positive
technologies

Iran's cybersecurity threatscape for 2021-2024

ptsecurity.com

2024

Content

About this report

Iran's rapid digital transformation, aimed at ensuring the nation's digital sovereignty, is happening against a backdrop of sustained global cyberthreats, the need for substituting imported digital platforms and services, and efforts to create functional hardware and software solutions to ensure the cyber-resilience of the infrastructure.

The Iranian state is implementing measures to ensure that the entire information infrastructure remains cyber-resilient, regardless of where the threats originate. These measures are comprehensive in nature, allowing Iran to implement a sovereign information policy that leverages the national information network, digitalize its public services, and develop its own national digital platforms and services. On this journey, Iran benefits from its own unique experience and close ties with friendly nations.

This report examines the cybersecurity posture of Iran, considering the country's unique geopolitical circumstances and, to some extent, comparing it to other Middle Eastern nations.

The following are the objectives of this report:

- Assess the cybersecurity threatscape for 2021–H1 2024.
- Highlight the region's distinctive cyberthreat trends.
- Provide recommendations for improving cybersecurity for governments, businesses, and individuals.

This report contains data on current information security threats in Iran, drawing on insights from Positive Technologies, dark web intelligence, and trusted third-party sources.

The study seeks to engage Iranian organizations and individuals with an interest in the current state of cybersecurity by highlighting the latest cyberattack tactics and motives. It also aims to identify key trends in the changing cybersecurity threatscape.

This report treats each mass attack, such as a phishing campaign, as one incident rather than several. The terms used in this report are explained in the Positive Technologies glossary.

Overview of Iran's cybersecurity threatscape

The state is forced to operate on three cyberfronts simultaneously: countering cyberattacks from foreign state-sponsored APT groups, neutralizing hacktivist activities aimed at destabilizing the domestic situation, and combating financially motivated cybercriminals.

APT groups consist of highly skilled hackers who carry out multi-stage, meticulously planned cyberattacks targeting specific companies, industries, or groups of industries. Their goal is to obtain confidential information relevant to the political, economic, or military sectors, and to damage the critical infrastructure in certain countries. APT groups primarily target organizations, though occasionally certain categories of individuals are also attacked. They combine social engineering methods with an extensive arsenal of malware. The predominant form of attack is cyberespionage. APT groups such as APT15, Bahamut, Molerats, and Desert Falcons operated in the region during the period of 2021–H1 2024.

APT15 (known variously as Playful Taurus, BackdoorDiplomacy, Vixen Panda, KeChang, NICKEL) is believed to be Chinese in origin. Its key targets include government organizations, embassies, and sectors of the economy in various countries. APT15 is known to have first targeted Iran in early 2023 with a cyber-espionage campaign against the Iranian government conducted between July and December 2022.

The Bahamut APT group operates mainly in South Asia and the Middle East, where it provides attack-for-hire services, among other things. The group specializes in cyber-espionage, employing fake applications and spear-phishing campaigns to achieve its goals. Parts of the group's arsenal have been developed in-house. The group also contributes to malicious apps for Android and iOS devices, spreading the malware through Google Play and the App Store.

The APT groups Molerats (known variously as Gaza Hackers, TA402, and Extreme Jackal) and Desert Falcons (APT-C-23) frequently target the government, military, media, and energy sector. Desert Falcons' activities also impact the transportation industry and scientific and educational organizations, while Molerats focus on the manufacturing sector. Some researchers consider Desert Falcons a group of cyber-mercenaries conducting cyber-espionage campaigns in the Middle East. Researchers say that Molerats' cyberattacks often exploit geopolitical and military themes to lure users into opening Microsoft Office attachments or clicking malicious links. Both groups possess their own malware arsenals while also using popular remote access tools.

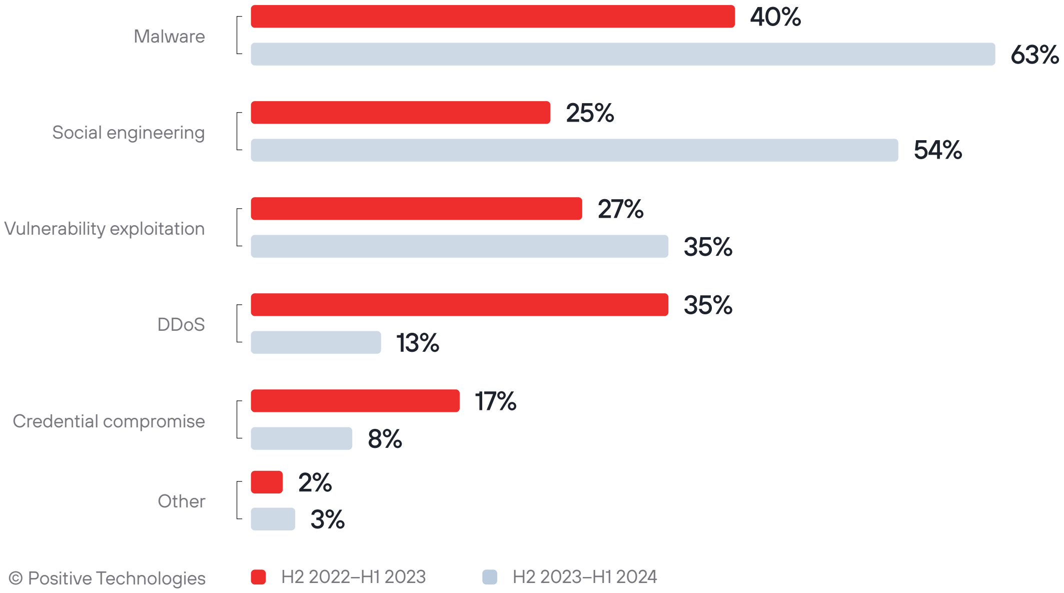
According to publicly available sources, some of the hacktivist groups operating in Iran are Black Reward, Tapandegan, Edalat-e Ali, GhostSec, Ghyamsarnegouni, Gonjeshke Darande, and WeRedEvils.

When analyzing the cybersecurity threatscape, we looked at two combined periods: from 2021 to 2022 and from 2023 to the first half of 2024. The trends in successful cyberattacks show that attackers targeted organizations more frequently (71% in both periods) than individuals (29% in both periods).

Dark web data also reveals a clear bias towards cyberattacks on organizations: 94% of advertisements in 2023–2024 targeted organizations, while only 6% were directed at individuals. This is likely because the motivation behind many dark web listings is financial gain, while organizations are more likely to pay up to recover their operational assets.

Malware remains the primary method of executing cyberattacks against both organizations and individuals across the Middle East.

Figure 1. Cyberattacks in the Middle East by method, H2 2022–H1 2023 and H2 2023–H1 2024

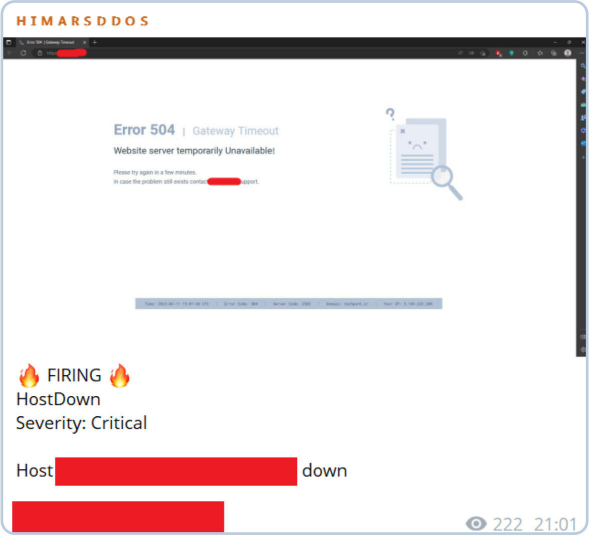


© Positive Technologies

Over the past year, there has been an increase in the percentage of social engineering attacks (by 29 percentage points) and vulnerability exploitation (by 8 percentage points).

The decline in DDoS attacks is likely due to the rise in cybercrime and financially motivated hacktivism. Stealing or encrypting data is profitable, unlike knocking a website or infrastructure component offline.

Figure 2. Screenshot of a dark web listing with the results of the DDoS attack on one of Iranian IT innovation park



HIMARSDDOS

Error 504 | Gateway Timeout

Website server temporarily Unavailable!

Please try again in a few minutes.
In case the problem still exists contact [redacted]upport.

Time: 2023-02-11 15:01:30 UTC | Error Code: 504 | Server Code: 2582 | Domain: techpark.ir | Your IP: 5.189.223.209

🔥 FIRING 🔥
HostDown
Severity: Critical

Host [redacted] down

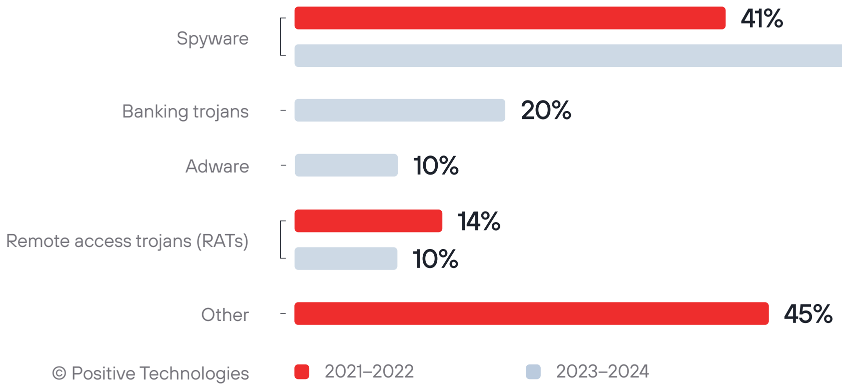
[redacted]

222 21:01

In 2023–H1 2024, a slight increase in the use of legitimate software in cyberattacks in Iran was observed. For example, in 2023, attackers infected a 20SpeedVPN installer with the EyeSpy malware, which itself included components from SecondEye, a legitimate parental control and monitoring app. In the same year, the Iranian hacktivist group Black Reward hacked the financial app 780 App, normally used for digital transactions, to send out anti-government messages.

Spyware was the prevalent type of malware in Iran throughout the observation period, increasing by 19% between 2023 and 2024 compared to 2021–2022. Banking trojans also saw an increase, reaching 20%.

Figure 3. Cyberattacks on organizations and individuals by malware category



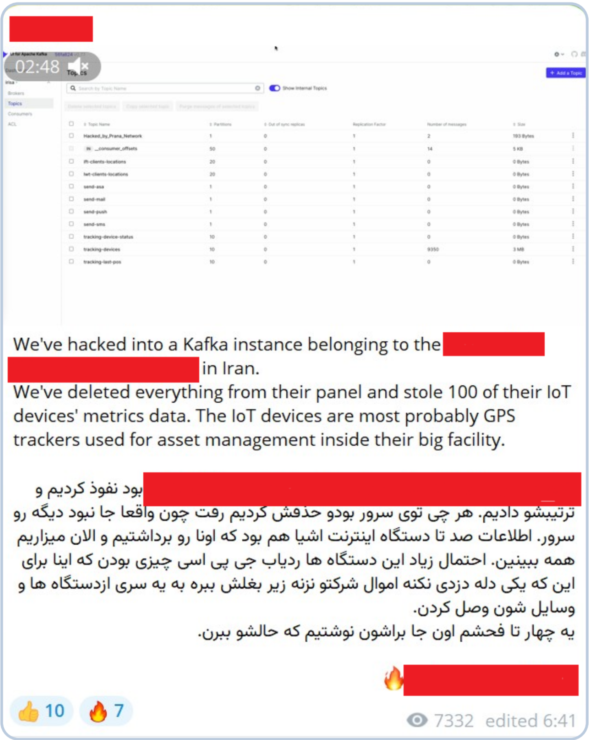
© Positive Technologies

In 2024, threat intelligence researchers at the PT Expert Security Center identified Dridex banking trojan activity as part of their threat intelligence, this malware is capable of hiding its presence on infected devices. These devices are integrated into a modular botnet, where malicious features can be added via modules or libraries. Dridex can inject code without triggering suspicious API calls to evade monitoring systems. The malware is distributed in archived format through Discord's CDN. Two files are extracted from the archive, one of which is the legitimate Oleview.exe, while the other is a DLL containing malware. The DLL is designed to be injected into the legitimate executable's process. The malicious DLL uses the LoadLibrary function to load two programs with hard-coded names, self.exe and testapp.exe, while it is running.

A region-specific feature is the use of wipers by attackers. Wipers delete user and system files, which can make hardware inoperable. The greatest danger arises when a wiper infects ICS devices and industrial systems equipped with IoT devices. Over the past year, the share of wiper use throughout the Middle East has increased from 3% to 8%, so it is expected that attackers in Iran are also use them in cyberattacks.

In February 2024, the hacker group GhostSec posted on the dark web claiming responsibility for a cyberattack on an Iranian steel foundry. The attackers claimed to have stolen 100 IoT device metrics and deleted all the data from the control panels. The nature of this cyberattack, provided it indeed occurred, suggests both exploitation of vulnerabilities in IoT devices and the use of a wiper.

