Iranian Spear-Phishing Operation Targets Former Israeli and US High-Ranking Officials

⋮ 6/14/2022

June 14, 2022

Introduction

Check Point Research uncovers a recent Iranian-based spear-phishing operation aimed against former Israeli officials, high-ranking military personnel, research fellows in research institutions, think tanks, and against Israeli citizens. The attacks use a custom phishing infrastructure, as well as a wide array of fake email accounts to impersonate trusted parties. To establish deeper trust with new targets, the threat actors performed an account takeover of some victims' inboxes , and then hijacked existing email conversations to start attacks from an already existing email conversation between a target and a trusted party and continue that conversation in that guise.

In order to facilitate their spear-phishing operation, the attackers operated a fake URL shortener **Litby[.]us**, to disguise the phishing links, as well as utilized a legitimate identity verification service **validation.com**, for the theft of identity documents.

In this publication, we analyze the infrastructure used by the threat actor, their methodologies, a possible attribution of the threat actor behind this attack and their underlying motives. The visible purpose of this operation appears to be aimed at gaining access to victims' inboxes, their Personally Identifiable Information (PII) and their identity documents. However, the recent escalating tensions between Israel and Iran, followed by the Israeli official publication uncovering evidence of Iranian cyber operations

leading to actions outside of the cyber domain, could shed more light on the real purpose of the infrastructure we describe in this report.

High profile targets of this operation include:

- Tzipi Livni – former Foreign Minister and Deputy Prime Minister of Israel
- Former Major General who served in a highly sensitive position in the Israeli Defense Forces (IDF)
- Chair of one of Israel's leading security think tanks
- Former US Ambassador to Israel
- Former Chair of a well known Middle East research centre
- Senior executive in the Israeli defense industry

Initial Vector: Spear-phishing

From our observations, the attackers use email communication as the main tool for the initial contact with the target. They often utilize the email thread hijacking technique and continue an already existing email thread. The continuation of the thread takes place either from the compromised account itself, or from a newly created email address – where they copy-paste an old thread to a new email.

For the purpose of impersonation, if the attackers want to impersonate `John Doe` working at `corp.org`, they would often create a new inbox with an online email provider, in the following format: `joe.doe.corp@gmail.com`

The conversations in many cases reference Iran and Israel security issues.

Case 1: Tzipi Livni

Tzipi Livni is an Israeli politician, diplomat and lawyer, and is also the former Foreign Minister of Israel, Deputy Prime Minister, Minister of Justice, and Leader of the Opposition.

Livni was approached via email by someone impersonating a well known former Major General in the IDF who served in a highly sensitive position. The email was sent from his genuine email address which had previous correspondence with her in the past. The email contained a link to a file which the attacker requested her to open and read. When she delayed doing so, the attacker approached her several times asking her to open the file using her email password. This prompted her suspicions. When she met the former Major General and asked him about the email, it was confirmed that he never sent such an email to her. She then approached Check Point to investigate this suspicious event.

Email Correspondence (partial):

Attacker (Day 1, 11:00 AM)

Original (Hebrew)

לידידים יקרים שלום רב,

רצ"ב בזה מאמר לסיכום השנה. ((*לעינכם בלבד*))

כמובן שאיני מעוניין להפיצו, כי הוא לא הגרסה הסופית
אשמח לקבל הערות מכל סוג

המשך יום נעים,

[redacted]

Translated

Hello my dear friends,

Please see attached article to summarize the year. ((*eyes only*))

Of course I don't want it to be distributed, because it is not the final version.

I would be happy to receive remarks of any kind

Have a great rest of the day,

[redacted]

Attacker (Day 1, 01:59 PM)

Original (Hebrew)

חברים
אני מחכה לשמוע את הערותיכם.
אותם חברים שעדיין לא הצליחו לגשת לקובץ, אני
אומר להם שזה קישור פרטי ואפשר שאתם צריכים
לאמת את זהותכם בכניסה לחשבון.
אם יש בעייה אני מוכן לעזור
בכבוד רב.
[redacted]

Translated

Friends

I am waiting to hear your comments.

Those friends who still were unable to access the file, I tell them

that this is a private link, and that you need to verify your identity,

when trying to access the account.

It there is a problem, I am willing to help

Best regards.

[redacted]

Attacker (Day 1, 02:17 PM)

Original (Hebrew)

ציפי
את הצלחת לראות את המאמר?
[redacted]

Translated

Tzipi
Have you managed to view the article?
[redacted]

This was followed by several exchanges between Livni and the attacker.
Unsuccessful to achieve his goals, the attacker resumed its phishing attempt after several days.

