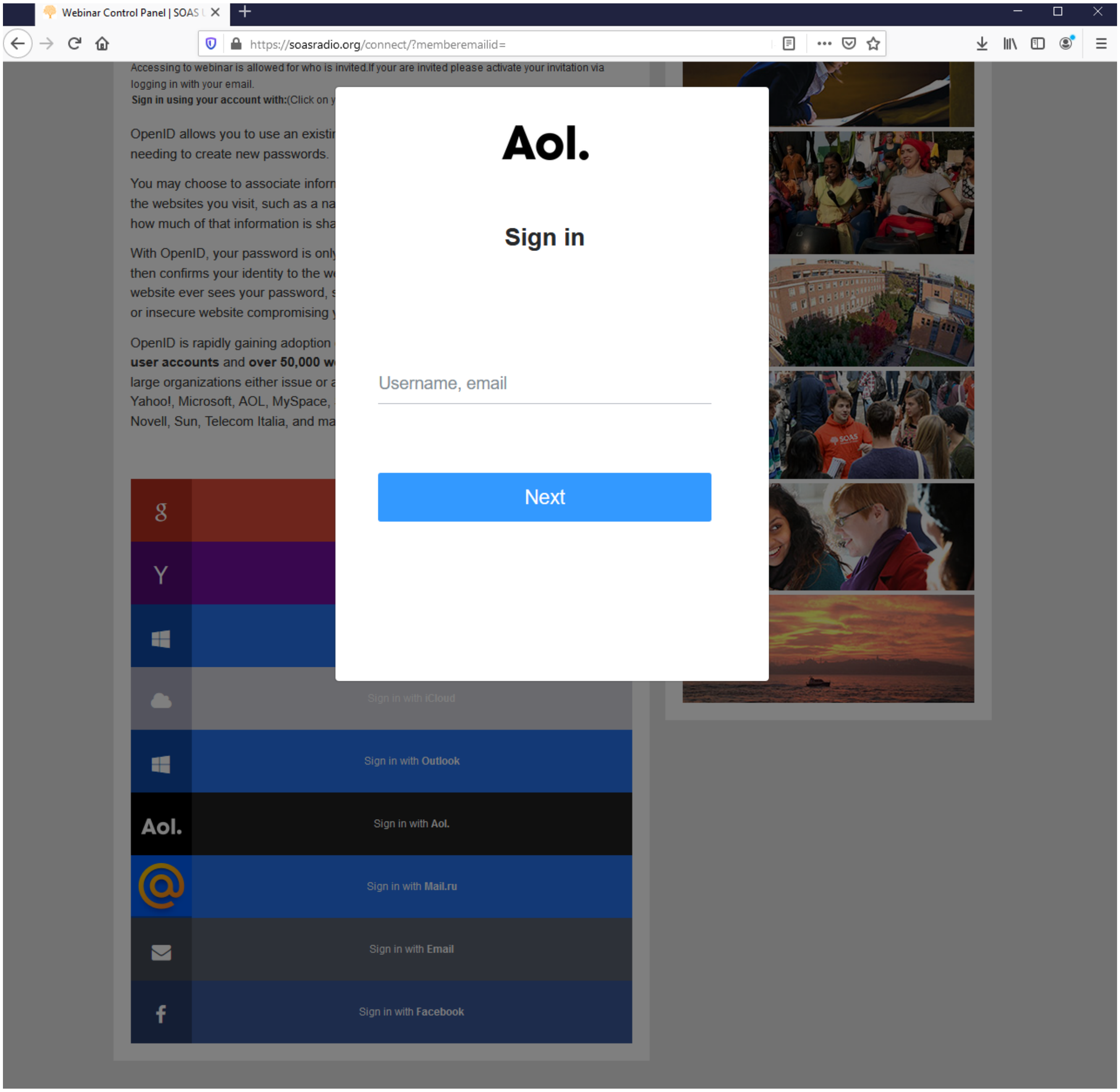
OpenID is rapidly gaining adoption on the web, with over **one billion OpenID enabled user accounts** and **over 50,000 websites accepting OpenID** for logins. Several large organizations either issue or accept OpenIDs, including Google, Facebook, Yahoo!, Microsoft, AOL, MySpace, Sears, Universal Music Group, France Telecom, Novell, Sun, Telecom Italia, and many more.

