Iran Cyber Threat Intelligence Report

MIAAN GROUP

The Silent War Against Ethnic Minorities and Civil Society

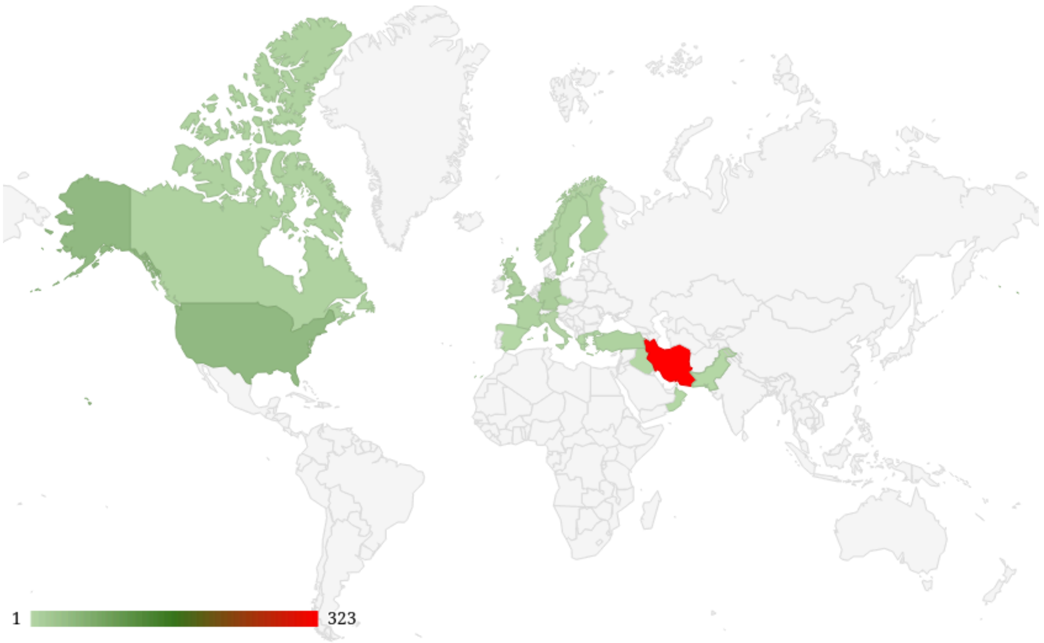
Second Half of 2024

Miaan
Digital Security
Help Desk

https://www.miaan.org
https://www.miaan.org/dsh
https://filter.watch

Executive Summary

This report examines the trends of cyberattacks, content management, digital rights violations, and patterns of arrests in the second half of 2024, based on data from the Digital Security Helpdesk (DSH) of the Miaan Group. The Islamic Republic of Iran's security agencies have escalated their cyber-repression efforts, employing more organized and sophisticated tactics against ethnic minorities, civil activists, and political dissidents. These measures aim to more effectively suppress dissenting voices through targeted content management, arrests, and the confiscation of electronic devices. These actions have significantly restricted freedom of expression and tightened state control over cyberspace.