Attacker (Day 6, 07:16 AM)

Original (Hebrew)

בוקר טוב
לא שמעתי ממך
כמה חברים שלחו לי הערות. גם הערותיך חשובות מאוד בשבילי.
אני יודע שאת עסוקה מאוד. אבל רציתי לבקש ממך לקחת את הזמן שלך ולקרוא את המאמר.
שבוע טוב
[redacted]

Good morning
I haven't heard from you
Some friends sent me remarks. Your remarks are also very important to me.
I know you are very busy. But I wanted to ask you to take your time and read the article.
Good week
[redacted]

Translated

This was followed by an unsuccessful attempt to convince Tzipi Livni to reset an online password

---

<u>Case 2: The Former Ambassador and the Security Think Tank Chair</u>

In this case, the attackers impersonated an American diplomat (who previously served as the ambassador of the United States to Israel), to target a Chair of one of Israel's leading security think tanks. The following email correspondence took place following a genuine copy-pasted thread between the two entities, from two weeks prior, that was stolen from the inbox of one of the victims (email thread hijacking technique).

Email Correspondence (partial):

Attacker (Day 1, 2:25 PM)

Hi [redacted]
I am invited to a private important meeting to provide consultation about Iran nuclear deal and Vienna talks.
I wrote my thoughts in one page and like to know your ideas about it.
I uploaded it to a personal folder and gave you access to read it.
May you please take a look at it and let me know your opinion.
Look forward to hearing from you.
Kol tuv,
[redacted]

Victim (Day 2, 10:51 PM)

Shalom [redacted]

Sorry! My email at [redacted] went dead for a day! I just saw it, but I cannot access the doc you sent – what to do?

Attacker (Day 3, 8:42 AM)

Shalom [redacted]
Why cannot you access the doc?
What is the problem?
May you give this one a try.

Attacker (Day 3, 2:59 PM)

[redacted]
Do you still have problem with your [redacted] email?

Similar to the email exchange in “Case 1” above, the attackers demonstrate a less-than-patient approach. In this case, with only six hours in between the last two messages sent by the attacker.
In both cases, the underlined blue text within the emails are hyperlinks to `Litby[.]us` URLs – a fake URL shortener service.

Litby – Fake URL Shortener

The attackers created a fake URL shortener service to facilitate their attacks. `Litby[.]us`, which from its name obviously tries to bear some resemblance to the widely used Bitly.com URL shortener – is at the center of these attacks.

Browsing directly to `Litby[.]us`, shows the below page (Fig. 1), which looks like a generic URL shortener service. Although benign at first glance, the website doesn't hold any real functionality: trying to create a new short URL would ask you to register for the service, and trying to click on "Sign Up" would ask you to send an email. At this point, we became suspicious that the attackers didn't just abuse a little-known URL shortener, but this is in fact a site which is part of their infrastructure.

