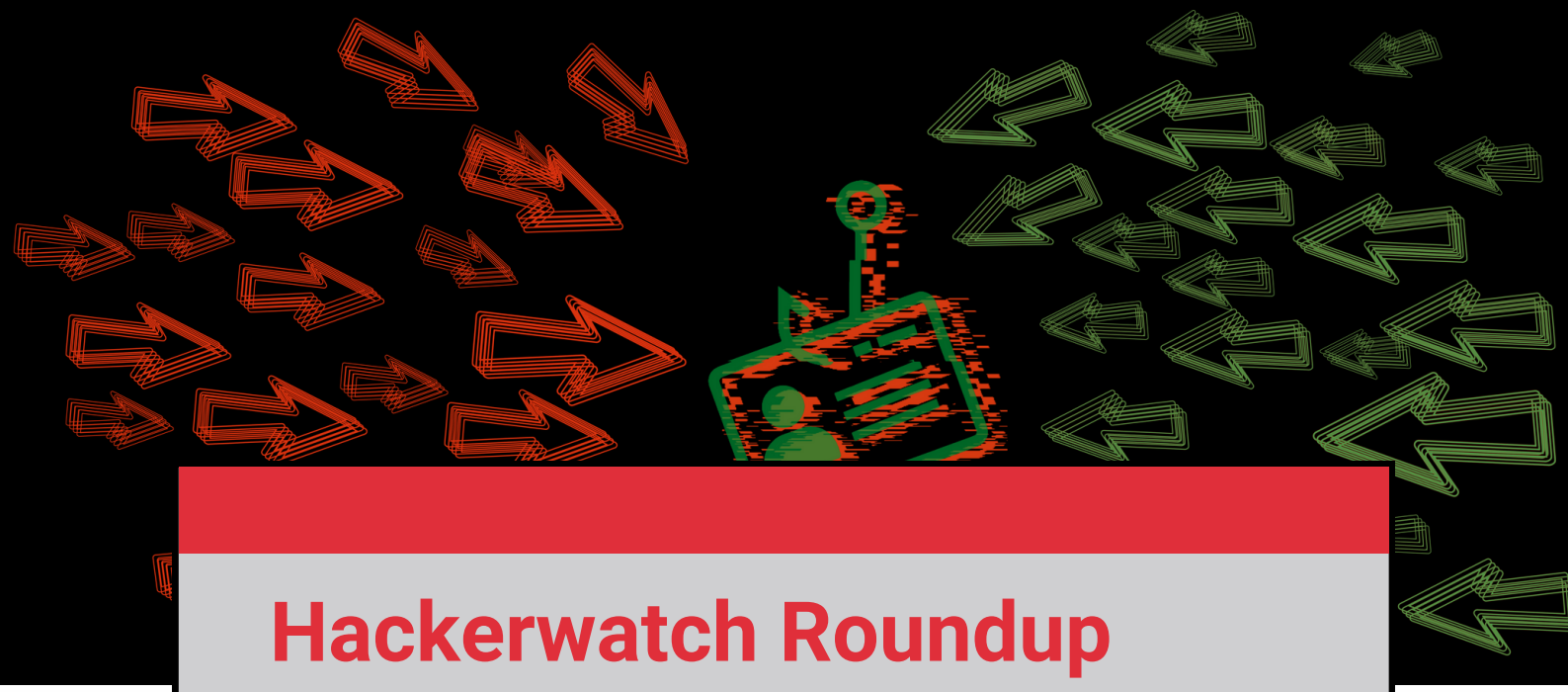


Hackerwatch Roundup

The Rising Wave Of Impersonation

Filterwatch

January - November 2023

Executive Summary

Miaan Group has documented multiple attacks on civil society groups inside and outside of Iran, which constitute the largest and most coordinated impersonation and phishing campaign since the outbreak of the Mahsa Jina Amini movement last year.

This report is the result of research and documentation of over 100 attacks that targeted journalists, civil society activists, and rights defenders of ethnic and religious minorities domestically and abroad in 2023. The focus of this report is on examining trends instead of individual cases. However, some examples of the attacks are provided to illustrate the trends and methods.

The attackers, who are believed to be sponsored by the Iranian government, have been impersonating U.S.-based think tanks, such as the Atlantic Council, that have been vocal in supporting Jina's movement and other pro-democracy causes in Iran. However, unlike the previous attacks that targeted mainly the think tanks themselves or their affiliates, the recent wave of attacks has expanded its scope and sophistication to target a wider and more diverse range of civil society actors, especially ethnic minorities, journalists, and human rights lawyers.