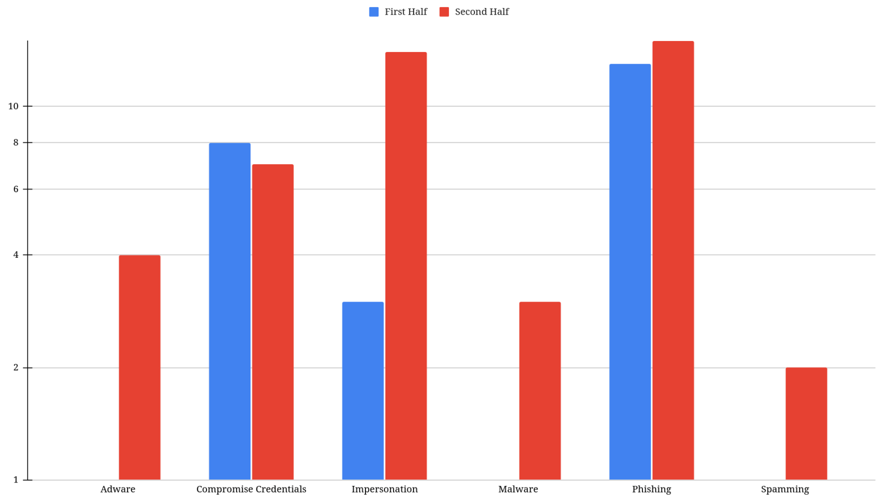


Geographical Distribution of Attacks Against Iranian Activists

Main Trends

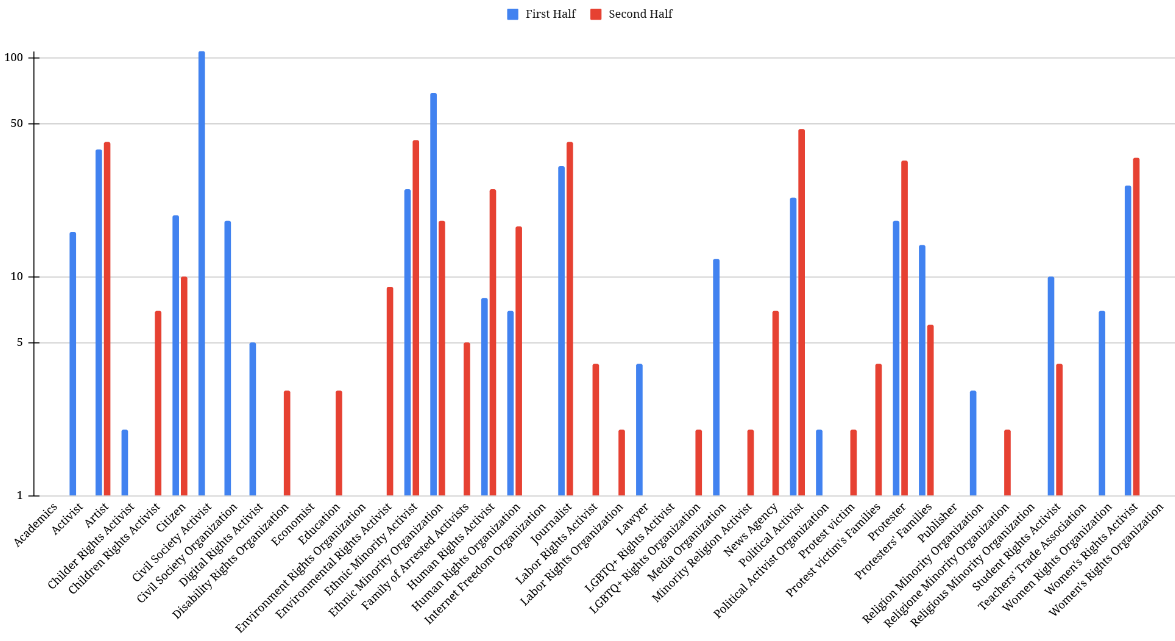
- **Targeted Cyberattacks**:
  - These attacks include account breaches, phishing, malware, and identity fraud. For the first time, we observed a case where Quishing (a type of phishing attack using QR codes) was utilized. This approach is more complex and harder for victims to identify compared to traditional phishing methods.
- **Targeted Content Management**:

    - Telegram groups were misused to appear as though they were distributing child exploitation content, a tactic aimed at inciting harassment against political and civil activists.
    - The removal of posts and accounts belonging to prominent activists occurred through mass reporting on social media platforms.
    - Journalists were pressured by having their SIM cards cut, forcing them to delete all their social media posts or shutting down accounts belonging to civil activists.
    - Fake content was spread to defame activists and disseminate misleading information in public spaces.
- **Arrests and Devices Confiscation**:
    - Activists were arrested under security pretenses, and their electronic devices, including laptops and smartphones, were confiscated. Our findings show that, during detention, the victim's phone is set to Airplane Mode to prevent any remote support or security for their accounts.
    - The confiscation of devices has become a tool for accessing activists' online accounts and personal information.
    - There has been an increase in restrictions on internet access and tools like VPNs, leading individuals to rely more on insecure tools.



Comparison of Cyberattacks in the First and Second Half of 2024

All of the aforementioned actions are part of the broader digital control and repression policy of the Islamic Republic, significantly affecting the digital rights, freedom of expression, and the personal security of civil activists and political dissidents both inside Iran and abroad.