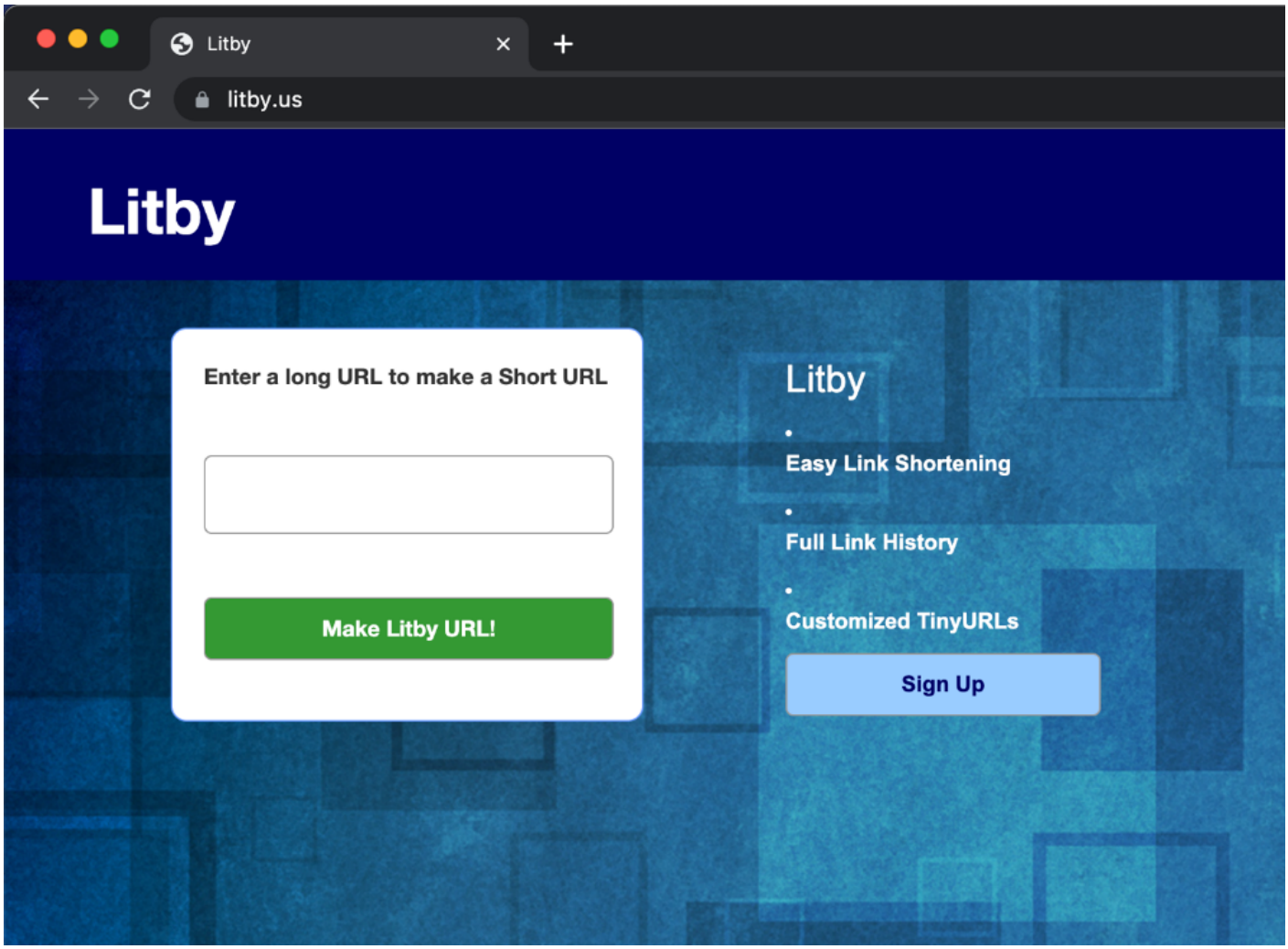

Figure 1: Fake shortener Litby main page.

Redirect Flows

After noticing that `Litby[.]us` is suspicious, we pivoted on this domain via VirusTotal and other sources, to find the various "shortened" URL paths, such as `litby[.]us/Shagrir` (Shagrir means ambassador in Hebrew). Every such URL would redirect the victim to a different flow.

For example:

```
litby[.]us/Ehuziel →  litby[.]us/Ehuziel/continueto.php →
litby[.]us/Ehuziel/index0.php

→ Legitimate Yahoo Inbox page
```

The redirects themselves are implemented using JavaScript, such as in the following reply from the attacker's server:

```
HTTP/1.1 200 OK
keep-alive: timeout=5, max=100
x-powered-by: PHP/7.2.34
content-type: text/html; charset=UTF-8
content-length: 78
vary: Accept-Encoding
date: [redacted]
server: LiteSpeed
x-turbo-charged-by: LiteSpeed

<script>window.location.assign('https://mail.yahoo.com/d/folders/1');</script>
```

Figure 2: JavaScript-based redirect on the attacker's server.

In the below graphics, we showcase the various redirection chains we observed during this research. In the next sections, we will deep dive into the more interesting redirect flows.

Full resolution image.

