THREAT ANALYSIS GROUP

Iranian backed group steps up phishing campaigns against Israel, U.S.

Aug 14, 2024 · 8 min read

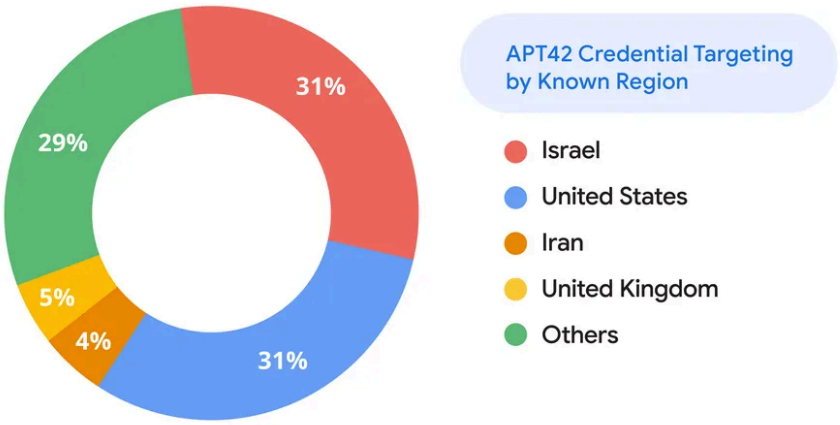
Share

Google Threat Analysis Group

Listen to article 20 minutes

Today Google's Threat Analysis Group (TAG) is sharing insights on APT42, an Iranian government-backed threat actor, and their targeted phishing campaigns against Israel and Israeli targets. We are also confirming recent reports around APT42's targeting of accounts associated with the U.S. presidential election.

Associated with Iran's Islamic Revolutionary Guard Corps (IRGC), APT42 consistently targets high-profile users in Israel and the U.S., including current and former government officials, political campaigns, diplomats, individuals who work at think tanks, as well as NGOs and academic institutions that contribute to foreign policy conversations. In the past six months, the U.S. and Israel accounted for roughly 60% of APT42's known geographic targeting, including the likes of former senior Israeli military officials and individuals affiliated with both U.S. presidential campaigns. These activities demonstrate the group's aggressive, multi-pronged effort to quickly alter its operational focus in support of Iran's political and military priorities.



Between February and late July 2024, APT42 heavily targeted users in Israel and the U.S.

Spikes in APT42 targeting against Israel

Targeted APT42 credential phishing campaigns focused on Israel between February and late July 2024

In April 2024, APT42 intensified their targeting of users based in Israel. They sought out people with connections to the Israeli military and defense sector, as well as diplomats, academics, and NGOs.

APT42 uses a variety of different tactics as part of their email phishing campaigns — including hosting malware, phishing pages, and malicious redirects. They generally try to abuse services like Google (i.e. Sites, Drive, Gmail, and others), Dropbox, OneDrive and others for these purposes. In the course of our work to disrupt APT42, TAG reset any compromised accounts, sent government-backed attacker warnings to the targeted users, updated detections, disrupted malicious Google Sites pages, and added malicious domains and URLs to the Safe Browsing blocklist — dismantling the group's infrastructure.

Government-backed attacker warning

Google Sites phishing: We took down multiple APT42-created Google Sites pages that masqueraded as a petition from the legitimate Jewish Agency for Israel calling on the Israeli government to enter into mediation to end the conflict. The text of the petition was embedded in image files instead of HTML. The Sites page included an ngrok redirect URL, a free service for developers that APT42 has previously used to redirect users to phishing pages.

APT42 Google Sites abuse from an April 2024 phishing campaign

Targeting military, defense, diplomats, academics, and civil society: APT42 attempted to use social engineering to target former senior Israeli military officials and an aerospace executive by sending emails masquerading as a journalist requesting comment on the recent air strikes. They also sent social engineering emails to Israeli diplomats, academics, NGOs and political entities. The emails were sent from accounts hosted by a variety of email service providers, and did not contain malicious content. These emails were likely meant to elicit engagement from the recipients before APT42 attempted to compromise the targets. Google suspended identified Gmail accounts associated with APT42.

A June 2024 campaign targeting Israeli NGOs used a benign PDF email attachment impersonating the legitimate Project Aladdin, which contained a shortened URL link that redirected to a phishing kit landing page designed to harvest Google login credentials.