Comparison of Requests in the First and Second Half

Findings and Patterns

1. **Targeting Ethnic Minorities**: 17.5% of all cases relate to cyberattacks on activists from the Baluchi, Kurdish, and Turkic communities.
    a. Regional Breakdown:
        i. Sistan and Baluchestan: Over 8% of cases.
        ii. Kurdistan: Over 7% of cases.
        iii. East and West Azerbaijan: Over 2% of cases.
    b. Types of Activities:
        i. Widespread arrests of cultural and political activists.
        ii. Publication of forced confessions and identity fraud in cyberspace.
        iii. Military and security forces deployed to suppress protests in high-conflict regions.
2. **Focus on Reference Groups**: Ethnic rights activists were the primary targets of cyberattacks, constituting 21.5% of all cases.
    a. Other targeted groups include:
        i. Political dissidents: 13%.
        ii. Participants in social, political, or economic protests: Around 10%.
        iii. Women's rights activists: Over 10%.
        iv. Artists: 11.25% of cases, especially from mid-July to early September 2024 (July and August).
3. **Attacks on Online Accounts**: 70% of all cases related to breaches of user account security. The primary reasons include:

   a. Arrests and devices confiscation.
   b. Increased pressure to limit access to the internet and tools like VPNs.
4. **Digital Repression of Iranian Activists Abroad**.
   a. Journalists from Persian-language media outlets outside Iran: Around 24%.
   b. Human rights and political activists: Close to 22%.
   c. Most targeted countries: United States, France, the United Kingdom, Sweden, and Turkey.

Repression of Iranian Ethnic Minorities: A Primary Target of Security Forces

Ethnic minorities were among the main targets of cyber repression by security agencies from May to December 2024. The geographical distribution map of cases referred to the Miaan DSH in Iran shows that 8% of all cases were related to Sistan and Baluchestan. Kurdistan accounted for more than 7%, and East and West Azerbaijan for over 2%.

During this period, Baluchi, Kurdish, and Turkic minorities represented 17.5% of all cases referred to the DSH. This statistic reflects the particular focus of the Iranian security forces on suppressing ethnic activists.

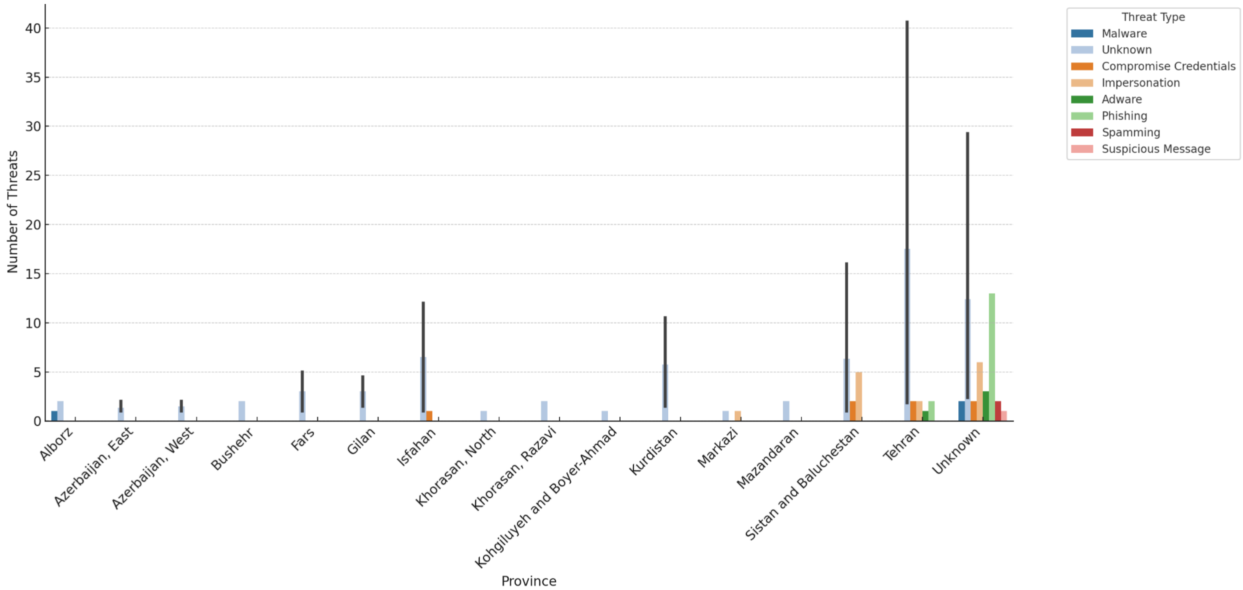
The findings of the DSH align with reports from human rights organizations regarding the intensifying repression in Sistan and Baluchestan, Kurdistan, East Azerbaijan, and West Azerbaijan.