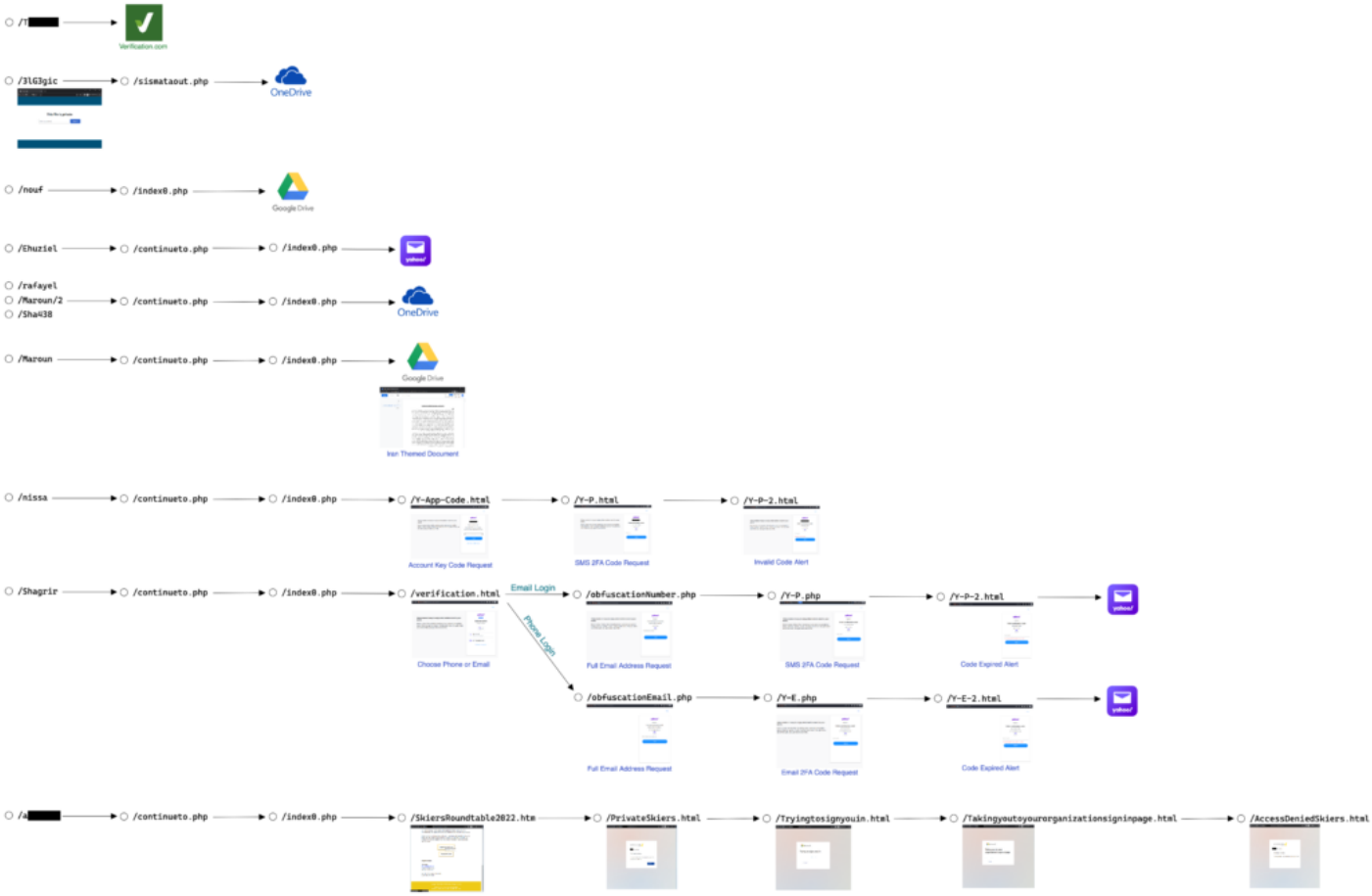

Figure 3: Redirection flows.

General Observations

- Each URL path, which might appear random at first, has indicators that represent the target.
- Phishing pages are customized specifically for the target.
- The redirections often end with the login page of a legitimate service such as Yahoo or some kind of document on OneDrive and GoogleDrive.

Phishing Pages

One of the straightforward purposes of this campaign is to gain access to the inboxes of its victims, specifically for Yahoo inboxes from the flows we observed.
The phishing pages include several stages- asking the user for their account ID followed by an SMS code verification page. It is interesting to note that the truncated phone number within the phishing page was customized specifically for the target, and it corresponds to the public records.
We suspect that once the victim enters his account ID, the phishing backend server would send a password recovery request to Yahoo, and the 2FA code would allow the attackers to gain access to the victim's inbox.

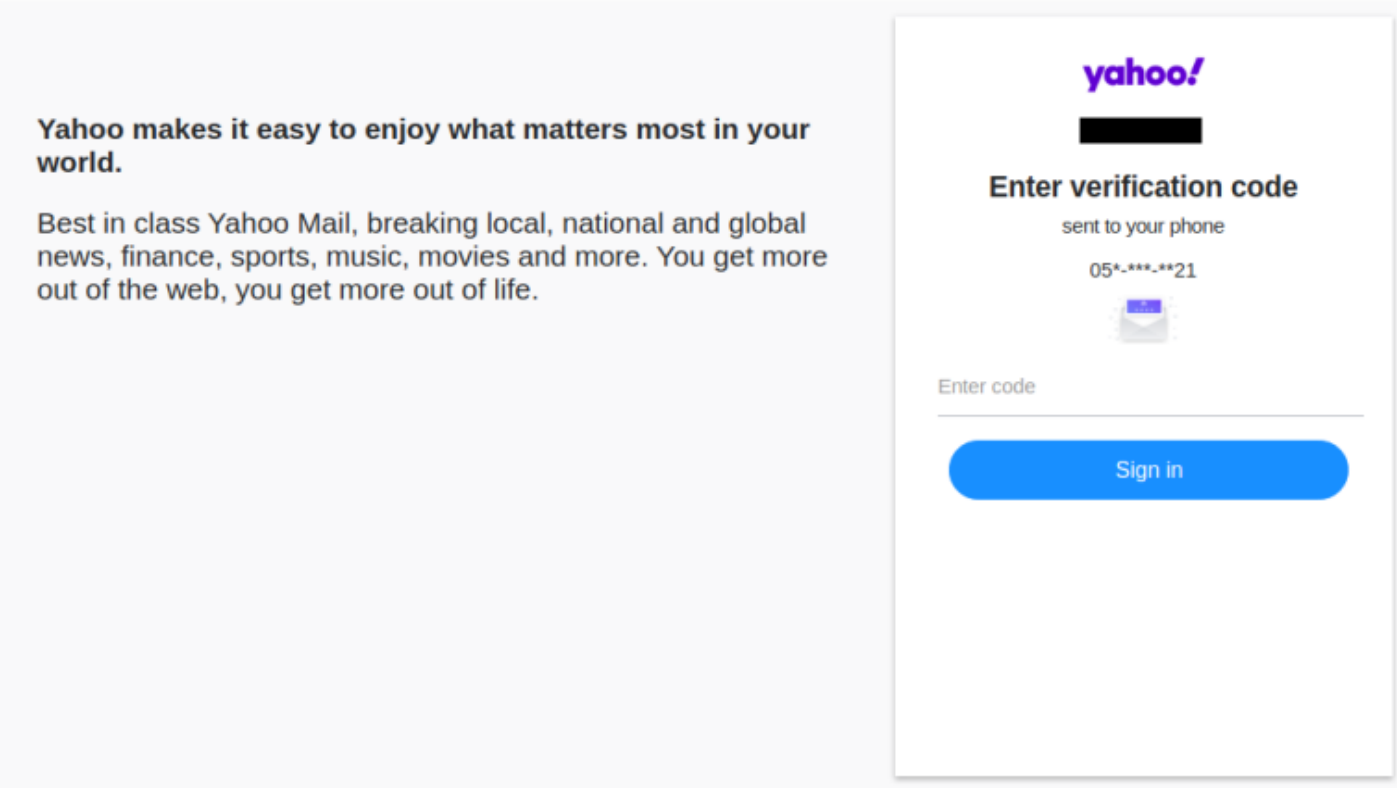

Figure 4: Phishing page used to bypass Yahoo's 2FA.