Benign PDF leading to an APT42 phishing kit landing page

Targeted credential phishing: APT42's success in credential phishing is the result of persistence and heavy reliance on social engineering to appear more credible to their targets. They regularly create accounts or domains that impersonate organizations that might be of interest to the target. For example:

- APT42 masqueraded as the legitimate Washington Institute for Near East Policy in multiple campaigns since April 2024, targeting Israeli diplomats and journalists, researchers at U.S. think tanks, and others. In these campaigns, attackers set the email display name as a legitimate researcher affiliated with the Washington Institute, but the underlying email address was not from the official .org domain.

- APT42 registers typosquat domains very close to the legitimate domains of the organizations they impersonate. For example, APT42 used the domain understandingthewar[.]org to target U.S. military members by impersonating the legitimate Institute for the Study of War. Similarly, APT42 registered brookings[.]email, to spoof the Brookings Institution and used it in multiple campaigns targeting Israel.

Targeting individuals related to the U.S. presidential election

For many years, Google has worked to identify and disrupt malicious activity in the context of democratic elections. During the 2020 U.S. presidential election cycle, we disrupted APT42 attempts to target accounts associated with the Biden and Trump presidential campaigns.

In the current U.S. presidential election cycle, TAG detected and disrupted a small but steady cadence of APT42's Cluster C credential phishing activity. In May and June, APT42 targets included the personal email accounts of roughly a dozen individuals affiliated with President Biden and with former President Trump, including current and former officials in the U.S. government and individuals associated with the respective campaigns. We blocked numerous APT42 attempts to log in to the personal email accounts of targeted individuals.

Recent public reporting shows that APT42 has successfully breached accounts across multiple email providers. We observed that the group successfully gained access to the personal Gmail account of a high-profile political consultant. In addition to our standard actions of quickly securing any compromised account and sending government-backed attacker warnings to the targeted accounts, we proactively referred this malicious activity to law enforcement in early July and we are continuing to cooperate with them.

At the same time, we also informed campaign officials that Google was seeing heightened malicious activity originating from foreign state actors and underscored the importance of enhanced account security protections on personal email accounts.

Today, TAG continues to observe unsuccessful attempts from APT42 to compromise the personal accounts of individuals affiliated with President Biden, Vice President Harris and former President Trump, including current and former government officials and individuals associated with the campaigns.

Understanding APT42's tailored credential phishing

In phishing campaigns that TAG has disrupted, APT42 often uses tactics like sending phishing links either directly in the body of the email or as a link in an otherwise benign PDF attachment. In such cases, APT42 would engage their target with a social engineering lure to set-up a video meeting and then link to a landing page where the target was prompted to login and sent to a phishing page. One campaign involved a phishing lure featuring an attacker-controlled Google Sites link that would direct the target to a fake Google Meet landing page. Other lures included OneDrive, Dropbox and Skype. Over the last six months, we have systematically disrupted these attackers' ability to abuse Google Sites in more than 50 similar campaigns.

Another APT42 campaign template is sending legitimate PDF attachments as part of a social engineering lure to build trust and encourage the target to engage on other platforms like Signal, Telegram or WhatsApp. We expect the attackers would then use these platforms to send a phishing kit to harvest credentials.

APT42 has a number of phishing kits that target a variety of sign-on pages including:

- GCollection/LCollection/YCollection: a sophisticated credential harvesting tool observed by TAG, capable of gathering credentials from Google, Hotmail and Yahoo users respectively. This kit has seen consistent development since it was first observed in use by APT42 in January 2023. The current version implements a seamless flow that supports multi-factor authentication, device PINs and one-time recovery codes in all 3 platforms. A set of landing page URLs are included with the indicators of compromise.

- DWP: a browser-in-the-browser phishing kit often delivered via URL shortener that is less full featured than GCollection.

This spear phishing is supported by reconnaissance, using open-source marketing and social media research tools to identify personal email addresses that might not have default multi-factor authentication or other protection measures that are commonly seen on corporate accounts.

APT42 has also developed a strong understanding of the email providers they target, often researching the security settings of accounts they're targeting using failed login or recovery workflows to determine the configured second factor for authentication to better target their initial phishing attempts. For example, in some cases they have identified that an account is configured to use Device Prompts as an accepted second factor and added support for them in their GCollection phishing kit. APT42 then combines this approach with knowledge of the target's current geographic location based on either public research or social engineering. As a result, APT42 login and recovery attempts often originate from the correct geographic location with the correct credentials and correct second factor for user authentication.

Once APT42 gains access to an account, they often add additional mechanisms of access including changing recovery email addresses and making use of features that allow applications that do not support multi-factor authentication like application specific passwords in Gmail and third-party app passwords in Yahoo. Google's Advanced Protection Program revokes and disables these application specific passwords in Gmail, protecting users from this tactic.