Figure 4. Screenshot of a Telegram post regarding a cyberattack on Iranian steel foundry



[redacted]

	Topic Name	Partitions	Out of sync replicas	Replication Factor	Number of messages	Size
□	Hacked_by_Prana_Network	1	0	1	2	193 Bytes
□	IN __consumer_offsets	50	0	1	14	5 KB
□	ift-clients-locations	20	0	1	0	0 Bytes
□	lwt-clients-locations	20	0	1	0	0 Bytes
□	send-asa	1	0	1	0	0 Bytes
□	send-mail	1	0	1	0	0 Bytes
□	send-push	1	0	1	0	0 Bytes
□	send-sms	1	0	1	0	0 Bytes
□	tracking-device-status	10	0	1	0	0 Bytes
□	tracking-devices	10	0	1	9350	3 MB
□	tracking-last-pos	10	0	1	0	0 Bytes

We've hacked into a Kafka instance belonging to the [redacted] in Iran.
We've deleted everything from their panel and stole 100 of their IoT devices' metrics data. The IoT devices are most probably GPS trackers used for asset management inside their big facility.

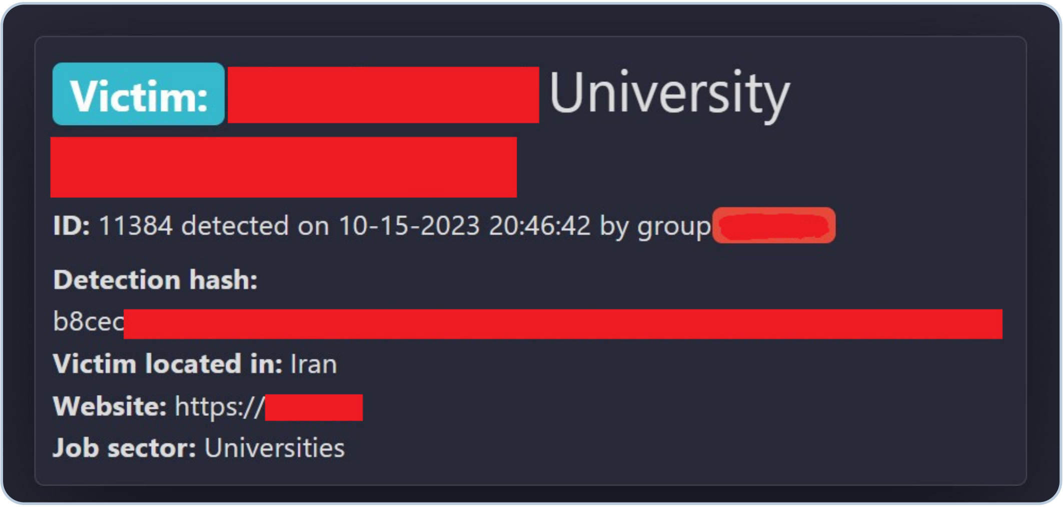
[redacted] بود نفوذ کردیم و
ترتیبشو دادیم. هر چی توی سرور بودو حذفش کردیم رفت چون واقعا جا نبود دیگه رو
سرور. اطلاعات صد تا دستگاه اینترنت اشیا هم بود که اونا رو برداشتیم و الان میزاریم
همه ببینین. احتمال زیاد این دستگاه ها ردیاب جی پی اسی چیزی بودن که اینا برای
این که یکی دله دزدی نکنه اموال شرکتو نزنه زیر بغلش ببره به یه سری ازدستگاه ها و
وسایل شون وصل کردن.
یه چهار تا فحشم اون جا براشون نوشتیم که حالشو ببرن.

🔥 [redacted]

👍 10 🔥 7 7332 edited 6:41

The increased cybercriminal activity in the region has been characterized by a rise in ransomware attacks. Victims have included a manufacturing company, an online university, and a digital currency exchange platform.

Figure 5. Screenshot of a dark web listing offering ransomware to target an online university



Victim: [redacted] University

[redacted]

ID: 11384 detected on 10-15-2023 20:46:42 by group [redacted]

Detection hash:

b8cec[redacted]

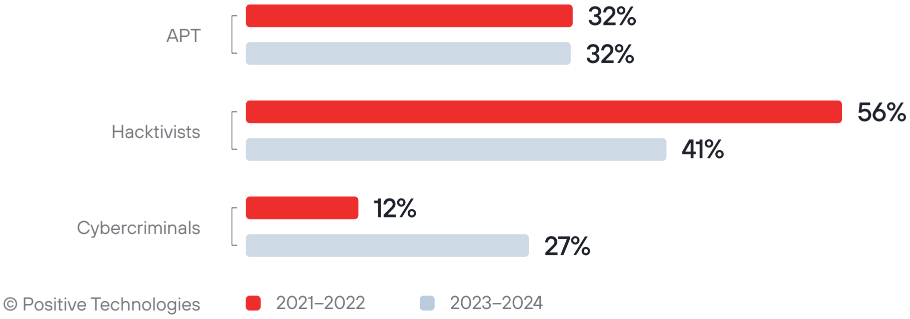
Victim located in: Iran

Website: https://[redacted]

Job sector: Universities

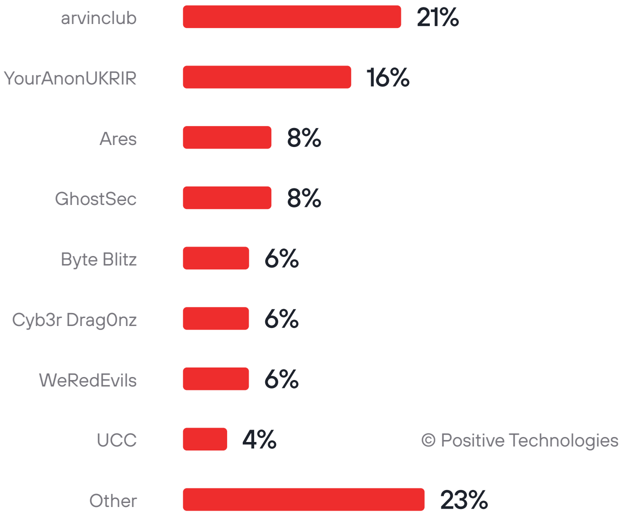
Despite a 15% drop in 2023–2024, hacktivist cyberattacks dominated in Iran in both periods under review.

Figure 6. Cyberattacks in Iran by actor type, 2021–2022 and 2023–H1 2024



Hacktivists operating in Iran primarily target government organizations: 42% and 40% of hacktivist cyberattacks were aimed at state institutions during the respective periods. The predominant methods include DDoS attacks on websites and defaces. Hacktivists typically use the dark web to post announcements. According to Positive Technologies insights that draw from an analysis of dark web platforms, the majority of dark web announcements in Iran come from the hacktivist group Arvin Club (21%), the group YourAnonUKRIR (16%), the financially motivated Ares group, and the hacktivists GhostSec (8% each). Arvin Club and YourAnonUKRIR seem to be posting on the dark web as part of a PR campaign to demonstrate their cyber-capabilities. GhostSec, which has been running double-extortion ransomware attacks using its own ransomware-as-a-service model, is tapping the dark web for financial gain.

Figure 7. Hacktivists and cybercriminals that posted most Iran-related dark web announcements in 2023–2024

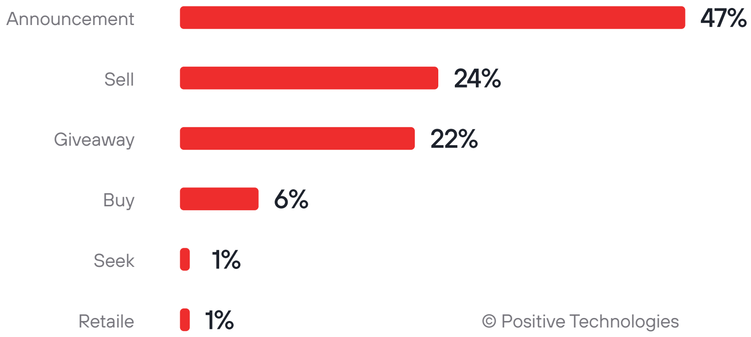


Arvin Club, which positions itself as an opposition hacktivist group, relies heavily on ransomware. In 2021, the group carried out cyberattacks on an Iranian bank and an educational messenger. The group frequently posts announcements on the dark web, all these falling in the Ransomware category.

The hacktivist groups Gonjeshke Darande (Predatory Sparrow) and WeRedEvils have similarly displayed political motivations. Gonjeshke Darande's cyberattacks targeted industrial facilities (steel plants in Iran and a chemical plant), Iran's rail infrastructure, gas stations, and one of Iran's ministries. WeRedEvils has conducted multiple cyberattacks on manufacturing and telecommunications infrastructure, including hacking into the project management system of Iran's oil infrastructure.

Statistics collected from shadow platforms indicate that during 2023–H1 2024, almost half (47%) of all cases saw cybercriminals announce breaches of various organizations. In 24% of cases, they offered stolen data (databases and access to organizations' infrastructure) for money, and in 22%, they offered these for free.

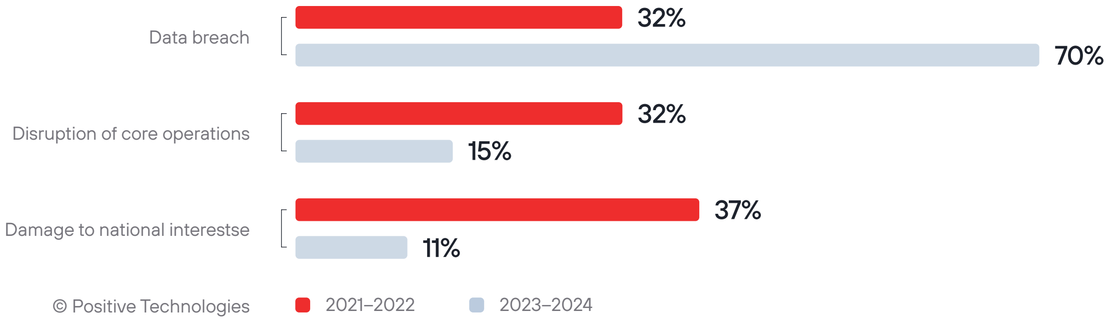
Figure 8. Dark web posts by type, 2023–2024



© Positive Technologies

The increase in data breaches, from 32% to 70%, in 2023–2024 is linked to the intensified activity of cybercriminals looking to monetize stolen data.

Figure 9. Cyberattacks in Iran by consequence, 2021–2022 and 2023–H1 2024



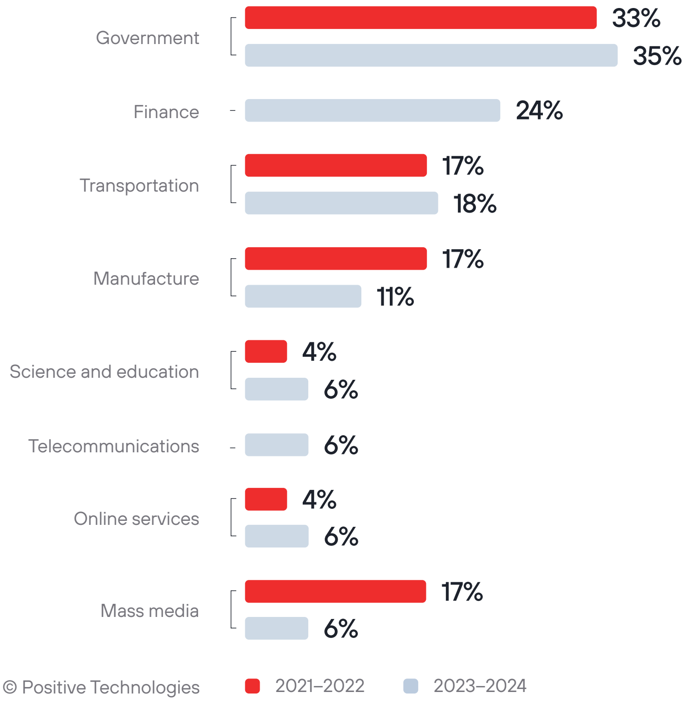
© Positive Technologies

Cyberattacks on organizations

Cybersecurity threatscape for organizations

Government institutions were the type of organizations most frequently attacked during both periods under review. In 2021–2022, they accounted for 33% of cyberattacks, a figure that rose to 35% in 2023–2024. We have seen a significant increase in cyberattacks on financial institutions. Similarly, there has been a rise in attacks on the telecoms sector (up 6%), science and education, and online services (the latter two 4% to 6% each).

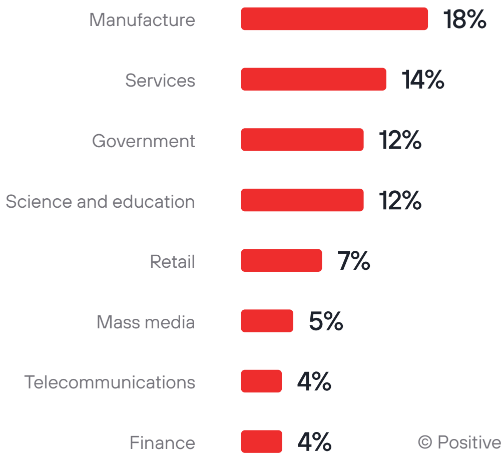
Figure 10. Cyberthreat trends by target sector, 2021–2022 and 2023–H1 2024



© Positive Technologies

Dark web statistics suggest that manufacturing companies dominate the categories of organizations successfully attacked in 2023–2024 with 18%. They were followed by services sector organizations (14%), government institutions (12%), and research centers and schools (12%).

Figure 11. Cyberthreat targets by category according to dark web data, 2023–H1 2024



© Positive Technologies

The difference in most targeted categories between dark web and public data could be due to dark web sellers being primarily motivated by profit. All these categories store large volumes of confidential information, which cybercriminals can sell at a profit. In the case of manufacturers, cybercriminals can similarly monetize access to infrastructure.