Identity Documents Theft

Using a legitimate service to facilitate an attack is always a great bonus for a threat actor. It saves resources and the need to develop anything on their own, not to mention that the target and any security solution would be less suspecting of a legitimate service. In this case, the attackers used validation.com, an identity verification service created by the domain registration giant NameCheap, that allows anyone to easily validate their customer's identity by providing an option to scan an ID or documents directly from the webcam, or by uploading a file.

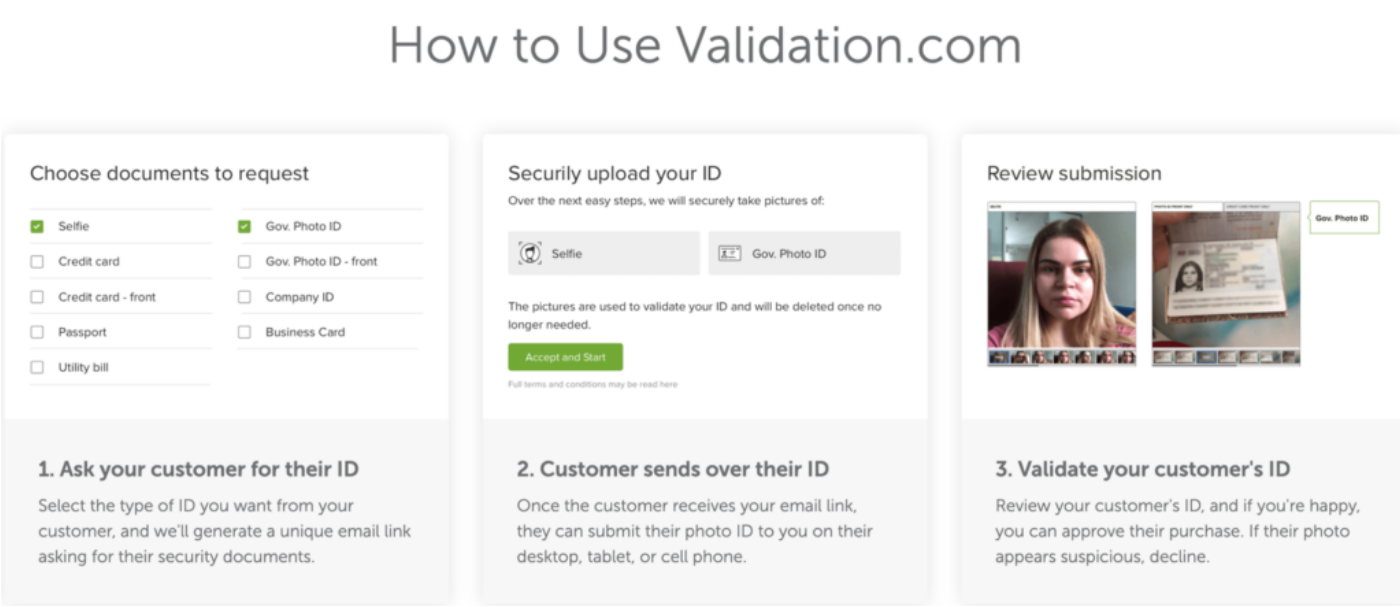

Figure 5: Validation.com service workflow. Source: https://www.namecheap.com/id-validation/.

In this campaign, we have seen one redirection flow from Litby[.]us which leads to a URL on validation.com, and as part of our analysis, we had an indication that the attacker obtained the Passport scan of another high end target. This scan was likely collected by the same means, highlighting the effectiveness of this technique.

Hunting with GHunt – More Fake Profiles

Investigation of another redirection flow: `Litby[.]us/Maroun` showed us possible connections to more personas, whose publications are likely used by the attackers as a lure for their phishing operations. This redirection chain ends up in a benign document (in Hebrew) hosted on Google Docs, discussing Israel's strategy concerning Iran's nuclear program. This document is just a copy of a publication available online by the Jerusalem Institute for Strategy and Security (JISS), and was likely only used as a conversation starter by the attacker.