The attackers have been exploiting the lack of information and awareness among the target groups, as well as various crises in Iran, such as the mysterious suspected poisoning of hundreds of school girls earlier this year, to lure them into clicking on malicious links or opening infected attachments. The links and attachments are designed to harvest the targets' account credentials and personal data, and to compromise their devices and networks.

The attacks pose a serious threat to the security and privacy of the target groups, as well as to the integrity and credibility of the information and communication channels that they rely on. The attacks also reveal the increasing capabilities and ambitions of the Iranian government in conducting cyber operations against its perceived enemies, both domestically and internationally.

Key Findings

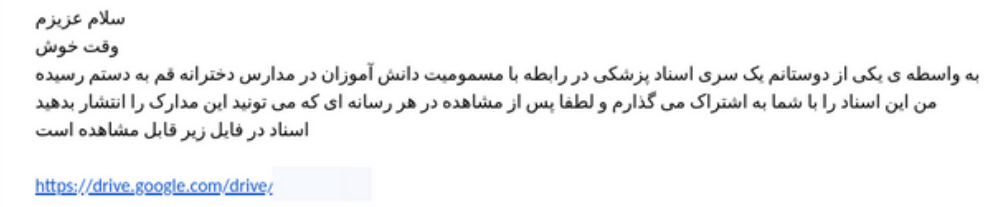
1. **The main target group of the attacks are individuals and organizations of ethnic minorities, such as Kurds and Turkish-Azerbaijanis. The attackers have been impersonating U.S.-based think tanks or NGOs that claim to support the rights and interests of these minorities, and offer them funding, training, or advocacy opportunities.**
2. **Journalists who are working on different angles of Jina's movement, such as the legal, social, or cultural aspects, are also targeted by the attackers.**
3. **Independent artists, art galleries and art spaces who were supporters of the "Woman, Life, Freedom" movement were among victims.**
4. **Lawyers who are trying to form a council to support protesters, detainees, and their families, who have been affected by the brutal crackdown of the Iranian government on Jina's movement and other dissenting voices, are also targeted by the attackers.**
5. **The attacks are not sophisticated on the technical side, as they rely on basic phishing techniques and tools, such as fake Google drive links or Microsoft Word documents. However, they are sophisticated on the social engineering side, as they use convincing and customized messages that appeal to the targets' emotions, needs, or curiosity.**
6. **The attacks show that the Iranian government has improved its open-source intelligence (OSINT) operation, as it is able to research and collect information about its targets, such as their names, affiliations, interests, or activities, and use this information to craft more effective and persuasive social engineering attacks.**
7. **The attacks are using legitimate Google infrastructure such as Google Site to design a phishing attack.**
8. **Account owners mostly had two-step authentication. Phishing was designed in such a way that the victim was asked to enter a two-step authentication code.**
9. **Social engineering tactics mainly focused on threatening users to close their accounts for violating the terms of the platforms, receiving blue ticks on social media, and requesting interviews for research.**

Incidents Analysis

This section provides a chronological overview and a detailed analysis of the incidents that have been documented, involving impersonation and phishing attacks on civil society groups inside and outside of Iran.

Targeting Journalist Working on Suspected Poisoning of School Girls

On this date, hackers believed to be sponsored by the Iranian government took advantage of the reports on the suspected poisoning of hundreds of school girls across the cities of Qom, Borujerd and Pardis since November 2022. This event was quite unique because no one had any credible information on how and why this happened. The Iranian authorities denied any responsibility and blamed foreign enemies or environmental and psychological factors.
The hackers started claiming to have documents and investigative reports on this event, and sent them to their targets via email, WhatsApp, Skype, or Telegram. The targets included journalists, Iran analysts, ethnic minority rights activists.
The following screenshot shows an example of an email sent to a victim, pretending to have information on gas attacks to girls schools.


سلام عزیزم
وقت خوش
به واسطه ی یکی از دوستانم یک سری اسناد پزشکی در رابطه با مسمومیت دانش آموزان در مدارس دخترانه قم به دستم رسیده
من این اسناد را با شما به اشتراک می گذارم و لطفا پس از مشاهده در هر رسانه ای که می توئید این مدارک را انتشار بدهید
اسناد در فایل زیر قابل مشاهده است