Government institutions

Cyberattacks on Iranian government institutions during the period under review were mainly carried out by hacktivists and APT groups. The main consequences of those attacks were disruptions to core operations and data breaches. Among the hacktivist groups attacking government institutions, disrupting their operations, and publishing compromised data are Black Reward, Edalat-e Ali, Tapandegan, Ghyamsarnegouni, and KromSec.

For example, Black Reward threatened to release documents related to Tehran's nuclear program. Edalat-e Ali attacks government facilities and publishes anti-government messages, classified information, and videos. The Ghyamsarnegouni hacktivists targeted Iran's broadcasting service and some government organizations.

The hacktivist group KromSec participated in several high-profile cyberattacks, including selling the database of some Iran's ministry on the dark web.

A DDoS hacktivist attack, presumably by Anonymous, knocked out the websites of an Iranian bank, the national government portal, and several state media outlets. A cyberattack on the Iranian municipality allegedly resulted in hacking around 5,000 traffic monitoring cameras.

Data related to the defense activities was breached in 2024 during a cyberattack on an Iranian company. The hacker group PRANA Network claimed responsibility for hacking company's email servers and gaining access to a database containing information about the company's financial infrastructure, fleet, oil sales operations, regasification processes, and key officers.

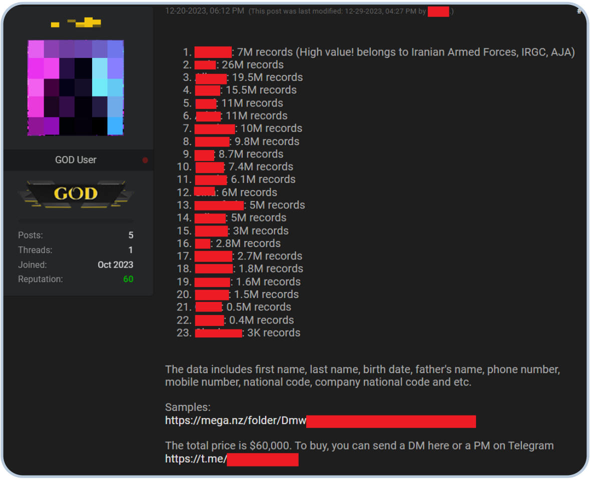
Non-tolerable events in the public sector can have devastating consequences for citizens, destabilizing society and the economy, creating political tensions, and undermining trust in government online services. These incidents can drive citizens away from government digital services, increasing administration costs.

Finance

Iranian financial organizations were attacked in 24% of cases between 2023 and 2024, with most attackers primarily motivated by financial gain. Non-tolerable events for banks, insurance and investment companies, and cryptocurrency exchanges, can cause huge financial losses and drive away customers. It is critical for these institutions to have strong cybersecurity measures in place.

An attack on Iran's insurance companies can serve as an example of cyberattacks on its financial organizations. On December 20, 2023, a hacker known as "irleaks" posted on the dark web offering to sell more than 160 million records from 23 of the country's leading insurance companies. A sample of the data, discovered by Hudson Rock, included passport numbers and other sensitive information. Hudson Rock researchers confirmed that the data appeared to be genuine and noted that attacking such a large number of insurance companies was extremely difficult.

Figure 12. Screenshot of a dark web listing offering data from insurance companies and their clients



Posts: 5
Threads: 1
Joined: Oct 2023
Reputation: 60

12-20-2023, 06:12 PM (This post was last modified: 12-29-2023, 04:27 PM by [redacted].)

1. [redacted]: 7M records (High value! belongs to Iranian Armed Forces, IRGC, AJA)
2. [redacted]: 26M records
3. [redacted]: 19.5M records
4. [redacted]: 15.5M records
5. [redacted]: 11M records
6. [redacted]: 11M records
7. [redacted]: 10M records
8. [redacted]: 9.8M records
9. [redacted]: 8.7M records
10. [redacted]: 7.4M records
11. [redacted]: 6.1M records
12. [redacted]: 6M records
13. [redacted]: 5M records
14. [redacted]: 5M records
15. [redacted]: 3M records
16. [redacted]: 2.8M records
17. [redacted]: 2.7M records
18. [redacted]: 1.8M records
19. [redacted]: 1.6M records
20. [redacted]: 1.5M records
21. [redacted]: 0.5M records
22. [redacted]: 0.4M records
23. [redacted]: 3K records

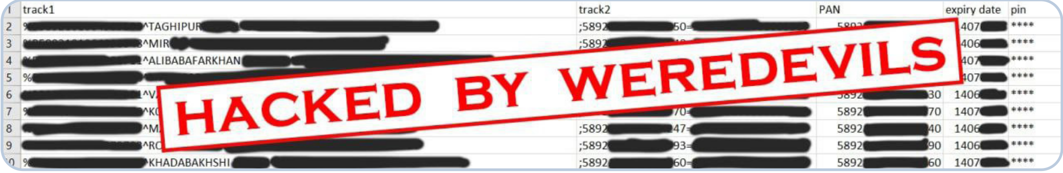
The data includes first name, last name, birth date, father's name, phone number, mobile number, national code, company national code and etc.

Samples:
https://mega.nz/folder/Dmw[redacted]

The total price is $60,000. To buy, you can send a DM here or a PM on Telegram
https://t.me/[redacted]

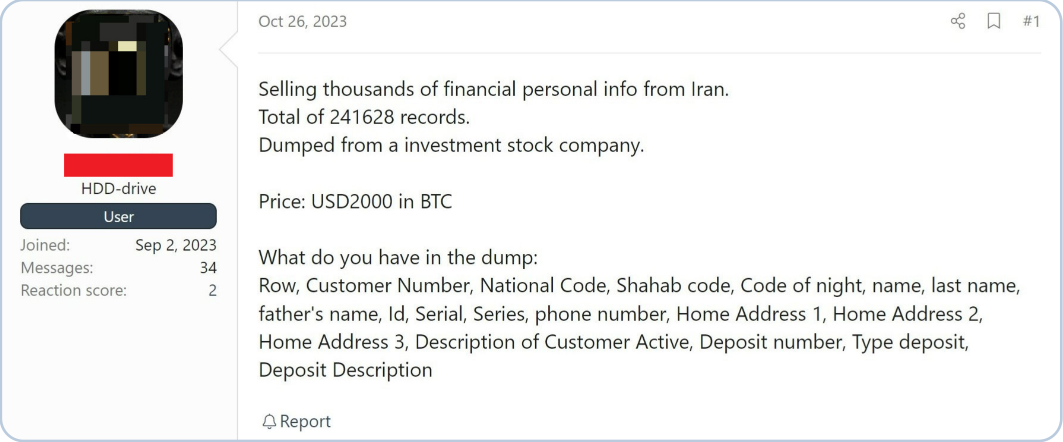
The hacker group WeRedEvils posted on their Telegram channel about hacking an Iranian bank, claiming they had stolen personal and payment data of the bank's clients, including credit card numbers and PINs.

Figure 13. Screenshots of announcements about the hack of an Iranian bank



1	track1	track2	PAN	expiry date	pin
2	%[redacted]^TAGHIPUR[redacted]	;5892[redacted]60=[redacted]	589[illegible]	1407[redacted]	****
3	[redacted]3^MIR[redacted]	;5892[redacted]	[illegible]	1406[redacted]	****
4	[redacted]^ALIBABAFARKHAN[redacted]	[illegible]	[illegible]	1407[redacted]	****
5	%[redacted]	[illegible]	[illegible]	1407[redacted]	****
6	[redacted]^V[illegible]	[illegible]	5892[redacted]30	1406[redacted]	****
7	%[redacted]^K[illegible]	[illegible]70=[redacted]	5892[redacted]70	1407[redacted]	****
8	[redacted]^M[illegible]	;5892[redacted]47=[redacted]	5892[redacted]40	1406[redacted]	****
9	[redacted]^R[illegible]	;5892[redacted]93=[redacted]	5892[redacted]90	1406[redacted]	****
10	%[redacted]KHADABAKHSHI[redacted]	;5892[redacted]60=[redacted]	5892[redacted]60	1407[redacted]	****

Figure 14. Example of an advertisement selling financial data of an Iranian investment company's clients



[redacted]
HDD-drive

Joined: Sep 2, 2023
Messages: 34
Reaction score: 2

Oct 26, 2023

Selling thousands of financial personal info from Iran.
Total of 241628 records.
Dumped from a investment stock company.

Price: USD2000 in BTC

What do you have in the dump:
Row, Customer Number, National Code, Shahab code, Code of night, name, last name, father's name, Id, Serial, Series, phone number, Home Address 1, Home Address 2, Home Address 3, Description of Customer Active, Deposit number, Type deposit, Deposit Description

A 2023 espionage campaign targeting banks and discovered by researchers at Sophos X-Ops continued later that year. Cybercriminals attacked several Iranian banks. This latest iteration was designed to target an expanded list of banks. However, the functionality of the new malware variant could potentially have implications for individuals as well. The malware harvested information about applications installed on the user's device, specifically looking for several cryptocurrency wallet applications. Researchers believe that these cryptocurrency wallets may be targeted soon.

We must mention here a large-scale cyberattack that occurred outside the period under review, on August 14, 2024, affecting 20 of the 29 active credit institutions in Iran.

The attackers managed to gain access to a vast amount of confidential data from individual client accounts.

Manufacture

Cyberattacks on manufacturers disrupted technological processes and provided attackers with access to internal control systems, as well as employee and operational data.

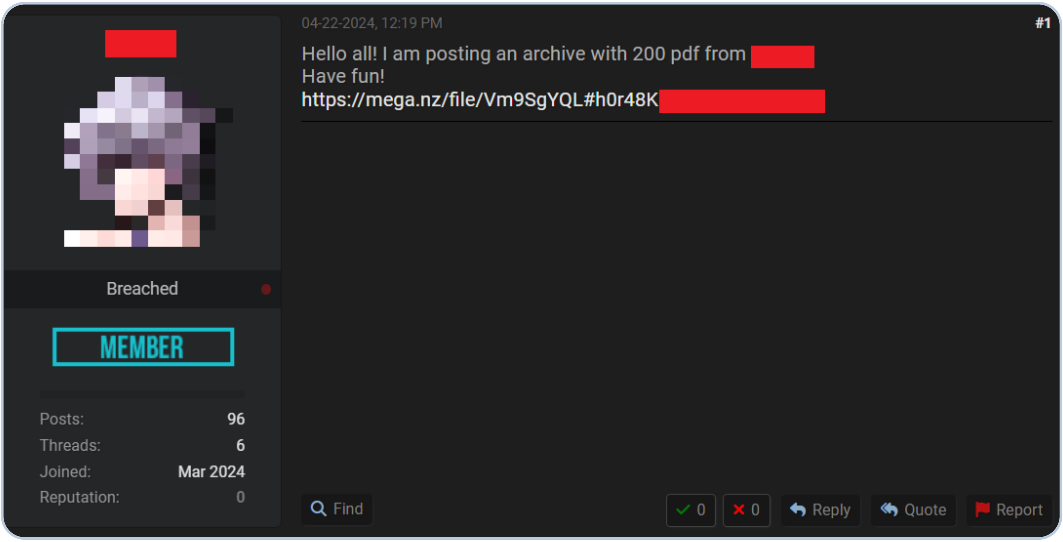
In 2022, a cyberattack damaged the industrial infrastructure of several Iranian companies. The attackers deployed Kali Linux, which targets operational technology platforms. They exploited vulnerabilities using Metasploit and conducted a Modbus attack on programmable logic controllers.

The hacker groups GhostSec and Gonjeshke Darande (Predatory Sparrow, presumably of Israeli origin) frequently attacked Iran's industrial infrastructure. In 2022, a cyberattack by Gonjeshke Darande disrupted operations at three steel companies. At one of the foundries, the attackers managed to cause a ladle of molten iron to collapse, setting the shop floor on fire.

Another hacker group in 2023 hacked the project management system of Iran's oil infrastructure. In April 2024, GhostSec attacked a manufacturer of electrical panels, gaining access to its SCADA system.

The hacktivist group ArvinClub posted on the dark web, claiming to have obtained data from 20,000 breached email accounts of an Iranian petrochemical corporation. Some of the listings that can be found on dark web offer data stolen form industrial companies, such as an engineering firm and an energy company, for sale or for free.

Figure 15. Screenshot of a dark web post about the leak of 200 PDF files from an energy company



[redacted]

Breached

MEMBER

Posts: 96
Threads: 6
Joined: Mar 2024
Reputation: 0

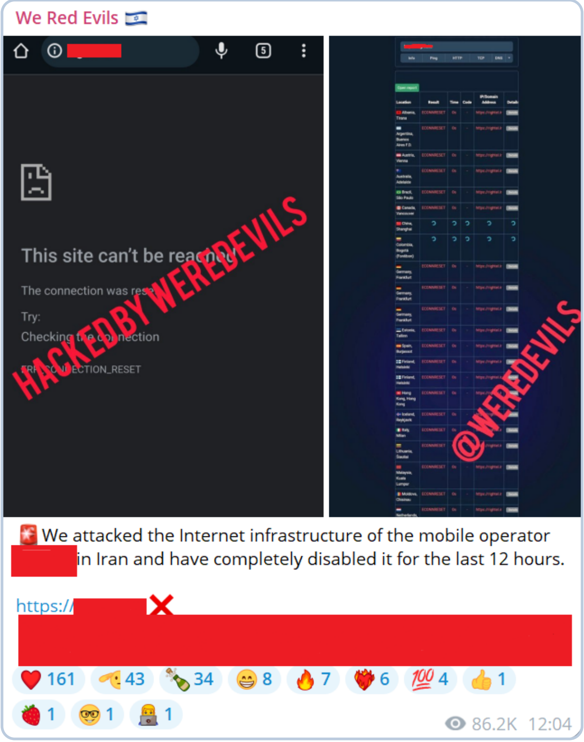
04-22-2024, 12:19 PM #1

Hello all! I am posting an archive with 200 pdf from [redacted]
Have fun!
https://mega.nz/file/Vm9SgYQL#h0r48K[redacted]

Telecommunications

Iran's telecommunications infrastructure has also suffered from hacktivist activities. In 2023, cybercriminals attacked the Iranian mobile operator, forcing it to suspend operations for 12 hours. The group also managed to breach Iran's telecommunications infrastructure, causing significant Internet service disruptions across the country.