Conclusion

Google Threat Intelligence Group, inclusive of TAG and Mandiant, helps identify, monitor and tackle threats, ranging from coordinated influence operations to cyber espionage campaigns against high-risk entities. TAG tracks and works to disrupt more than 270 government-backed attacker groups from more than 50 countries, and we regularly publish our findings to keep the public informed of these threats.

As we outlined above, APT42 is a sophisticated, persistent threat actor and they show no signs of stopping their attempts to target users and deploy novel tactics. This spring and summer, they have shown the ability to run numerous simultaneous phishing campaigns, particularly focused on Israel and the U.S. As hostilities between Iran and Israel intensify, we can expect to see increased campaigns there from APT42.

We also remain vigilant for targeting around the U.S. election and encourage all high-risk individuals including elected officials, candidates, campaign workers, journalists, election workers, government officials, and others to sign up for Google's Advanced Protection Program. APP is a free, opt-in program designed to protect targeted users against such tactics, preventing unauthorized users from signing into an account even if they know the password.

Indicators of Compromise

APT42 Domains and URLs

DWP Phishing Kit related

accredit-navigation[.]online

hXXps://n9[.]cl/4xgro

GCollection Phishing Kit related

panel-short-check[.]live

check-pabnel-status[.]live

meetroomonlin1925.w3spaces[.]com

smaaaal[.]cfd

click-choose-figured[.]cfd

short-ion-per[.]live

checking-paneling[.]live

hXXps://panel-short-check[.]live/PhyfkFQX

hXXps://check-pabnel-status[.]live/Gcollection/Ref/CkliPwaM

hXXps://check-pabnel-status[.]live/Gcollection/Password

hXXps://panel-short-check[.]live/ZZqt3LYD

hXXps://check-pabnel-status[.]live/Lcollection/Ref/F53OQQkE

hXXps://check-pabnel-status[.]live/Lcollection/Password

hXXps://meetroomonlin1925.w3spaces[.]com/

hXXps://smaaaal[.]cfd/Wp59tqKU

hXXps://click-choose-figured[.]cfd/Gallery/Ref/FSaEM5gG

hXXps://click-choose-figured[.]cfd/Gallery/Password

hXXps://short-ion-per[.]live/08EFNZ1

hXXps://checking-paneling[.]live/aliasauthG/Password

hXXps://checking-paneling[.]live/aliasauthG/autoref/vNSX6c2m

Other

understandingthewar[.]org

brookings[.]email

sharedrive.webredirect[.]org

visioneditor.loseyourip[.]com

s3api[.]shop

hXXps://sharedrive.webredirect[.]org/Khn/shoaGzA/cGNt/dMPaV/kvvhK

hXXps://firebasestorage.googleapis[.]com/v0/b/share-box-5f395.appspot.com/o/onedrive-qrty45.html

hXXps://visioneditor.loseyourip[.]com

hXXps://s3api[.]shop/api/

APT42 Samples (SHA256)

c67cd544a112cab1bb75b3c44df4caf2045ef0af51de9ece11261d6c504add32 *(NEWSTERMINAL)*

bc2597ce09987022ff0498c6710a9b51a1a47ed8082ac044be2838b384157527 (*OFFICEFUEL)*

baac058ddfc96c8aea8c0057077505f0ad3ff20311d999886fed549924404849 (*OFFICEFUEL)*

0180f4f29c550aa1ffaa21af51711b29de99fb1d7c932d008a0e9356ae8a7d60 (*FUELDUMP*)

f83e2b3be2e6db20806a4b9b216edc7508fa81ce60bf59436d53d3ae435b6060 (*FUELDUMP*)

82ae2eb470a5a16ca39ec84b387294eaa3ae82e5ada4b252470c1281e1f31c0a *(FUELDUMP)*

89c1d1b61d7f863f8a651726e29f2ae3de7958f36b49a756069021817947d06c *(FUELDUMP)*

c3486133783379e13ed37c45dc6645cbee4c1c6e62e7988722931eef99c8eaf3 *(GORBLE PS - LNK)*

33a61ff123713da26f45b399a9828e29ad25fbda7e8994c954d714375ef92156 (*GORBLE PS - Stage 1)*

4ac088bf25d153ec2b9402377695b15a28019dc8087d98bd34e10fed3424125f (*GORBLE PS - Stage 2)*

APT42 - IPs Addresses

49.13.194[.]118 (C2 - OFFICEFUEL/FUELDUMP)

91.107.150[.]184 (C2 - OFFICEFUEL/FUELDUMP)

POSTED IN:

Threat Analysis Group Safety & Security