During this period, the suppression of ethnic minorities in Iran by security and police forces, especially against Kurds, Baluchis, and Khuzestani Arabs, increased. Protests in areas with large populations of these ethnic groups were severely repressed, with widespread arrests, executions, and use of force by security forces.

Reports have emerged of executions and violent crackdowns by military forces aimed at suppressing protests in Sistan and Baluchestan. Similarly, widespread arrests of cultural and political activists have been reported in Kurdish regions. These actions are part of the broader systemic discrimination and repression against ethnic minorities in Iran, who often seek to uphold their cultural and political rights.

Cyber Threat Distribution Map

Data from the DSH reveals that over the past six months, while security agencies concentrated on cyber repression targeting ethnic minorities, civil activists in Tehran—home to universities, civil institutions, and political parties—accounted for 46.5% of the cases reported to the DSH.



The map of cyberattacks and threats categorized by provinces in the second half of the year

Civil activists in Isfahan, Gilan, Fars, Alborz, and Khorasan Razavi followed in the number of cases reported to the DSH. It is important to note that, to protect client privacy, we do not ask for their place of residence unless they choose to disclose it. As a result, many cases remain unidentified by province and are categorized as "Unknown."

Additionally, during the election period and around Labor Day, phishing and malware attacks specifically targeted groups boycotting the election and labor activists.

Targeted Groups of Cyberattacks by Security Forces

Among the groups targeted by cyberattacks or digital repression by security agencies, organizations working on ethnic rights and their activists are at the top of the list. In total, 21.5% of all cases during this period were related to this group.

After ethnic activists, political dissidents against the Islamic Republic accounted for the highest number of cyberattacks by security agencies, with more than 13% of the DSH cases. Participants in protests and rallies accounted for about 10% of the cases referred to the DSH.

One notable trend in the second half of 2024 is the increase in repression of artists. Compared to the first half of the year, the number of cases referred to the DSH from this social group has increased by 150%. In the second half of 2024, 11.25% of all cases examined were related to artists. In this period, reports of the widespread repression of artists in various cities of Iran were published in the media.

Women's rights activists were the next most targeted group, accounting for more than 10% of the reported cases of cyberattacks or repression to the DSH. In August 2024, Iranian security forces arrested 12 women's rights activists and one political activist in Gilan province. These pressures not only weakened the women's rights organizations and activists in Gilan but also created an atmosphere of fear and repression for other civil activists in the region.

Journalists, human rights activists, and other civil activists were also targeted by cyber pressures from security agencies during this period.

Online Accounts as the Primary Targets of Security Forces

Nearly 70% of reported security threats to the accounts of civil activists involve account breaches. The primary challenges include arrests, device confiscations, and the summoning of activists. Our data indicates a significant rise in the confiscation of activists' electronic devices by security agencies.

Between May and September 2024, the Islamic Republic of Iran applied considerable pressure on activists involved in internet access rights and VPN creators. This pressure increased with the introduction of new laws restricting access to these tools and heightened efforts to block them. The government has officially declared the use of VPNs—essential for bypassing censorship and accessing restricted information—illegal. As a result, citizen reliance on VPNs has grown, leading to a rise in requests for VPN support reported to the DSH.

Digital Security Threat Patterns for Iranian Activists Abroad

Examining the patterns of digital attacks on Iranians abroad reveals different results. While political activists, ethnic activists, artists, and human rights activists in Iran are targeted by security agencies, Persian-language media journalists abroad are the first targets.

Following them are human rights and political activists, who account for the highest number of attacks reported to the DSH. In the Iranian diaspora, political activists rank fourth in terms of the most targeted groups for cyberattacks by the Islamic Republic.

Among the civil activist groups abroad, ethnic activists, labor rights activists, and women's rights activists have had the least need for digital support.