Figure 16. Screenshot of a cyberattack on a mobile operator



We Red Evils 🇮🇱

[redacted]

This site can't be reached

The connection was reset

Try:
Checking the connection

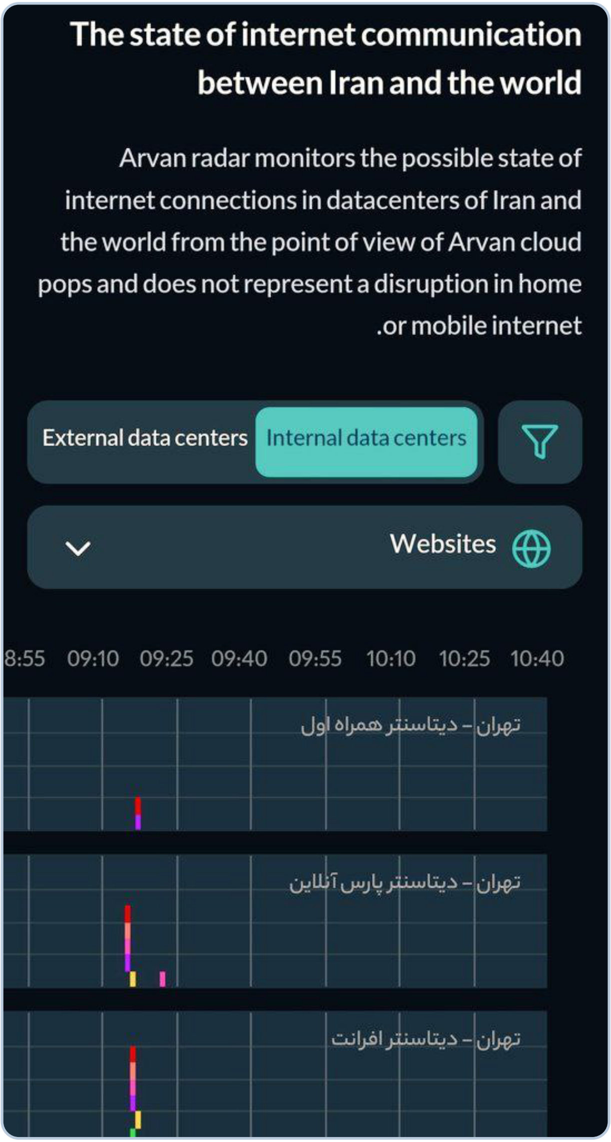
ERR_CONNECTION_RESET

🚨 We attacked the Internet infrastructure of the mobile operator [redacted] in Iran and have completely disabled it for the last 12 hours.

https://[redacted] ❌

[redacted]

Figure 17. Screenshot of a cyberattack on the telecoms infrastructure

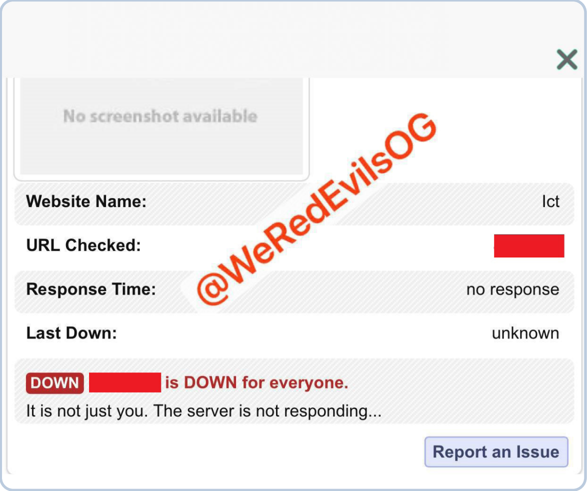


The state of internet communication between Iran and the world

Arvan radar monitors the possible state of internet connections in datacenters of Iran and the world from the point of view of Arvan cloud pops and does not represent a disruption in home .or mobile internet

In 2024one of Iranian ministries fell victim to a cyberattack, which caused its websites either go down or return a 403 error. According to the hacktivists, they managed to obtain confidential data, which they handed over to the Israeli government.

Figure 18. Dark web screenshot of the hacked site of an Iranian ministry



No screenshot available

@WeRedEvilsOG

Website Name: Ict

URL Checked: [redacted]

Response Time: no response

Last Down: unknown

DOWN [redacted] is DOWN for everyone.

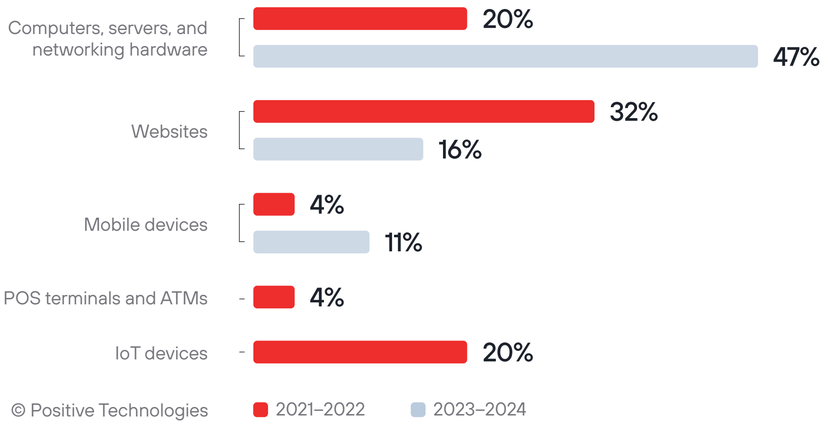
It is not just you. The server is not responding...

The cybersecurity of the telecommunications sector demands particular attention, as non-tolerable events within such systems can lead to disruptions in Internet service at a national level.

Cyberattack targets in organizations

In 2023–H1 2024, the vector of cyberattacks shifted toward workstations, servers, and networking hardware (47%).

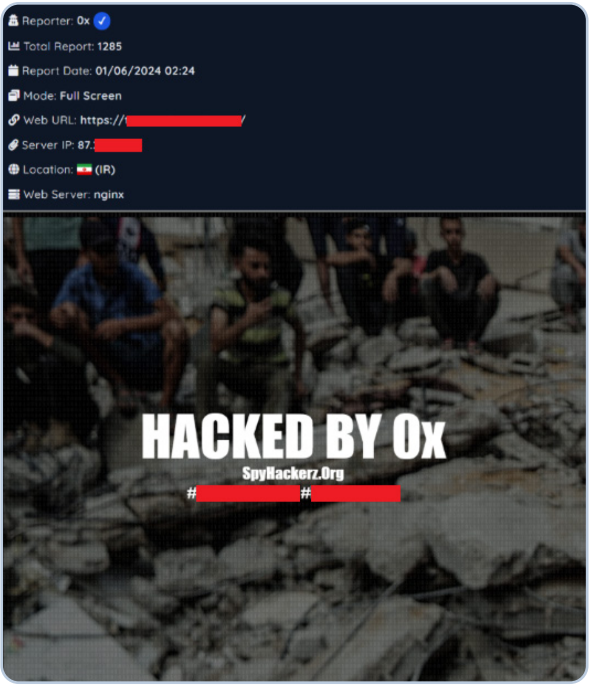
Figure 19. Cyberattacks on organizations by target asset type, 2021–2022 and 2023–H1 2024



© Positive Technologies

During 2021–2022, websites primarily experienced denial-of-service attacks and the exploitation of web server vulnerabilities, enabling attackers to replace legitimate content on compromised websites with their own (deface).

Figure 20. Example of a defacement of an Iranian website



Reporter: 0x ✓

Total Report: 1285

Report Date: 01/06/2024 02:24

Mode: Full Screen

Web URL: https://[redacted]/

Server IP: 87.[redacted]

Location: (IR)

Web Server: nginx

HACKED BY 0x

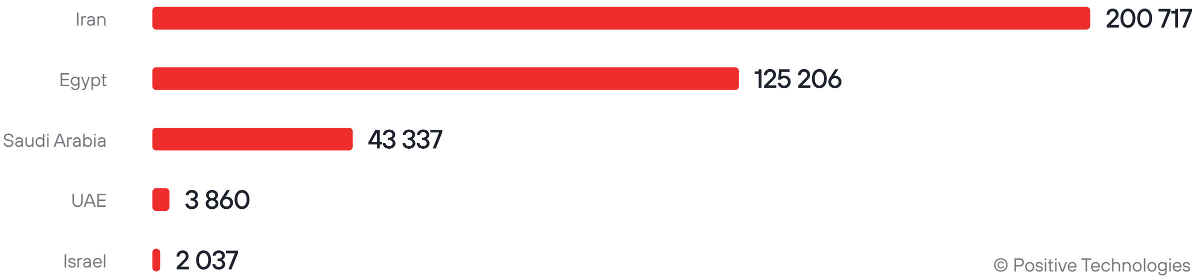
SpyHackerz.Org

#[redacted] #[redacted]

In 2021, the hacktivist group Gonjeshke Darande knocked out the website, ticket offices, and freight services of Iran's rail network.

Cyberattacks on IoT devices are common throughout the Middle East. Iran ranks first by number of IoT devices in the region.

Figure 21. Number of IoT devices among leading countries in the Middle East



© Positive Technologies

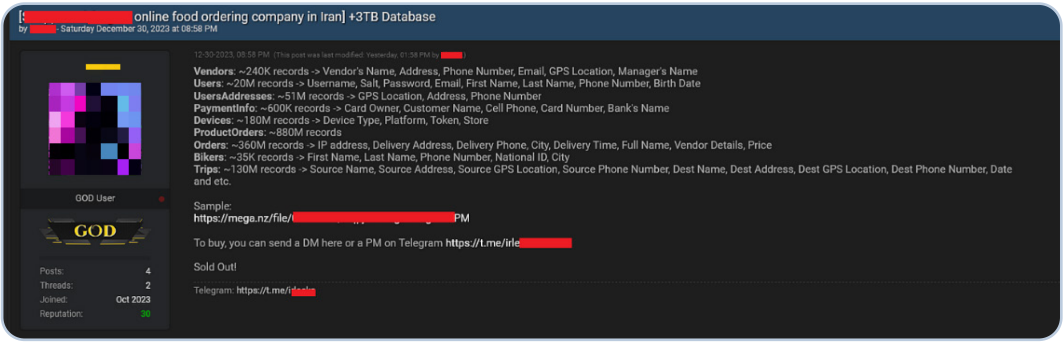
The substantial number of successful cyberattacks on manufacturers (17% and 11% for the respective periods) is presumably due to the widespread use of IoT devices in industrial infrastructure, which often turn out to be poorly protected weak links.

Methods of cyberattacks on organizations

The most common method of cyberattacks in Iran (63%) involves the use of malware, which is also the most frequent method for organizations, accounting for 36% of total attacks. In December 2021, researchers at Amnpardaz discovered the iLOBleed rootkit hidden in the firmware of HP iLO devices. It was used in real attacks to knock out the servers of various Iranian organizations.

In late 2023, a massive cyberattack targeted the online food delivery company. Hudson Rock researchers discovered that a company employee's computer had been infected with the StealC stealer, which presumably resulted in many of the company's confidential credentials being exposed to the hackers and used as the initial vector for the attack. On December 30, a three-terabyte dataset of user data was put up for sale on the cybercrime market. It included email addresses, passwords, phone numbers, physical addresses, and credit card details.

Figure 22. Screenshot of a dark web listing for online food ordering company customer data



[[redacted] online food ordering company in Iran] +3TB Database
by [redacted] - Saturday December 30, 2023 at 08:58 PM

12-30-2023, 08:58 PM (This post was last modified: Yesterday, 01:58 PM by [redacted])

Vendors: ~240K records -> Vendor's Name, Address, Phone Number, Email, GPS Location, Manager's Name
Users: ~20M records -> Username, Salt, Password, Email, First Name, Last Name, Phone Number, Birth Date
UsersAddresses: ~51M records -> GPS Location, Address, Phone Number
PaymentInfo: ~600K records -> Card Owner, Customer Name, Cell Phone, Card Number, Bank's Name
Devices: ~180M records -> Device Type, Platform, Token, Store
ProductOrders: ~880M records
Orders: ~360M records -> IP address, Delivery Address, Delivery Phone, City, Delivery Time, Full Name, Vendor Details, Price
Bikers: ~35K records -> First Name, Last Name, Phone Number, National ID, City
Trips: ~130M records -> Source Name, Source Address, Source GPS Location, Source Phone Number, Dest Name, Dest Address, Dest GPS Location, Dest Phone Number, Date
and etc.