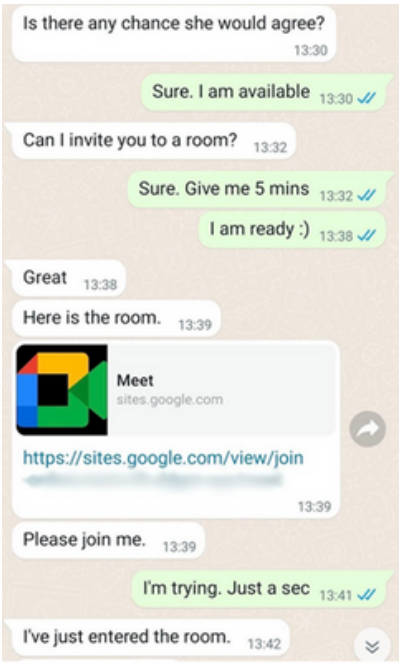
https://drive.google.com/drive/

Screenshot of email sent to a victim

The email contains an infected Google Drive link that is designed to compromise the victim's device and network.

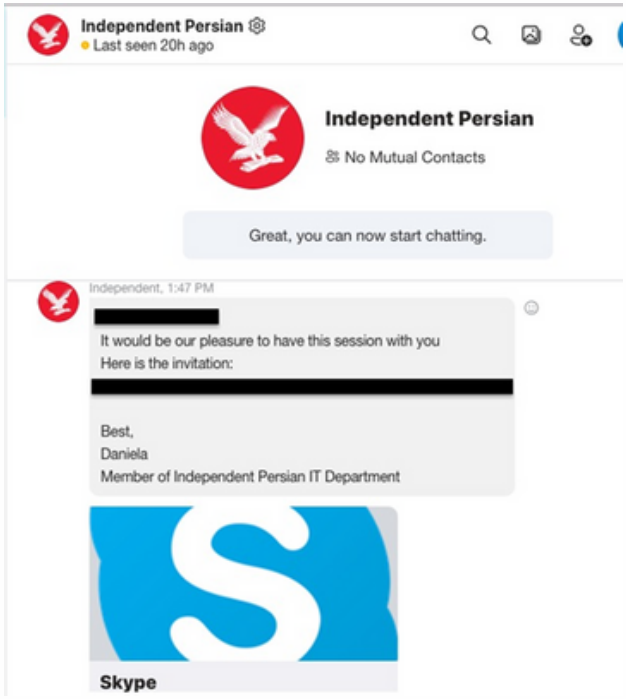
These kinds of messages were sent via various platforms, such as Gmail, WhatsApp, Skype or Telegram, depending on the preference and availability of the targets. The hackers used different techniques to persuade the targets to click on the links or open the attachments, such as appealing to their curiosity, urgency, or fear.

The following screenshot shows an example of a WhatsApp chat of an attacker tracking a victim to click on a link.



Screenshot of WhatsApp chat of attacker with a victim

We have seen the same kind of social engineering on March 1, June 13, and August 31, 2023, using different events and topics as bait, such as interviewing Iran analysts.



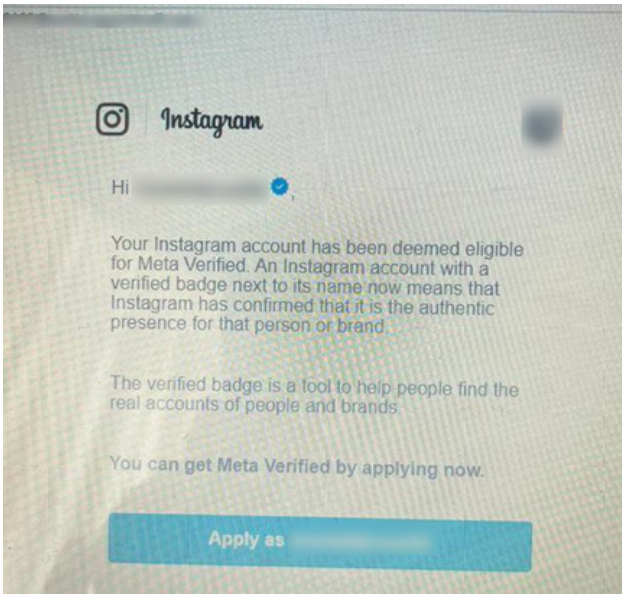
Screenshot of Skype chat of attacker tracking victim to click on a link

Targeting Artists And Art Spaces

In June 2023, an independent artist organization in Iran that supports the Women, Life, Freedom movement was targeted. The hackers compromised the credentials of their organization's social media accounts and some of their members' accounts.