SOAS University of London 10 Thornhaugh Street, Russell Square, London WC1H 0XG
Tel: +44 (0)20 7637 2388

© SOAS University of London (School of Oriental and African Studies) 2020. All rights reserved.

Figure 2. SOAS displayed webpage.

When a particular provider is clicked, a pop-up box (Figure 3) displays the actual credential phishing box. Of the options, Google, Microsoft, and Email buttons prefilled the target's email address. Based on the variety of email providers along with TA453's insistence that the target log on when TA453 was online, Proofpoint assesses that TA453 was planning on immediately validating the captured credentials manually.



Accessing to webinar is allowed for who is invited.If your are invited please activate your invitation via logging in with your email.
Sign in using your account with:(Click on y

OpenID allows you to use an existi
needing to create new passwords.

You may choose to associate infor
the websites you visit, such as a na
how much of that information is sha

With OpenID, your password is onl
then confirms your identity to the w
website ever sees your password, s
or insecure website compromising y

OpenID is rapidly gaining adoption
user accounts and **over 50,000 w**
large organizations either issue or a
Yahoo!, Microsoft, AOL, MySpace,
Novell, Sun, Telecom Italia, and ma

Figure 3. "AOL login window"

Hanns Kendel was not the only SOAS scholar spoofed by TA453 during Operation SpoofedScholars. Months later, TA453 began spoofing Tolga Sinmazdemir, another individual associated with SOAS. These emails solicited contributions to a "DIPS Conference" and would have likely followed a similar kill chain discussed above. In mid-May, TA453 returned, using a different email (hanse.kendel4[@]gmail.com) to recruit for a webinar.

Attribution

As discussed previously in Proofpoint’s research on TA453’s BadBlood campaign, Proofpoint analysts cannot independently confirm that TA453 is part of the IRGC. However, the tactics and techniques used by the group and their overall targeting detected by Proofpoint is in line with IRGC intelligence collection priorities, which gives us high confidence in our assessment that TA453 operates in support of the IRGC. The IRGC, specifically the IRGC Intelligence Organization, collects intelligence and conducts operations in support of a variety of assigned responsibilities. According to the Meir Amit Intelligence and Terrorism Information Center’s November 2020 report, some of the IRGC IO’s responsibilities include foiling political subversion, combating western cultural penetration, and supporting the arrest of Iranian dual nationals.

Likewise, attribution specifically for Operation SpoofedScholars is based on TTP similarities to previous TA453 campaigns and consistency with TA453’s historical targeting. TA453 often uses free email providers to spoof individuals familiar to their targets to increase the likelihood of successful compromise. Additionally, as previously discussed, TA453 concentrates their credential phishing to specific individuals of interest to collect intelligence through exfiltration of sensitive email and contacts or initial access for future phishing campaigns.

Mitigation

For specific mitigations against Operation SpoofedScholars, Proofpoint recommends investigating network traffic to soasradio[.]org, specifically URIs starting with hxxps://soasradio[.]org/connect/?memberemailid=. Additionally, emails from hanse.kendel4[@]gmail.com, hannse.kendel4[@]gmail.com, and t.sinmazdemir32[@]gmail.com should be considered suspect and investigated.

Broader mitigation efforts against TA453 campaigns include increased awareness and investigation of unusual communication from professional contacts. Academics, journalists, and think tank scholars should practice caution and verify the identity of the individuals offering them unique opportunities, especially if those opportunities occur virtually. Using multifactor authentication provides another layer of protection against TA453 credential harvesting.

Conclusion

TA453 illegally obtained access to a website belonging to a world class academic institution to leverage the compromised infrastructure to harvest the credentials of their intended targets. The use of legitimate, but compromised, infrastructure represents an increase in TA453’s sophistication and will almost certainly be reflected in future campaigns. TA453 continues to iterate, innovate, and collect in support of IRGC collection priorities. While some of the identified selectors no longer appear to be active in TA453 operations, Proofpoint assesses with high confidence that TA453 will continue to spoof scholars around the world in support of TA453’s intelligence collection operations in support of Iranian government interests. Academics, journalists, and think tank personnel should practice caution and verify the identity of the individuals offering them unique opportunities.

ET Signature

2033317 - ET Malware Operation SpoofedScholars Activity (GET)

Subscribe to the Proofpoint Blog