Sample:
https://mega.nz/file/[redacted]PM

To buy, you can send a DM here or a PM on Telegram https://t.me/irle[redacted]

Sold Out!

Telegram: https://t.me/i[redacted]

In June 2024, threat intelligence experts at the PT Expert Security Center found that the Agent Tesla stealer was being used in Iran. This malware is available as a service, allowing cybercriminals to rent or buy it for attacks. Agent Tesla functions as a keylogger, captures screenshots, and collects information from browsers, email clients, and FTP servers.

In 2024, during an incident response effort, the PT Expert Security Center team discovered an unknown keylogger embedded in a customer's main Microsoft Exchange Server page. It was harvesting account credentials into a file accessible via a special path from the Internet. An ensuing investigation revealed over 30 victims, mostly government entities in African and Middle Eastern countries. All the victims have been notified of the breach.

Windows devices in Iran have been heavily targeted by attackers using RATs. In 2024, two such malware tools, Millenium RAT and Xeno RAT, were found to be active.

Millenium RAT is a sophisticated remote access tool written in C# and targeting Windows systems. This malware has an extensive range of capabilities for secretly gathering user data, bypassing detection with advanced anti-analysis methods, maintaining persistence, and remotely controlling a compromised system. The malware can exfiltrate data, collect system information, evade sandbox detection, resist debugging, disrupt processes, activate self-destruction mechanisms, and execute remote commands via Telegram. Additionally, the malware specializes in intercepting browser data, Discord tokens, keystrokes, and system information.

Xeno RAT, also developed in C#, targets Windows devices, particularly Windows 10 and Windows 11. Xeno RAT's features include a reverse SOCKS5 proxy server, real-time audio recording, and integration with a hidden virtual network computing (hVNC) module, giving attackers remote access to the infected computer.

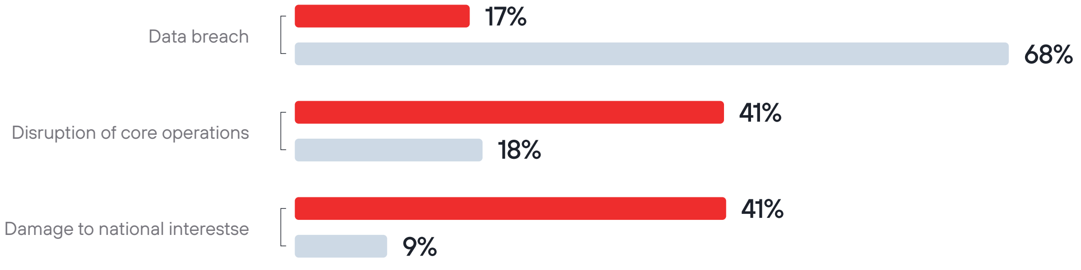
The PT Expert Security Center team noted that during the attacks on websites in 2024, attackers relied heavily on the FormBook malware. FormBook injects itself into various processes, logs keystrokes, and extracts information from the victim's HTTP sessions. Other functions include keylogging, clipboard monitoring, extracting information from HTTP/HTTPS/SPDY/HTTP2 forms, stealing passwords from browsers and email clients, and taking screenshots.

FormBook can execute commands from a malicious actor's server to upload and run files, start processes, use ShellExecute, clear browser cookies, harvest passwords, capture screenshots, upload and unpack ZIP archives, and shutdown or restart the system. One of the most interesting features of FormBook is reading the Windows ntdll.dll module and directly calling its functions, making user-level interception ineffective. FormBook can also change its file path, name, extension, and registry key used for persistence at random to ensure long-term presence in the system.

Consequences of attacks on organizations

While the 2021–2022 period was characterized by hacktivist and APT group actions aimed at damaging Iran's information and industrial infrastructure, 2023–H1 2024 an increase in attacks aimed at stealing confidential information.

Figure 23. Cyberattacks on organizations in Iran by consequence, 2021–2022 and 2023–H1 2024

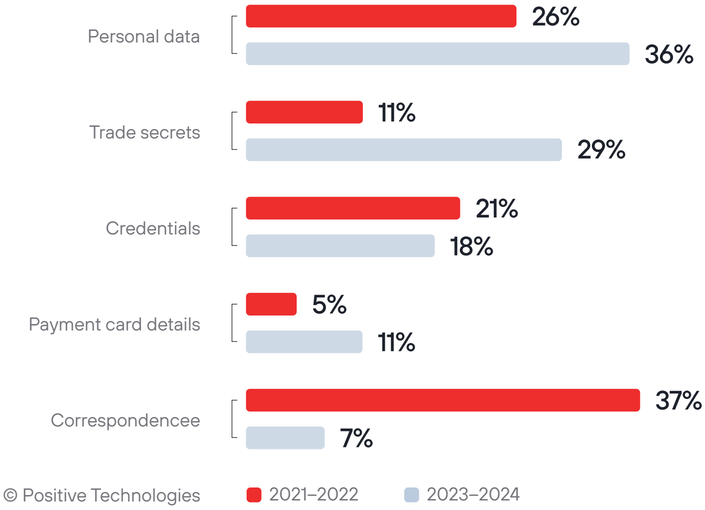


© Positive Technologies

During the period of 2021–2022, malicious activities, primarily targeting government institutions, most often led to disruptions in the core operations of Iranian organizations and harmed the interests of the state (in 41% of cases). However, in 2023–2024, the main type of *consequence* was a data breach (68%), while the share of disruptions to core operations and damage to national interests dropped by 23 and 32 percent, respectively.

During the 2021–2022 period, marked by elevated levels of hacktivist and APT group activity in the region, the most frequently stolen data types were correspondence (37%) and personal data (26%).

Figure 24. Data stolen in Iran by category, 2021–2022 and 2023–H1 2024



© Positive Technologies

According to dark web data, in 2023–H1 2024, 47% of listings announced successful cyberattacks on organizations and private individuals, indicating increased hacktivist activity aiming to publicize cyberincidents.

The more-than-twofold increase in cybercrime (from 12% to 27%) can be linked to financially motivated attacks on financial institutions. Cybercriminal activity in 2023–H1 2024 also affected the dynamics of data breaches, whose share rose from 32% in 2021–2022 to 70%. In 2023–2024, attackers mostly sold data on the dark web that had been stolen from manufacturers (22%), services (19%), retail and the government (11% each), telecommunications, and finance (7% each).

Among data breaches, personal data (36%) was the most common, followed by trade secrets (29%). Around 25% of dark web listings offered personal data stolen either from organizations or private individuals, which supports these statistics.

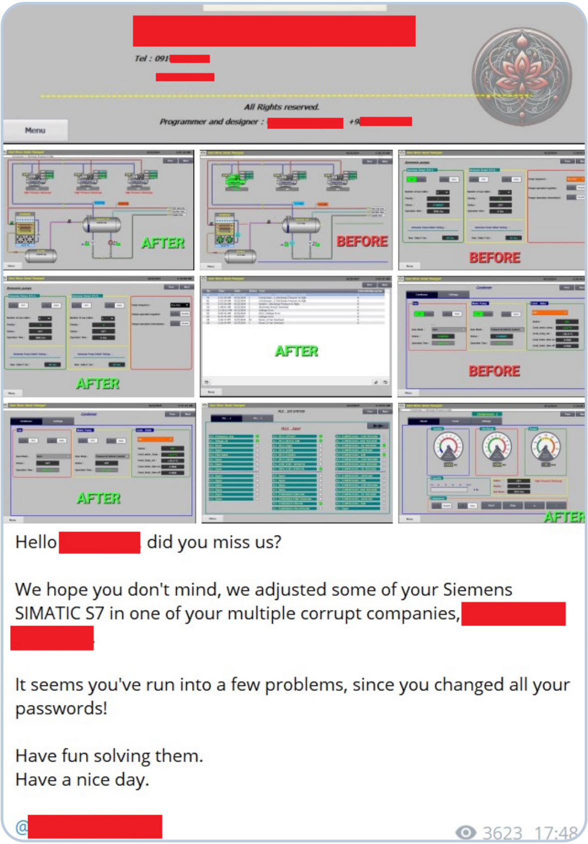
Conclusions on the cybersecurity threatscape for organizations

In both periods under review, government institutions were the most frequent targets of cyberattacks, accounting for over 30% of all attacks. According to dark web data for 2023–2024, government institutions ranked among the top three categories of organizations by number of breaches, with a share of 12%.

Attackers have repeatedly caused considerable damage to government infrastructure, despite the isolation of telecommunication and broadcasting networks and many government resources from external access. The nature of cyberattacks and the characteristics of Iran's Internet segment suggest insider actions (internal attackers) with the knowledge and capabilities to carry out such illicit activities. Experts from Threadstone71 claim that attackers had direct access to data, physical access to hardware and infrastructure, and deep knowledge of the infrastructure.

Cyberthreats targeting IoT devices remain relevant for the Middle East and Iran in particular. This is highlighted by a large number of dark web listings containing information on compromised industrial controllers, SCADA systems, and cameras.

Figure 25. Screenshot of an announcement on the dark web about the hack of industrial controllers at the manufacturing company (2024, outside the period under review)



Hello [redacted] did you miss us?

We hope you don't mind, we adjusted some of your Siemens SIMATIC S7 in one of your multiple corrupt companies, [redacted]

It seems you've run into a few problems, since you changed all your passwords!

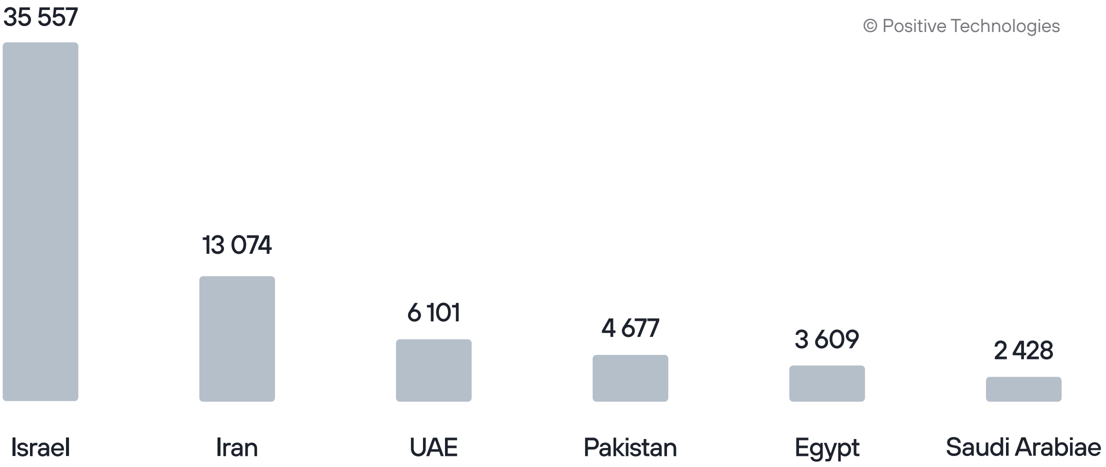
Have fun solving them.
Have a nice day.

@[redacted]

3623 17:48

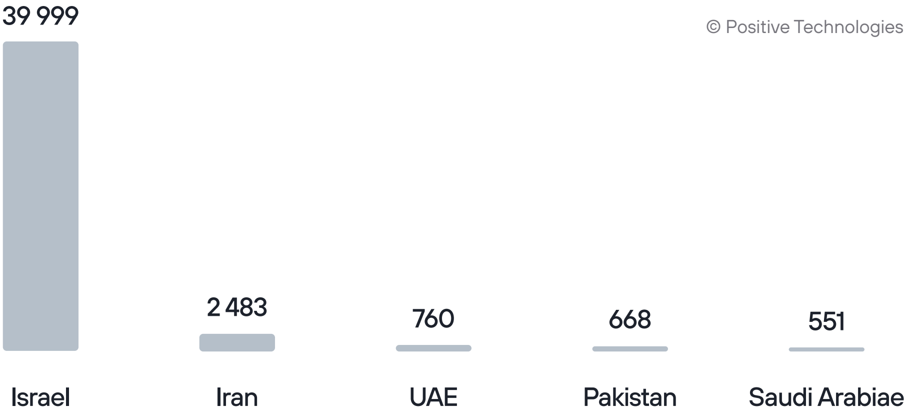
Successful cyberattacks on industrial sites may be partly due to insecure hardware configurations, which allow for example, remote connections to servers on open ports 3389 (default RDP) and 5900 (default VNC). Among Middle Eastern countries, Iran ranks second by number of publicly accessible servers with open ports 3389 and 5900, according to data from the Shodan service.