This attack was interesting for two reasons:

1. **The hackers used a custom-made infrastructure to launch the phishing attack, which they had not done for a long time.**
2. **The hackers used an infrastructure in Japan for the first time. Previously,they mostly used cloud infrastructures in Germany or other European countries.**

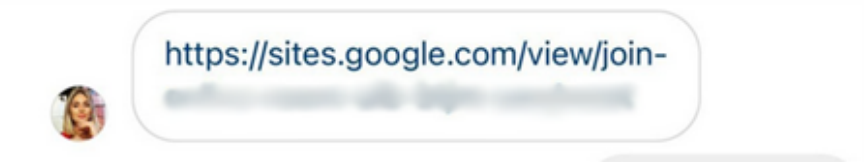


Screenshot of an email sent to an artist

The hackers used a common social engineering method in this attack. They sent an email to the victim, claiming that their Instagram account was eligible for a blue tick verification. They asked the victim to click on a link and enter their information to receive the verification.
We have identified over 100 domains linked to the same infrastructure targeting instagram users.

Targeting of Ethnic Minorities

In September 2023, we observed a shift in terms of targets and social engineering messages. Although the hackers still relied mainly on impersonation, their target group became ethnic minorities, such as Kurds and Turkish-Azerbaijanis. They pretended to beU.S.-based think tanks or NGOs that claimed to support the rights and interests of these minorities. They offered them funding, training, or advocacy opportunities.
One of the organizations that was targeted was a non-governmental organization that works to promote and protect the human rights of the Turkish-Azerbaijani people in Iran.



Screenshot of a phishing link

The attacker pretends to be a researcher of the International Institute for Strategic Studies (IISS), which is a prominent think tank on international security and strategy, based in London. The attacker claims to be working on a project related to the violation of human rights against Turkish ethnic minorities in the Middle East, and invites them to collaborate and share his insights. Based on Miaan Group's preliminary research, the victim's work email was also targeted.
This type of impersonation has been used more frequently than ever by the Iranian government since the September 2022 death in custody of Mahsa Jina Amini.

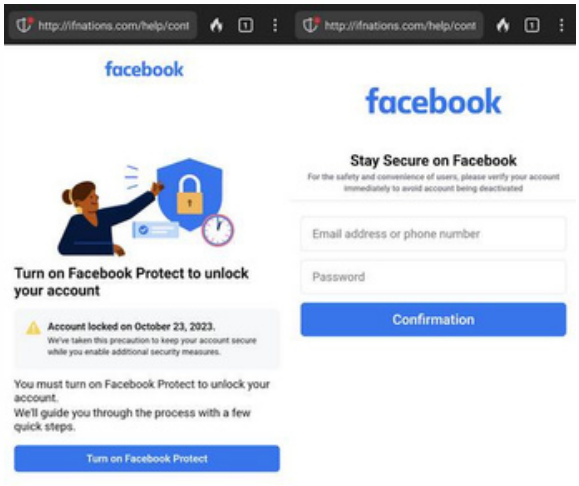
Targeting of Kurdish Activists

In October 2023, we observed another change in the social engineering impersonation messages used by the hackers, as they switched their target group from Turkish ethnic minorities to Kurdish activists and journalists. The Kurds are another oppressed and marginalized minority in Iran, who have been struggling for their cultural, political, and human rights for decades.

One of the individuals who was targeted was a prominent Kurdish human rights defender and the founder of an independent organization that monitors and documents the human rights violations against the Kurdish people in Iran.

The hackers used an old and well-known technique of impersonating Meta by sending direct messages to their Facebook page and to the personal accounts of the people who are directly or indirectly affiliated with the organization. The hackers claimed that the targets violated the terms of service of Meta, and threatened to disable their pages or accounts if they did not comply with their instructions.

The following screenshot shows a fake Facebook site behind a shortened URL that was used to impersonate the Facebook reporting system.



Screenshot of fake Facebook site behind shorten URL

The hackers used this fake site to lure the targets into providing their Facebook credentials and personal data.
The message contains a shortened URL that is designed to redirect the targets to a fake Meta login page, where they are asked to enter their credentials and personal data. The hackers used https://www.rebrandly.com/, which is a URL shortener service that hides the actual URL behind the shortened URL.
Based on our investigation, the hackers were using the same infrastructure that was used to attack the Turkish activists and their organization in September 2023. This suggests that the hackers are operating from a centralized command center, and that they have a list of potential targets that they update and prioritize according to their objectives and opportunities.

Targeting Journalists Working On Social, Women Rights, And Foreign Relations

So far, all the targets of these attacks were outside of Iran. However, in October 2023, we also saw similar attacks targeting journalists in Iran who are working on social, women rights, or foreign relations issues. These journalists played an important role in revealing the details of Mahsa Jina Amini's death.