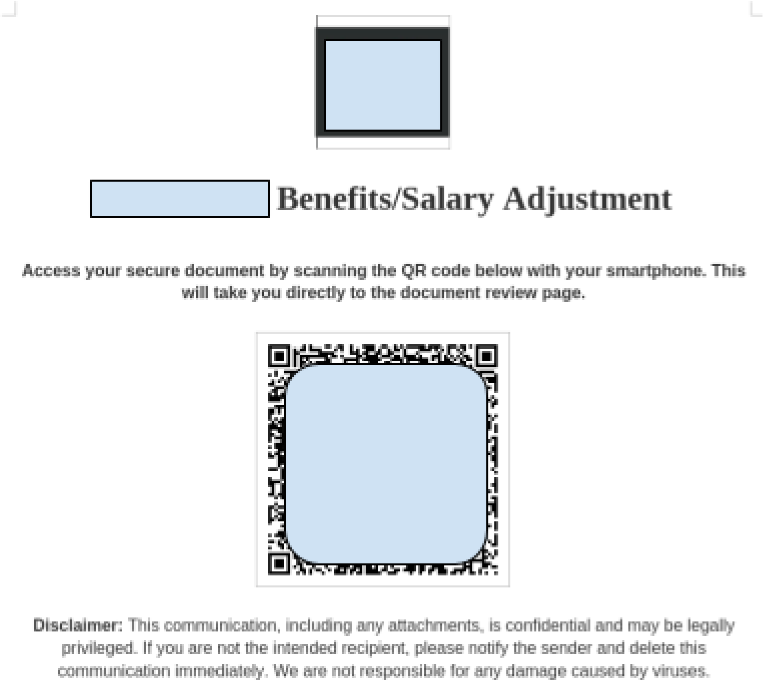
The distribution map of activists at risk abroad also shows that civil activists in the United States have the highest number of digital security breach reports. France, the UK, Sweden, and Turkey follow in ranking.

Types of Cyberattacks

The Iranian government uses different methods to digitally repress civil activists, including phishing attacks. In the six-month period from May to December 2024, 17 cases of phishing attacks were reported to the DSH. Activists have been repeatedly targeted with this method, and Miaan Group has published several reports on the goals and methods of hackers. In the past six months, phishing methods have become more diverse, making them increasingly difficult for users to detect.

Examining a Phishing Attack Case

In one example, the attackers, claiming to collaborate with the victim in a reputable human rights organization, sent an email containing a text file and requested the victim to read it. The attachment contained a QR code, and once scanned by the victim, it redirected them to several deceptive websites, eventually taking them to a phishing link.



[redacted]

[redacted] Benefits/Salary Adjustment

Access your secure document by scanning the QR code below with your smartphone. This will take you directly to the document review page.

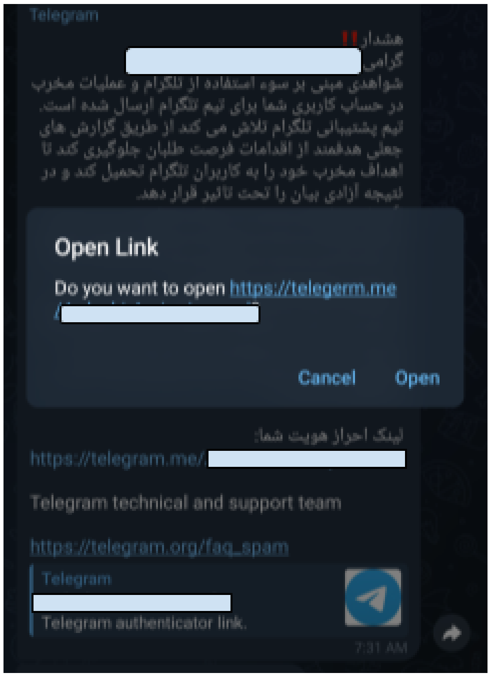
[redacted]

Disclaimer: This communication, including any attachments, is confidential and may be legally privileged. If you are not the intended recipient, please notify the sender and delete this communication immediately. We are not responsible for any damage caused by viruses.

Our digital threat laboratory findings show that the infrastructure of this attack was designed in a way that the attacker could instantly switch from a phishing link to downloading malicious files, such as malware. This method allows attackers to change their attack strategy with minimal time and resources.

Using Messaging Platforms for Phishing Attacks

As before, Telegram was one of the platforms used by hackers to send phishing links. However, the Iranian government's repressive methods have recently targeted civil activists with new techniques. In this new method, rather than placing the original link in the social engineering message, phishing links were hidden behind HTML codes. Although this is still phishing, the change in technique makes it harder to identify the link, especially on mobile devices.