Figure 26. Publicly accessible servers with open port 3389 in the Middle East



© Positive Technologies

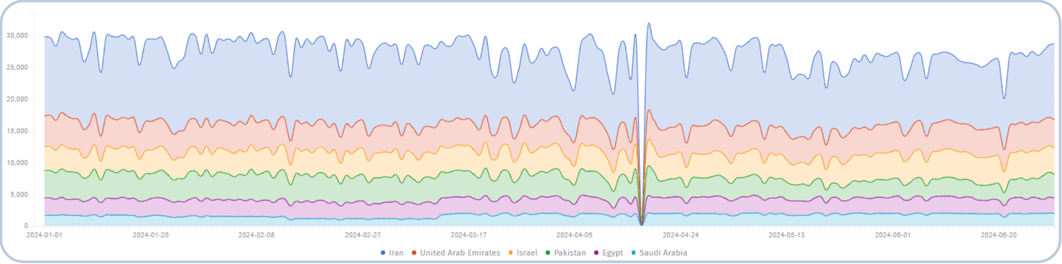
Figure 27. Publicly accessible servers with open port 5900 in the Middle East



© Positive Technologies

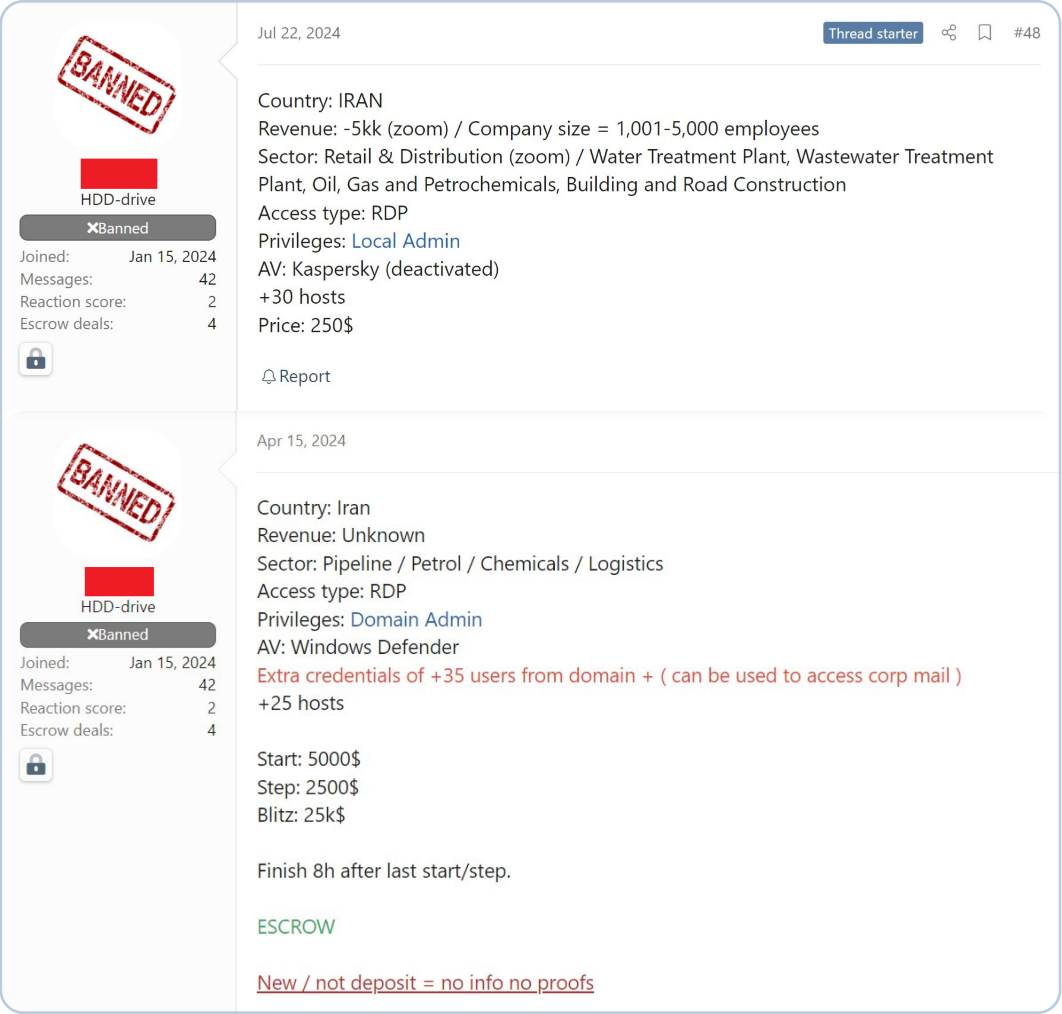
Statistics from the Shadowserver Foundation on publicly accessible servers running RDP in the first half of 2024 show that Iran leads among Middle Eastern countries in this metric, which suggests a significant cyberthreat.

Figure 28. Changes in the number of available servers running RDP in Iran compared to other Middle Eastern countries in H1 2024



The danger of using servers running RDP is highlighted by the substantial number of dark web ads selling access to infrastructure. Targets of cyberattacks include construction firms, trading companies, and petrochemical and water treatment facilities, among others.

Figure 29. Examples of dark web listings for RDP access to Iranian organizations



[redacted]
HDD-drive
✕Banned

Joined:	Jan 15, 2024
Messages:	42
Reaction score:	2
Escrow deals:	4

Jul 22, 2024 Thread starter #48

Country: IRAN
Revenue: -5kk (zoom) / Company size = 1,001-5,000 employees
Sector: Retail & Distribution (zoom) / Water Treatment Plant, Wastewater Treatment Plant, Oil, Gas and Petrochemicals, Building and Road Construction
Access type: RDP
Privileges: Local Admin
AV: Kaspersky (deactivated)
+30 hosts
Price: 250$

Report

[redacted]
HDD-drive
✕Banned

Joined:	Jan 15, 2024
Messages:	42
Reaction score:	2
Escrow deals:	4

Apr 15, 2024

Country: Iran
Revenue: Unknown
Sector: Pipeline / Petrol / Chemicals / Logistics
Access type: RDP
Privileges: Domain Admin
AV: Windows Defender
Extra credentials of +35 users from domain + (can be used to access corp mail)
+25 hosts

Start: 5000$
Step: 2500$
Blitz: 25k$

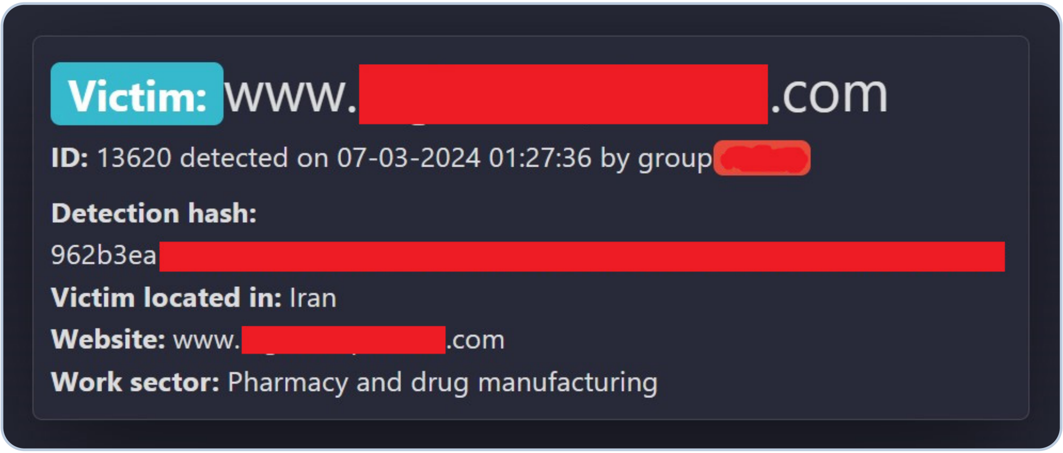
Finish 8h after last start/step.

ESCROW

New / not deposit = no info no proofs

3. The dominant use of malware in cyberattacks against organizations, particularly government and financial institutions, coupled with increased cybercriminal activity in the region, highlights the dangers posed by malicious actors employing not only wipers and stealers but also ransomware.

Figure 30. Screenshot of a dark web ad offering ransomware for attacking a pharmaceutical company



Victim: www.[redacted].com

ID: 13620 detected on 07-03-2024 01:27:36 by group [redacted]

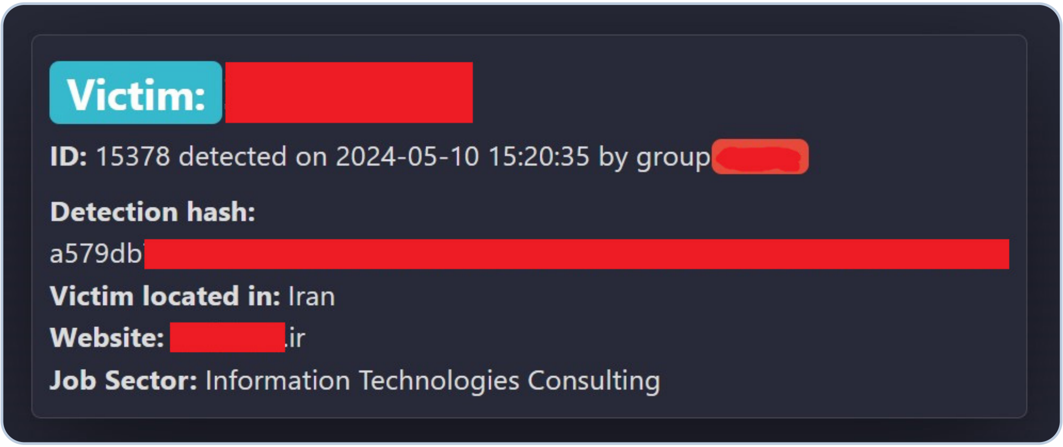
Detection hash:
962b3ea[redacted]

Victim located in: Iran

Website: www.[redacted].com

Work sector: Pharmacy and drug manufacturing

Figure 31. Screenshot of a dark web ad offering ransomware for attacking an IT company



Victim: [redacted]

ID: 15378 detected on 2024-05-10 15:20:35 by group [redacted]

Detection hash:
a579db[redacted]

Victim located in: Iran

Website: [redacted].ir

Job Sector: Information Technologies Consulting

Cyberattacks on private individuals in Iran

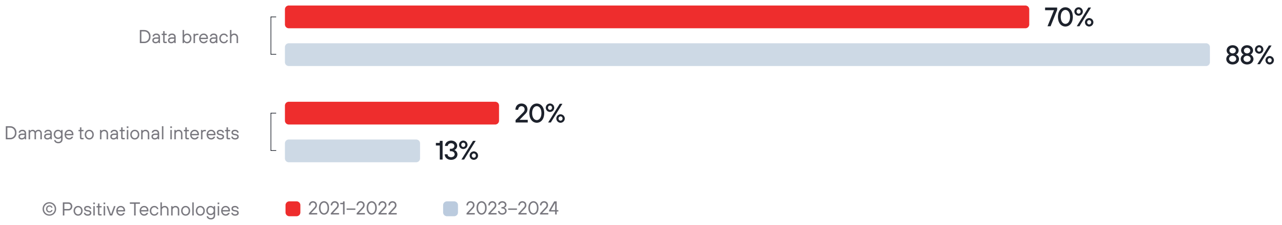
The share of cyberattacks on private individuals during both periods did not exceed 30%, but the absolute number of these attacks was significant. Cybercriminals will undoubtedly profit from the theft of payment card details and PINs. Moreover, obtaining the personal data of private individuals is the first and often crucial step in implementing a wide range of cyberthreats. With someone else's personal data on hand, attackers can increase the success of their cyberattacks through social engineering, tailoring them to a specific victim. An attacker can also impersonate the owner of the personal data, thereby obtaining information about the victim's social circle, as well as the operational infrastructure of the company where the victim is employed.

Private individuals are attacked by both cybercriminals and hacktivists: humans are the weakest link in any infrastructure, and social engineering techniques often provide access to the target's infrastructure or data. This partly explains the increase in the percentage of cyberattacks using social engineering techniques, both in Iran and the Middle East at large.

Cybersecurity threatscape for private individuals

In 2023–H1 2024, the percentage of *consequences* affecting state interests decreased from 20% to 13%, while data breaches increased by 18%. This indicates a shift in the focus of cyberattacks from state officials towards the general public in Iran.

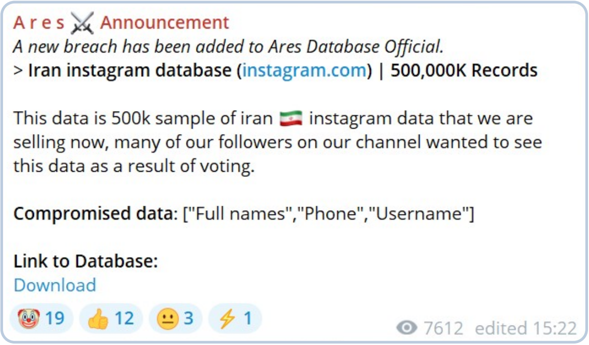
Figure 32. Cyberattacks on private individuals in Iran by consequence, 2021–2022 and 2023–H1 2024



© Positive Technologies

Personal data is the most common category of leaked data according to dark web statistics. For instance, one listing offered a database containing 500,000 lines of data on Instagram[1] (is banned in Iran) users who are Iranian citizens. The data included the user's full name, phone number, and profile name.

Figure 33. Screenshot of a dark web listing offering the data of Iranian Instagram[2] users



Ares ⚔️ Announcement
A new breach has been added to Ares Database Official.
> **Iran instagram database (instagram.com) | 500,000K Records**

This data is 500k sample of iran 🇮🇷 instagram data that we are selling now, many of our followers on our channel wanted to see this data as a result of voting.