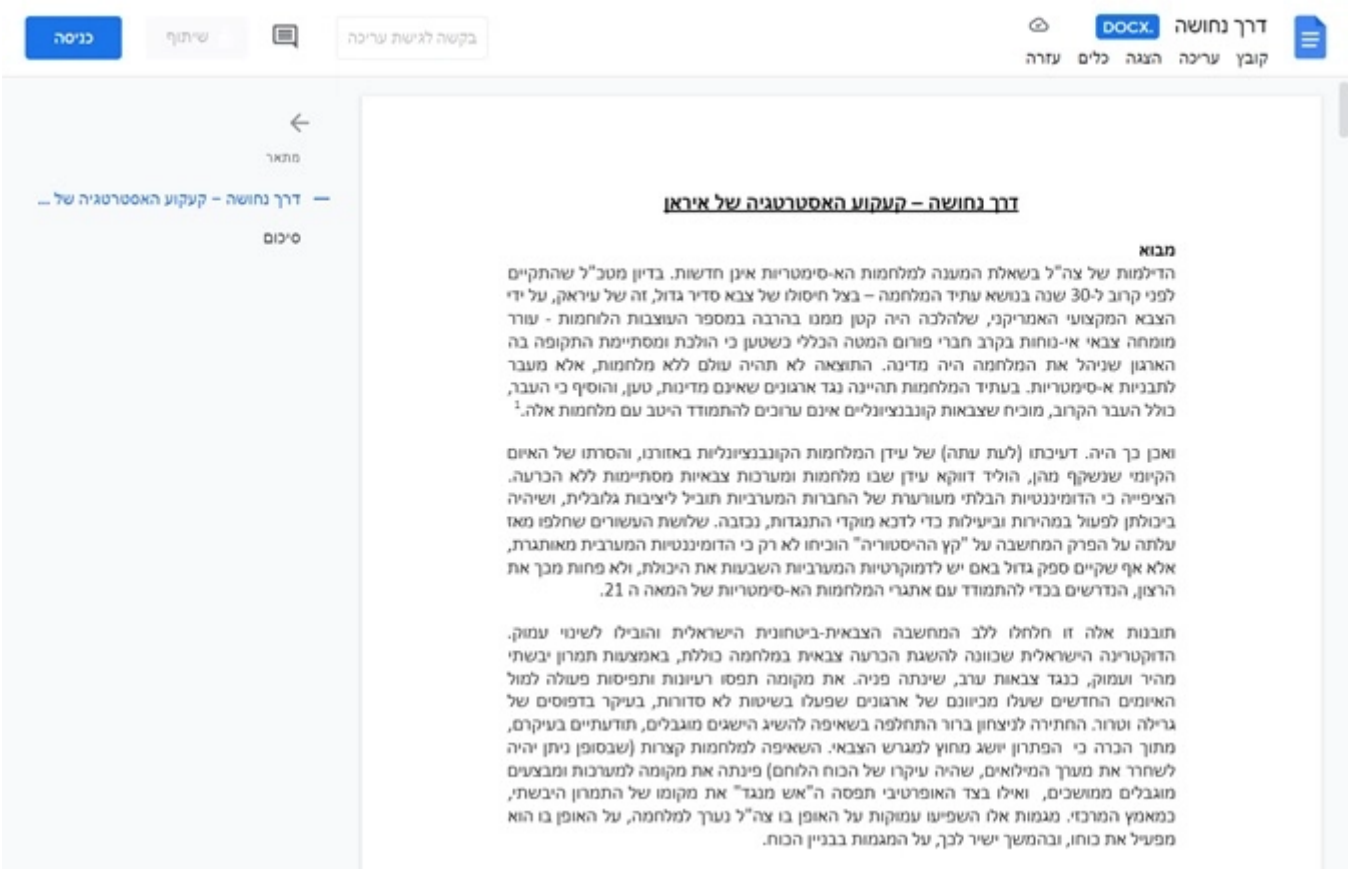

Figure 6: The lure document sent to one of the targets to start the conversation.

When we analyzed the above Google Document with GHunt (an OSINT framework for Google accounts), we were able to find additional details about the account that was used to host this document.
GHunt output showed us the Gmail email account that the attackers likely used to impersonate a Professor from the Jerusalem Institute for Strategy and Security (JISS).

```
Document ID : 1LKbhchznb3B5bISQGNC-wurZ1pTrHOun
[+] Creation date : 2022/02/17 07:48:06 (UTC)
[+] Last edit date : 2022/02/17 07:48:22 (UTC)
Public permissions :
- reader
[+] Owner found !
Name : ████████████
Email : ██████████████@gmail.com
Google ID : 07122295946386800582
[+] Custom profile picture !
=> <https://lh3.googleusercontent.com/a-/███████-█████-
e3kAkwyUkw1VrXQUByErLsyqGGqHP2=s64>
Profile picture saved !
```

Figure 7: GHunt output of the Google Docs URL.

Invitation Abroad

In another redirection chain, the victim lands on a page inviting them to an overseas “Skier’s Roundtable” event as shown below:

Skier's Roundtable Kickoff Email | January 21, 2022

Happy New Year everyone!!!

I am excited to say that we are planning on holding Skier’s Roundtable 2022 as planned. The event is scheduled for Wednesday, March 9 – Sunday, March 13, 2022. As I mentioned in a prior email, the biggest change from prior years is that we will be staying at The Cliff Lodge at Snowbird instead of in private homes/townhouses. We will still be doing our skiing at Alta.