Telegram

هشدار !!
[redacted] گرامی
شواهدی مبنی بر سوء استفاده از تلگرام و عملیات مخرب
در حساب کاربری شما برای تیم تلگرام ارسال شده است.
تیم پشتیبانی تلگرام تلاش می کند از طریق گزارش های
جعلی هدفمند از اقدامات فرصت طلبان جلوگیری کند تا
اهداف مخرب خود را به کاربران تلگرام تحمیل کند و در
نتیجه آزادی بیان را تحت تاثیر قرار دهد.

Open Link

Do you want to open https://telegerm.me/[redacted]

لینک احراز هویت شما:
https://telegram.me/[redacted]

Telegram technical and support team

https://telegram.org/faq_spam

Telegram
[redacted]
Telegram authenticator link.

7:31 AM

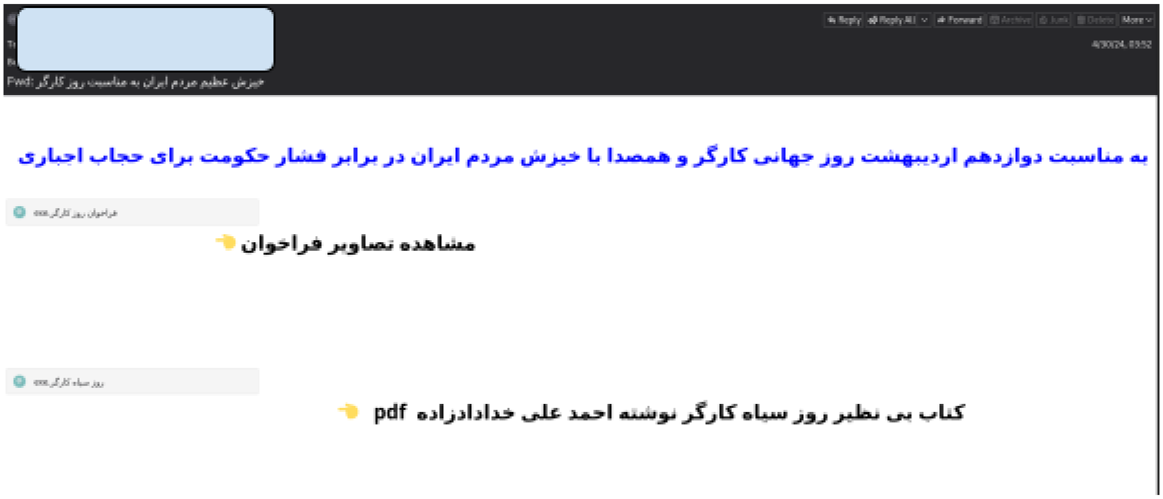
Identity Fraud: A Common Tactic of Iranian Security Forces

Identity fraud is a prerequisite for phishing attacks, and it is one of the ways hackers gain the trust of their victims. As previously mentioned, in many cases, hackers impersonate human rights organizations or tech companies to achieve their goals. However, identity fraud is not limited to these cases; in some instances, hackers also impersonate well-known individuals.

According to the data from the DSH, several human rights activists were attacked in the past six months using identity fraud. For instance, one of the members of a prominent human rights organization received an email from someone claiming to be a member of Human Rights Watch. The attacker claimed to be reaching out based on the recipient's background in reporting human rights violations in Iran, wishing to use their experience.

Examining a Cyberattack Case Using Malware

Labor activists received an email titled "Mass Uprising of the People of Iran for Labor Day," claiming that it contained two PDF files with statements, photos, and documents showing evidence of widespread labor protests.


[redacted]

4/30/24, 03:52

Fwd: خیزش عظیم مردم ایران به مناسبت روز کارگر

به مناسبت دوازدهم اردیبهشت روز جهانی کارگر و همصدا با خیزش مردم ایران در برابر فشار حکومت برای حجاب اجباری

فراخوان روز کارگر.exe

👈 مشاهده تصاویر فراخوان

روز سیاه کارگر.exe

👈 کتاب بی نظیر روز سیاه کارگر نوشته احمد علی خدادادزاده pdf

Image of the email sent to labor activists

Our investigations reveal that these two files were executable files for the Windows operating system. When executed, the first file named Labor Day Call.exe displayed an image in JPG format to the user. It then disabled Windows Defender in the Windows registry and attempted to connect to a command and control server. This malware establishes communication with a specific server and sends information from the victim's computer to that server. The information is encrypted or obfuscated to prevent detection.