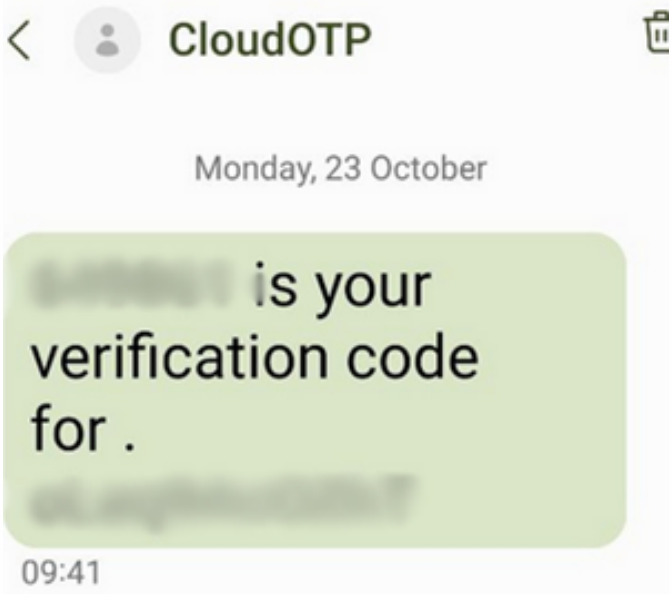
On October 19, 2023, a reporter's email account was hacked by a method unknown to us and linked to a mail client program. This program automatically downloads all the emails from the reporter's account, so we assume that the victim is exposed to the hacker (likely a security service).

That same day, another reporter was targeted on his Telegram account. The attackers were using the same IP address and device that were used to attack the previous reporter, suggesting that they were using the same infrastructure.

Following these attacks, the same IP address and devices were used to attack a third reporter.

Meanwhile, in addition to impersonating Meta and other platforms, the hackers also resorted to intercepting the text messages and 2-step verification codes of their targets based in Iran. This enabled them to bypass the security measures and gain access to their accounts and devices. The hackers used the government's infrastructure to attack them, as they have control over the telecommunications network and the internet service providers in Iran.

In October 2023, we observed another change in the social engineering impersonation messages used by the hackers, as they switched their target group from Turkish ethnic minorities to Kurdish activists and journalists. The Kurds are another oppressed and marginalized minority in Iran, who have been struggling for their cultural, political, and human rights for decades.



Screenshot of text messages sent without the request of the account owner

Recommendations

Based on the incidents and analysis presented in this report, we offer the following recommendations to enhance the digital security and resilience of the civil society groups, journalists, and other targets of the impersonation and phishing attacks by the Iranian government:

1. **More regular digital security training is needed for ethnic minorities organizations, as they are often the most vulnerable and under-resourced groups in terms of cyber awareness and protection. The training should cover the basics of phishing detection and prevention, such as verifying the sender, checking the URL, using strong passwords, enabling multi-factor authentication, and reporting suspicious messages or activities. Trainers might consider using https://shira.app/ as a learning platform.**
2. **Sending alerts in a more efficient way is a need, as the targets may not be aware of the latest threats or incidents that affect them or their peers. The alerts should be timely, accurate, and actionable, and should be delivered through multiple and secure channels, such as email, SMS, Telegram, Signal, WhatsApp, or even a push notification on mobile phones.**
3. **Access to the rapid response should be provided for wider community members, as they may need urgent and professional assistance or support in case of an attack or a breach.**
4. **Organizations need more regular digital security wellness checks.**
5. **Organizations need to have digital security policy guidelines and access to tools that can help them to implement those policies.**
6. **Specific training should be designed to combat social engineering, and those who may potentially be targeted should receive appropriate warnings and training before releasing public information about their lives, job and activism.**

Appendices:
Indicator of Compromise

- 164.132.136.54
- https://sites.googl[dot]com/view/join-online-room-[removed for security]
- https://sites.google[dot]com/view/join-online-room-[removed for security]
- https://rebrand[dot]ly/Meta-support-[removed for security]
- https://ifnations[dot]com/[removed for security]
- MetaSupportMail[dot]com
- 163.44.242.25
- Xn--MetaSpport-v43e[dot]com
- MetaSụpport[dot]com
- 163.44.242.16
- MetaeMailSecurity[dot]com
- MetaEmailSecurity[dot]net
- MetaSecurityEmail[dot]org
- MetaSupportMail[dot]co
- IGSecurity[dot]email
- Metahelpservice[dot]net