We are monitoring developments with Covid-19 as closely as we can and are hopeful that the number of cases of the Omicron virus will continue to decline over the coming weeks. Our timetable right now is that if we are making the decision to cancel the event, we will try and do that by the first week in February, so stay tuned. However, if for any reason you do not feel comfortable coming to the event, please let me know.

Figure 8: Invitation to the event abroad sent to one of the targets.

Scrolling to the end of the page, the victim is presented with two buttons, both leading to the same redirect chain, ending with a fake corporate login process.

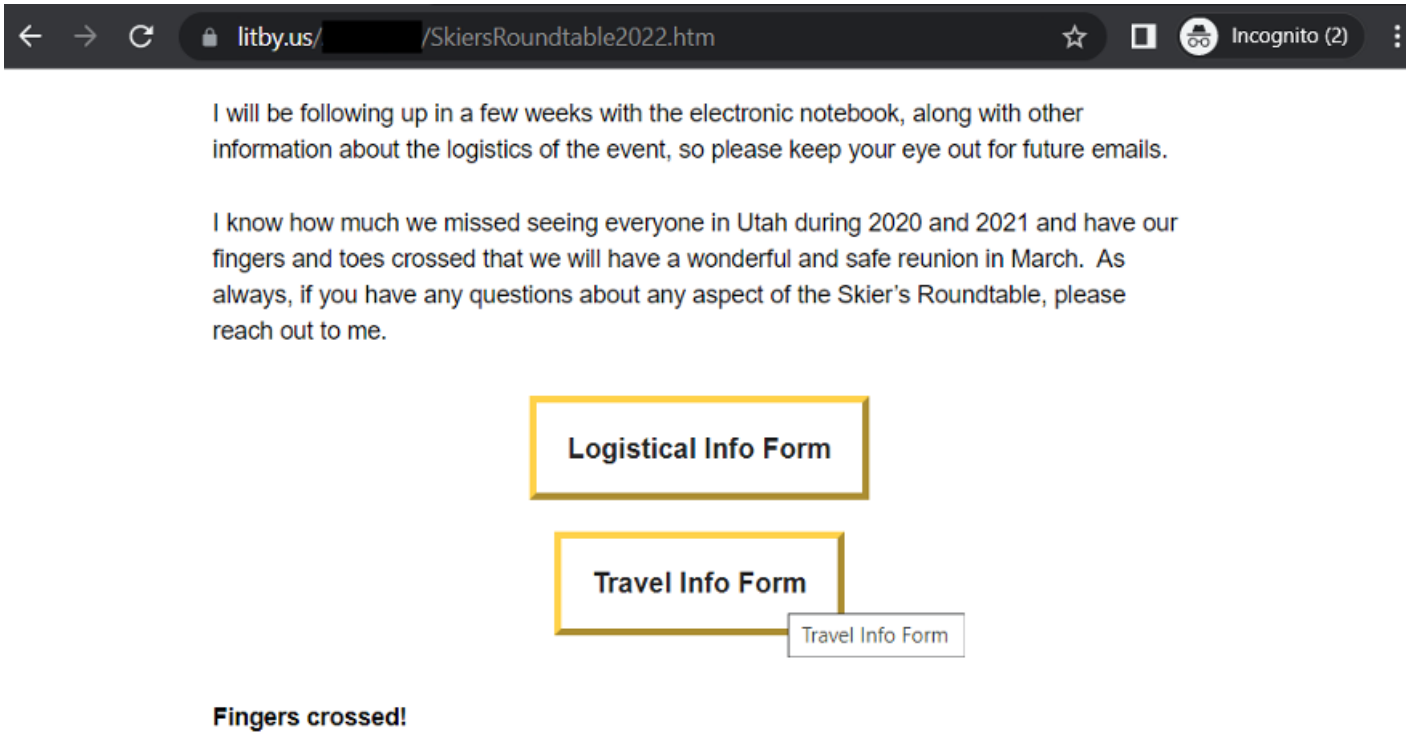

Figure 9: Action items at the end of the fake invitation.

After several fake redirection screens simulating Microsoft's SSO authentication, the victim is presented with a message saying "Access denied. Ask sender to give you access.", likely to further engage the victim in email communication, creating opportunities to request further information, or support credentials stealing attempts.