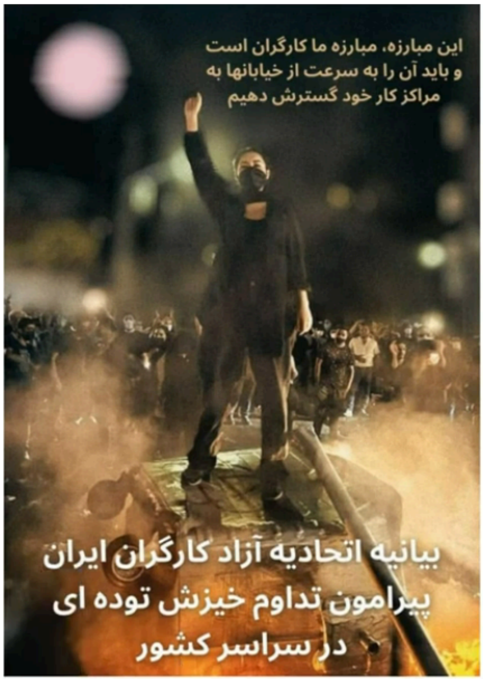

این مبارزه، مبارزه ما کارگران است
و باید آن را به سرعت از خیابانها به
مراکز کار خود گسترش دهیم
بیانیه اتحادیه آزاد کارگران ایران
پیرامون تداوم خیزش توده ای
در سراسر کشور

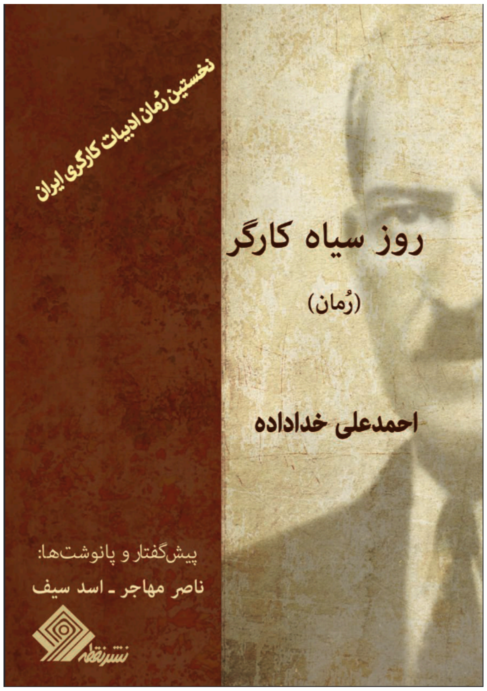
Image shown to the user after executing Labor Day Call.exe

This malware attempts to gather specific information from the victim's system and send it to a foreign server. The following communications demonstrate the malware's actions:

- Information Gathering: The malware collects data such as device IDs, encryption keys or hashes, and encrypted data from the user's system.
- Sending Information to the Server: The information is sent in the form of an HTTP POST request to a server located at IP address 188.212.125.119.

This malware operates like a "spyware" on the victim's system. It extracts important or specific information from the user's system and sends it to the attacker's server. The attacker can then use this information for various purposes, such as data theft or system control.

The second file, named Black Labor Day.exe, creates a PDF file called Black Labor Day.pdf on the user's device after being executed. This PDF is actually a novel about workers, and it automatically opens the document, performing similar actions to the first file.



نخستین رُمان ادبیات کارگری ایران

روز سیاه کارگر

(رُمان)

احمدعلی خداداده

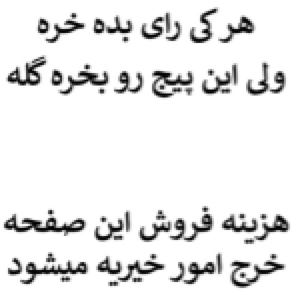
پیش‌گفتار و پانوشت‌ها:
ناصر مهاجر ـ اسد سیف

نشر نقطه

The Black Labor Day.pdf file created on the victim's device.