Compromised data: ["Full names","Phone","Username"]

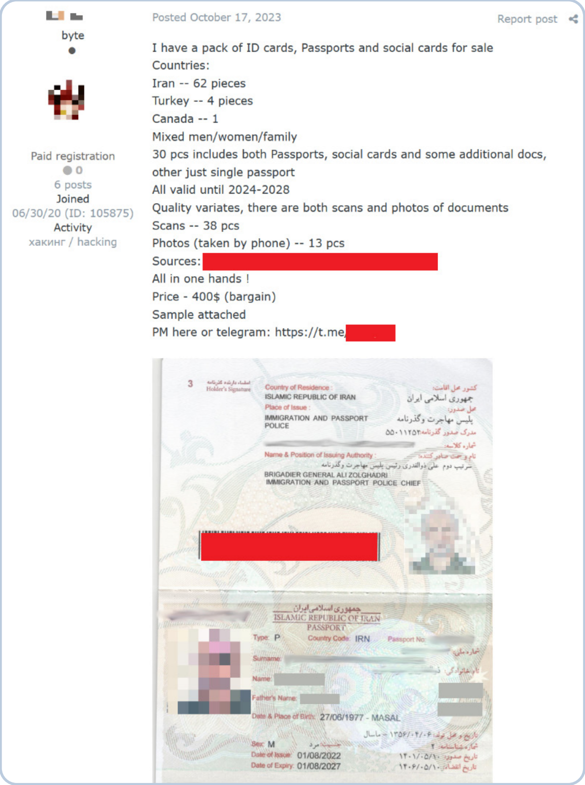
Link to Database:
Download

[1] A product from Meta, a company that has been designated as an extremist organization and banned in Russia under Russian law

[2] A product from Meta, a company that has been designated as an extremist organization and banned in Russia under Russian law

Among the most frequently encountered personal data are the person's full name, their mobile phone number, address, and scans of passports and social cards.

Figure 34. Screenshot of a dark web listing offering private individuals' personal data



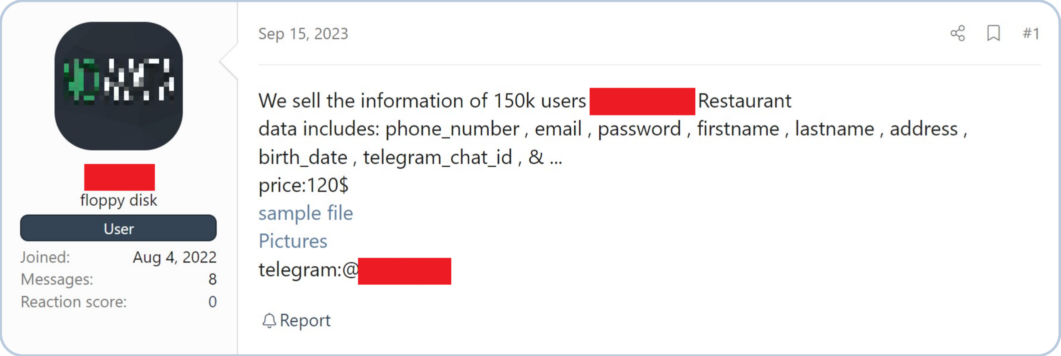
Posted October 17, 2023

I have a pack of ID cards, Passports and social cards for sale
Countries:
Iran -- 62 pieces
Turkey -- 4 pieces
Canada -- 1
Mixed men/women/family
30 pcs includes both Passports, social cards and some additional docs,
other just single passport
All valid until 2024-2028
Quality variates, there are both scans and photos of documents
Scans -- 38 pcs
Photos (taken by phone) -- 13 pcs
Sources: [redacted]
All in one hands !
Price - 400$ (bargain)
Sample attached
PM here or telegram: https://t.me[redacted]

[redacted]

For $120, the personal data of 150,000 customers of a pizzeria in Tehran, including phone numbers, home addresses, email addresses, passwords, and birthdates, can be purchased on the dark web.

Figure 35. Screenshot of a dark web listing offering the data of a pizzeria customers

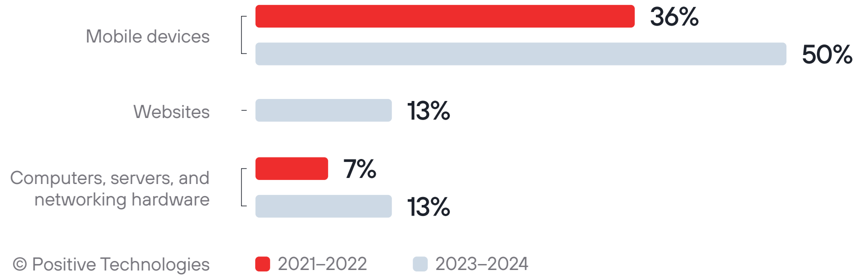


Sep 15, 2023

We sell the information of 150k users [redacted] Restaurant
data includes: phone_number , email , password , firstname , lastname , address ,
birth_date , telegram_chat_id , & ...
price:120$
sample file
Pictures
telegram:@[redacted]

In both periods under review, the share of cyberattacks targeting mobile devices remained the highest at 36% and 50%, respectively. This is due to the fact that Iranians primarily rely on mobile Internet service for communications, shopping, news, and so on, given its higher speed (31.82 Mbps) compared to fixed-line Internet connections. The high success rate of cyberattacks on mobile devices can be attributed to the predominance of the Android operating system, which offers users greater freedom to download and install various applications than iOS does. Cybercriminals frequently distribute malicious mobile apps that mimic legitimate ones. Due to the inconvenience of using the Google Play, where some apps are blocked, applications are distributed via popular websites and social networks.

Figure 36. Cyberattacks on private individuals in Iran by target asset type, 2021–2022 and 2023–H1 2024

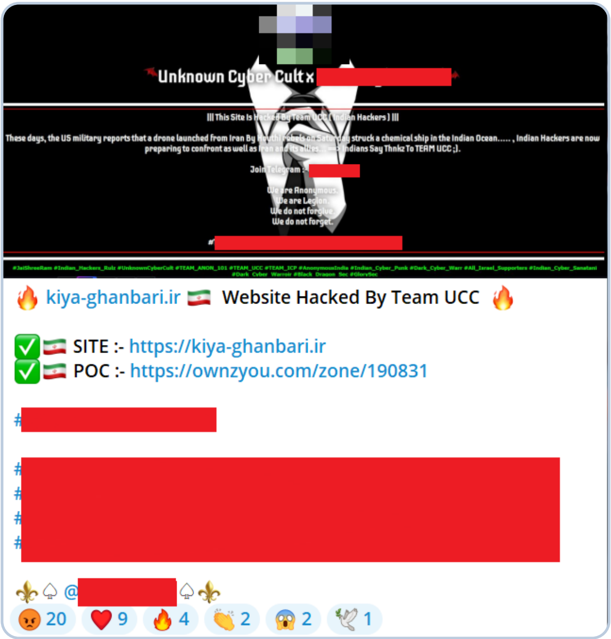


© Positive Technologies

A significant increase compared to the previous period was seen in the Websites category, which rose by 13%. Researchers at SafeBreach uncovered an espionage campaign where a PowerShell-based stealer named PowerShortShell, snatched Google and Instagram[3] login credentials from Persoan-speaking users. The malicious code exploits a Microsoft MSHTML vulnerability (CVE-2021-40444) in the Internet Explorer browser engine.

Among the cyberattacks on websites, locally known Iranian filmmaker Kiya Ghanbari's personal site was defaced by the UCC hacking group. This group, claiming to be Indian hackers, vandalized the website in retaliation for the drone attack on a chemical tanker that occurred in late 2023 approximately 200 nautical miles off the coast of India.

Figure 37. Screenshot of a dark web post about the defacement of the Iranian filmmaker's website



Unknown Cyber Cult x [redacted]

||| This Site Is Hacked By Team UCC (Indian Hackers) |||

These days, the US military reports that a drone launched from Iran By Houthi rebels on Saturday struck a chemical ship in the Indian Ocean..... , Indian Hackers are now preparing to confront as well as Iran and its allies... ==> Indians Say Thnkz To TEAM UCC ;).

Join Telegram :- [redacted]

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.

#[redacted]

#JaiShreeRam #Indian_Hackers_Rulz #UnknownCyberCult #TEAM_ANON_101 #TEAM_UCC #TEAM_ICP #AnonymousIndia #Indian_Cyber_Punk #Dark_Cyber_Warr #All_Israel_Supporters #Indian_Cyber_Sanatani #Dark Cyber Warrior #Black Dragon Sec #GlorySec

🔥 kiya-ghanbari.ir 🇮🇷 Website Hacked By Team UCC 🔥

✅🇮🇷 SITE :- https://kiya-ghanbari.ir
✅🇮🇷 POC :- https://ownzyou.com/zone/190831

#[redacted]

#
#
#
#[redacted]

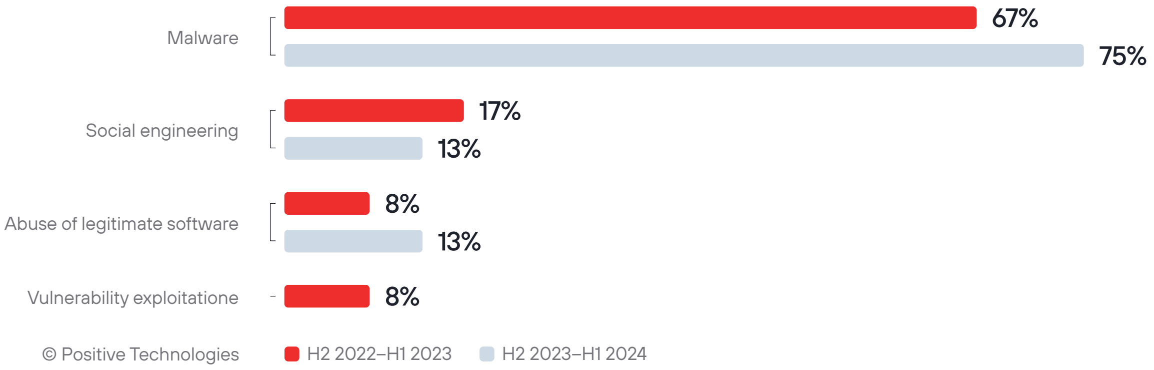
⚜♤@[redacted]♤⚜

😡 20 ❤️ 9 🔥 4 👏 2 😱 2 🕊 1

[3] A product from Meta, a company that has been designated as an extremist organization and banned in Russia under Russian law

As with organizations, malware remains the most commonly used method for carrying out cyberattacks on private individuals. Combined with the high proportion of cyberattacks on mobile devices (50%), it can be noted that Iran is characterized by cyberattacks involving malware that targets Android mobile devices.

Figure 38. Cyberattacks on individuals in Iran by method, H2 2022–H1 2023 and H2 2023–H1 2024



Data from Kaspersky confirms the relevance of cyberthreats targeting mobile devices in Iran. In 2022, Iran was among the three countries with the highest percentage of users attacked by mobile malware (Iran: 14.53%, Syria: 15.61%, and China: 17.70%). The most common mobile cyberthreat in Iran in 2022 was Trojan-Spy.AndroidOS.Agent.aas, a modified version of WhatsApp containing a spyware module. In 2023, the dominant malware in the country was Trojan.AndroidOS.Hiddad.da (97.39%), which not only copies but also destroys, modifies, and blocks it data. In the first half of 2024, the activity of the Trojan-Spy.AndroidOS.SmsThief.tt, conducting digital surveillance of users in Iran, reached 96.88%.

For example, in 2023, researchers at Zimperium discovered more than 200 fake mobile Android apps that mimicked major Iranian banks to steal client information. All of the apps were available for download from December 2022 to May 2023, harvesting online banking login credentials and credit card details, hiding and intercepting incoming text messages used for multi-factor authentication.

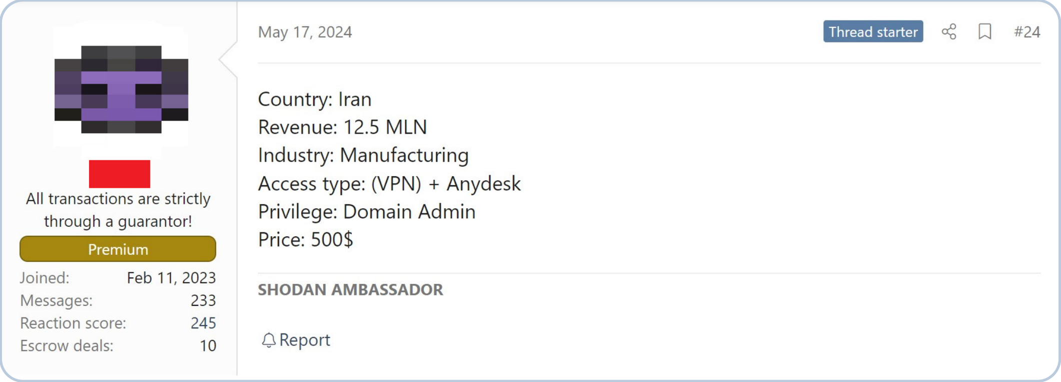
The 2023 espionage campaign targeting mobile users is not the first for Iran. In 2021, a widespread SMS phishing (smishing) campaign saw malicious actors impersonate Iranian government services. The cyberattack relied on social engineering and malware: Iranians received text messages purportedly from government services, containing a link that redirected them to a phishing website where they were notified of a complaint filed against them. The user was then asked to provide their personal details, such as name, phone number, and national ID number to proceed to the electronic system and avoid visiting an offline branch due to restrictions introduced during the COVID-19 pandemic.

A sizeable portion of mobile malware in Iran is designed to exploit legitimate VPN services or disguise itself as a VPN app. This type of cyberthreat is a regional characteristic due to the widespread use of VPN services among young people.

In 2023, Iranian users were attacked with a VPN malvertising campaign. Researchers at Trend Micro discovered malware for data theft, named OpcJacker, whose main capabilities included keylogging, taking screenshots, stealing confidential data from browsers, downloading additional modules, and replacing cryptocurrency addresses in the clipboard for theft.