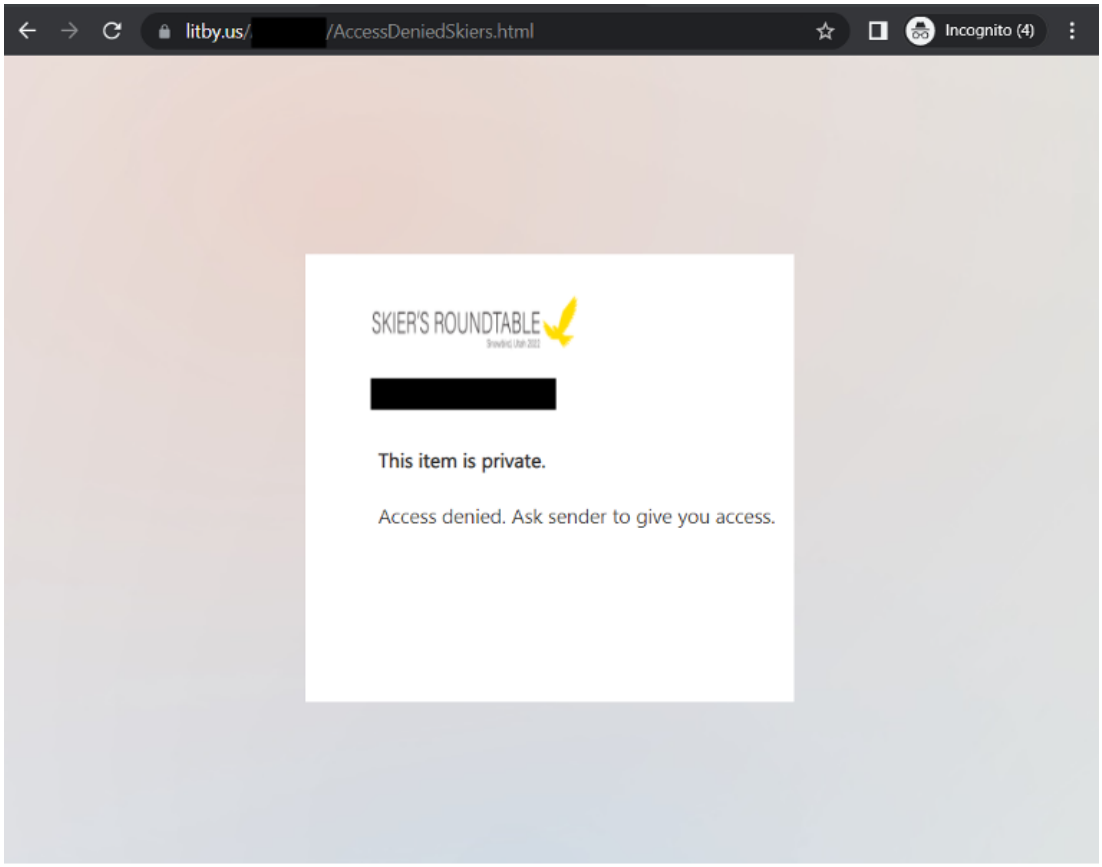

Figure 10: "Access denied" message following the fake login flow.

The Iranian Connection

This campaign exhibits several characteristics signaling to an Iranian backed entity:

- Prime Targets: Israeli officials are a constant prime target for Iranian state entities.
- A connection to the Iran-attributed Phosphorus APT group, which we explore in the next section.

The Iranian origins of the attack present another possibility, though extreme, as to the purpose of the invitation to "Skier's Roundtable" presented above: the victim is invited to an overseas event, possibly to be targeted in a ground operation. Such activity by Iranian state actors is reported quite frequently, amid increasing tension between Israel and Iran. The surrounding geopolitical events such as the Iran nuclear deal negotiations, Iran's increasing activity in the Middle East and Israel's attempts to combat it, all fuel this tension. In fact, it was recently reported that in another similar campaign, as exposed by the Israeli security agency Shin Bet, Israeli officials were invited to overseas events, in a suspected ploy to kidnap them.

The Phosphorus APT Connection

A commented-out section of the source code in one of the phishing pages mentioned above (`litby[.]us/Shagrir/verification.html`), points to the possibility that the same HTML page was previously used by actors in a different attack.

```
<!--  <a href="https://de-ma.online/bAkH2y1qE/1/index1.php"> <li data-challenge-index="300" data
        <div class="card-left">
            <div class="icon-email svg-bg"></div>
        </div>
        <div class="card-content">
            <div class="card-title">
                <strong class="card-title-caption">
                    a*****ky@yahoo.com
                                                </strong>
            </div>
        </div>
        <button type="submit" name="index" class="pure-button puree-button-primary validate-btn"
    </li></a>-->
```

Figure 11: Commented-out source code of the phishing page.

The highlighted domain `de-ma[.]online`, was used by an Iranian APT group named Phosphorus for credential harvesting purposes, according to a Microsoft report from 2020. The group has a long history of conducting high-profile cyber operations, aligned with the interest of the Iranian regime, as well as targeting Israeli officials.

Conclusion

The Iranian-affiliated Phosphorous APT group continues its spear-phishing activity against targets of the Iranian regime. The spear-phishing infrastructure we exposed above puts special focus on high-ranking Israeli officials in the midst of escalating tensions between Israel and Iran. With recent assassinations of Iranian officials (some affiliated with the Israeli's Mossad), and the thwarted attempts to kidnap Israeli citizens worldwide, we suspect that Phosphorous will continue with its ongoing efforts in the future.

Indicators of Compromise

litby[.]us – fake URL shortener

Updates and Corrections

2022-06-14: Iranian Connection section: removed an incorrect bullet that did not add to the attribution to Iran.