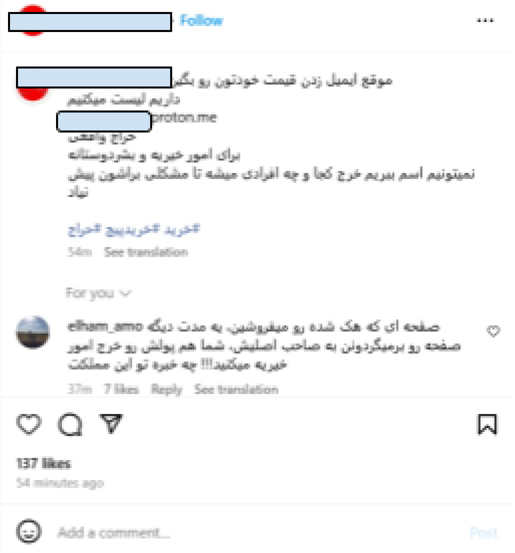
Examining an Account Breach Case

In other cases where hacking operations were fully executed, false information or financial requests were typically involved. In one instance, the Instagram account of a long-established reformist newspaper was hacked. The attackers used the account to demand money while simultaneously posting their own opinions until the payment was made.



هر کی رای بده خره
ولی این پیج رو بخره گله

هزینه فروش این صفحه
خرج امور خیریه میشود



[redacted] Follow ···

[redacted] موقع ایمیل زدن قیمت خودتون رو بگ
داریم لیست میکنیم
[redacted]proton.me
حراج واقعی
برای امور خیریه و بشردوستانه
نمیتونیم اسم ببریم خرج کجا و چه افرادی میشه تا مشکلی براشون پیش نیاد

#خرید #خریدپیج #حراج
54m See translation

For you

elham_amo صفحه ای که هک شده رو میفروشین به مدت دیگه صفحه رو برمیگردونن به صاحب اصلیش. شما هم پولش رو خرج امور خیریه میکنید!!! چه خبره تو این مملکت
37m 7 likes Reply See translation

137 likes
54 minutes ago

Add a comment... Post

Examples of Content Management Attacks

Beyond cyberattacks aimed at hijacking activists' accounts, there is evidence of efforts by Iranian security forces to manage online content. These campaigns aim to obscure or hide activists in cyberspace. Other goals include removing unwanted content for the Islamic Republic, generating fake news, harassing activists, and producing illegal content.

Attempts to Remove Unwanted Content

We have received reports of efforts by the Iranian government's cyber campaigns to remove content produced by prominent activists on social media between May and December 2024. In this method, posts or accounts are reported by large numbers of government-controlled accounts under false pretenses, such as "inciting violence" or "spreading false information."

Online Harassment

Reports of publishing private information, death threats, and encouragement to commit suicide were some of the types of online harassment reported during this period. This method seeks to create fear and discourage activists from participating in cyberspace or to alter their stance against the Islamic Republic.

Publishing Illegal Content

The spread of illegal content aims to discredit the online space and discourage users from participating. For instance, a network of Telegram channels is currently active, producing and distributing illegal content such as child sexual abuse videos and rape, while organizing campaigns to attack political activists and promote the official policies of the Islamic Republic. These channels use sophisticated methods to distribute criminal content, making it difficult for Telegram to identify them through conventional methods.

Indicators of Compromised

File Names:

Labor Day Call.exe
SHA256: 9d3b64bcdd14dcde1c3d293f0d152ae02a34320263f0728888c0b0848352f551
Black Labor Day.exe
SHA256: 576afbcd6760b127e98c423a1d2724ee9b784c3a0f9806d362908b908038d1ed
Black Labor Day.pdf
SHA256: 32764d097333f97ec47ccad89717b39fb244893260c38cdcf78617ba8fda1935

IP Addresses:

188.212.125.119

104.194.133.9
194.32.78.252
194.87.45.14
45.150.67.44
45.95.233.246
185.151.30.210
104.21.33.151
45.11.180.139
104.21.82.79
31.214.157.201
162.159.140.104

Links:

https://votecontestantin.3umailer[dot]space
https://telegerm[dot]me/ArdeshirAmirarjomand
https://help.manager-x-safe[dot]com
http://ir.fvhbj[dot]com
https://support-t[dot]me/login

Attacker email addresses:

mayur.korat[at]proexelancers.com
meifong_hrw[at]yahoo.com
she_anderson[at]yahoo.com
karen.s_brown[at]yahoo.com
catrionapeters[at]myyahoo.com