Users of the legitimate, popular 20Speed VPN service in Iran were attacked with EyeSpy, an online surveillance tool developed and distributed in Iran. Judging by dark web listings, the trend for using VPNs to carry out cyberattacks extends to organizations. Some dark web posts offer to provide access via VPN.

Figure 39. Example of a listing offering access to a manufacturing company via VPN



[redacted]

All transactions are strictly through a guarantor!

Premium

Joined: Feb 11, 2023
Messages: 233
Reaction score: 245
Escrow deals: 10

May 17, 2024

Country: Iran
Revenue: 12.5 MLN
Industry: Manufacturing
Access type: (VPN) + Anydesk
Privilege: Domain Admin
Price: 500$

SHODAN AMBASSADOR

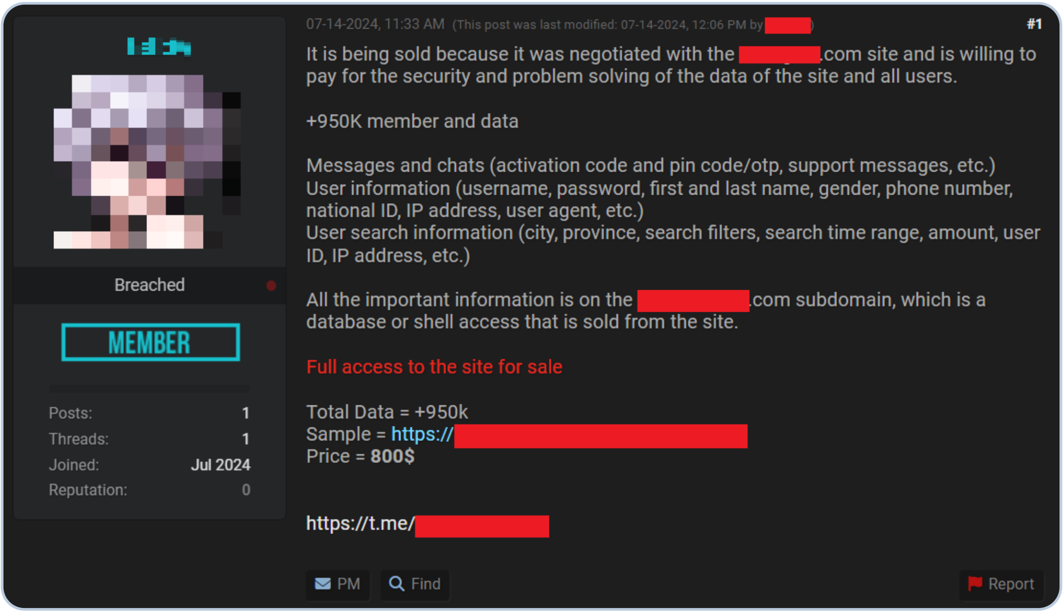
According to the team at the Positive Technologies expert center, many of the malware programs they detected in Iran imitated VPN services, such as Warp Plus, Psiphon, Warp-Plus GUI, and others.

Trend Micro analysts report that malware disguised as the GlobalProtect VPN tool from Palo Alto Networks is active in the Middle East. The initial vector of cyberattacks using this malware is still unknown. The attackers are understood to use phishing to convince victims that they are installing the legitimate GlobalProtect.

Another regional feature of Iran is the legal status of cryptocurrency. The media outlet Cybernews covered a notable security incident in 2024 caused by misconfiguration rather than cyberattacks. The incident affected an Iranian cryptocurrency exchange that supports more than 300 coins and tokens. A misconfiguration in the MinIO (high-performance object storage system) instance opened up access to cloud-based containers containing the platform's Know Your Customer (KYC) data. When interacting with the platform, users must verify their identity by uploading official documents. The MinIO configuration error compromised about 230,000 Iranian citizens, exposing their signed regulatory agreements, passports, IDs, and credit cards.

Data from the dark web in 2024 confirms a growing interest among hackers in cryptocurrency services. For example, there have been dark web listings offering to sell data from the Iranian cryptocurrency and blockchain company.

Figure 40. Screenshot of a dark web listing offering data and access to blockchain company



07-14-2024, 11:33 AM (This post was last modified: 07-14-2024, 12:06 PM by [redacted]) #1

It is being sold because it was negotiated with the [redacted].com site and is willing to pay for the security and problem solving of the data of the site and all users.

+950K member and data

Messages and chats (activation code and pin code/otp, support messages, etc.)
User information (username, password, first and last name, gender, phone number, national ID, IP address, user agent, etc.)
User search information (city, province, search filters, search time range, amount, user ID, IP address, etc.)

All the important information is on the [redacted].com subdomain, which is a database or shell access that is sold from the site.

Full access to the site for sale

Total Data = +950k
Sample = https://[redacted]
Price = **800$**

https://t.me/[redacted]

Breached

MEMBER

Posts:	1
Threads:	1
Joined:	Jul 2024
Reputation:	0

The database on offer contained the following:

- Messages and chats (activation codes, PINs, OTPs, support tickets, and so on)
- User details (username, password, first and last name, gender, phone number, national ID, IP address, user agent string, and so on)
- Search criteria (city, province, search filters, search time range, amount, user ID, IP address, and so on)

In addition to the data, the listed price of $800 included shell access to the subdomain.

Conclusions on the cybersecurity threatscape for individuals

Despite the smaller share of cyberattacks targeting individuals compared to organizations, the absolute number of these attacks is huge. Iran's digital landscape for individuals is characterized by widespread use of smartphones for communication, news browsing, and shopping. Mobile marketing dominates the Iranian e-commerce market. This is due to the wide availability of smartphones and faster mobile data rates compared to fixed-line links: 31.82 Mbps versus 12.76 Mbps on average.

The mobile cyberthreats situation is exacerbated by the widespread use of VPN services to access banned resources, such as YouTube or Instagram[4]. Data from 2023–2024 shows that VPN services, often in the form of mobile apps, have been frequently exploited by cybercriminals to attack individuals. Hackers use both legitimate VPN services that they can compromise and malicious apps posing as VPN services.

The rise in cyberattacks that rely on social engineering has been driven by advancements in AI technology. Experts at Avast report an increase in cybercrime involving audio and video deepfakes. AI is used as a generator of fake content and a tool for mass phishing.

[4] A product from Meta, a company that has been designated as an extremist organization and banned in Russia under Russian law

Tactics and techniques of APT and hacktivist groups operating in Iran, mapped to the MITRE ATT&CK Enterprise Matrix

A description of tactics and techniques is primarily available for APT groups, as they are more organized and highly skilled hackers than hacktivist groups. APT groups specialize in cyberespionage, focusing on covert system intrusion, trace eradication, and remote access.

This section delves into the tactics and techniques employed by the APT groups APT15, Bahamut, Molerats, Desert Falcons, and the hacktivist collective GhostSec.

APT groups' arsenal

APT groups typically combine their own custom malware with publicly available tools.

For example, APT15 uses widely accessible tools like Mimikatz and LaZagne (T1003.001, T1003.004, T1003.005), while their malicious functionality is primarily concentrated in backdoors like RoyalCli and RoyalDNS, Ketrum, BS2005/Ketrican/Graphican (one family with minor differences in functionality between members). APT15's arsenal includes tools for both Windows (Okrum, MirageFox) and Android: the surveillance tool SilkBean with extensive remote access trojan (RAT) features; HenBox, which targets Xiaomi devices running MIUI; and BadBazaar, primarily a banking trojan.

In addition to backdoors, APT15 uses trojans. For example, TidePool offers many capabilities typical of most RATs. It allows the attacker to read, write, and delete files and folders, and execute commands via named pipes. TidePool gathers information about the victim's computer, encodes data in base64, and sends it to the C2 server over HTTP. This matches the capabilities of the BS2005 malware family used by the Ke3chang actor. TidePool is embedded within an MHTML document that exploits CVE-2015-2545.

Molerats also have a substantial number of backdoors (DropBook, SharpStage, MoleNet, and others), which ensure access to data even if it is encrypted and protected. To dump passwords saved in victims' browsers (T1555.003), the group uses the publicly available BrowserPasswordDump10 tool.

Desert Falcons primarily use malware that functions as cyber-espionage tools. Thus, the custom-made Android spyware used by Desert Falcons is called Desert Scorpion. It can record sound from phone calls and the built-in microphone (Audio Capture), track location (Location Tracking), and view the user's confidential data (Protected User Data), such as contacts (T1636.003), text messages (T1636.004), and installed apps (Software Discovery). Other malware used by Desert Falcons to target Android devices includes VAMP, designed to steal data through call recording (Audio Capture) and stealing contacts and documents stored on the device, and GnatSpy, which expands VAMP's functionality by collecting information about battery usage, memory, storage, and SIM card status. For iOS devices, the group used Phenakite, which is capable of recording phone call audio, collecting and forwarding WhatsApp media files, photos, and files with specific extensions (Data From Local System), and redirecting victims to phishing pages for Facebook[5] and iCloud to steal credentials for these services (Input Capture).

[5] A product from Meta, a company that has been designated as an extremist organization and banned in Russia under Russian law

Bahamut utilized the publicly available, cross-platform remote administration tools (RATs) NETWIRE and Revenge RAT for remote control. Additionally, the group employed various malware for Software Discovery, particularly to gather a list of active processes, identify installed software, and check for specific antivirus programs (T1518.001), including Kaspersky, Quick Heal, AVG, BitDefender, Avira, Sophos, Avast!, and ESET.

Gaining initial access

To infiltrate the infrastructure, attackers have to find an initial entry point: a server, an employee's computer, or another network component, and infect that with malware to enable further lateral movement across the network.

Many of these groups began their cyberattacks with targeted phishing (Phishing). In particular, Bahamut and Molerats used phishing emails containing malicious links (T1566.002), and Microsoft Word and PDF attachments (T1566.001). Bahamut also leveraged messaging apps (T1566.003). APT15 operates with the characteristics of Iran in mind, gaining access via VPN through compromised accounts and stolen VPN certificates (External Remote Services, T1133), among other methods. Molerats sent malicious links via email, prompting users (User Execution) to open a RAR archive and run a file (T1204.001), and malicious files that tricked users into clicking “Enable Content” to run embedded macros and download malicious archives (T1204.002).

Gaining persistence in the target infrastructure

The next step is for the attackers to establish a foothold in the infrastructure. A common technique involves setting up malware to autostart (Boot or Logon Autostart Execution), either through registry keys or by adding a link to the malware to the Startup folder (T1547.001). For example, the Bahamut group created LNK files in the Startup folder.

APT15 developed its own malware, allowing it to persist within victim networks (T1587.001). Molerats saved malicious files in the AppData and Startup folders to maintain persistence in the system (T1547.001). Desert Falcons used the Subvert Trust Controls technique, utilizing a mobile app that, when launched on a Huawei device, added itself to the list of protected applications, so it could run even when the screen was off (T1553.006).

Infrastructure exploration

Groups use both system utilities and malware to investigate the processes running on compromised nodes (Process Discovery). For instance, APT15 collected process information using the command-line utility tasklist. APT15's malware captured credentials that victims entered on compromised devices (Input Capture).

Attackers also search files and directories on compromised nodes for any potentially useful information (File and Directory Discovery). For example, Bahamut relies heavily on file enumeration, and Desert Falcons have a special tool for recursively browsing directories across all drives and searching for certain files based on their paths. Molerats used the MoleNet and DropBook tools to collect system information (System Information Discovery) and retrieve the names of all files and folders in the Program Files directories.

GhostSec employs similar techniques to obtain valuable information (File and Directory Discovery, System Information Discovery), supplementing these by gathering data on registered services on the local system (System Service Discovery). The group uses automated tools (Automated Collection) to collect internal information about the compromised system or network infrastructure, and searches in local sources (Data from Local System), such as file systems, configuration files, or local databases, to find the files it needs and confidential data before forwarding these to a remote server.

Collecting valuable information

To access certain information, hackers may need additional credentials. To get these, they often extract passwords from system process memory (OS Credential Dumping). APT15 used the Mimikatz and LaZagne tools, and extracted accounts from the NTDS.dit file, a database that stores Active Directory information (T1003.003). APT15, Bahamut, Desert Falcons, and Molerats relied heavily on Input Capture to intercept the data entered by victims on compromised devices. These groups used keyloggers for this purpose.

Some of the groups archive data they collect (Archive Collected Data). Molerats used DustySky, which created temporary directories for storing collected files and allowed these to be archived before forwarding outside of the corporate infrastructure.

The financially motivated GhostSec's group encrypts valuable data it collects from target systems (Data Encrypted for Impact) to disrupt access to the system and network resources for the compromised device. Embedded data may be deleted, and services designed to assist in system recovery are disabled to prevent restoring access to the data (Inhibit System Recovery).

Evasion techniques

A common technique for evading protection is Masquerading, where malware is disguised as legitimate files or applications. For example, Bahamut used icons mimicking Microsoft Office files to mask malware and tried to hide executable files by changing the file extension to .scr to imitate Windows screensavers. Desert Falcons also delivers its application via a malicious app marketplace (Deliver Malicious App via Other Means, T1476).

GhostSec employs bootkit elements, which automatically execute upon system startup (T1037.005) to retain access, for example, after the compromised device reboots. The group also uses various evasion techniques: file or information obfuscation (Obfuscated Files or Information), process injection by executing arbitrary code in the address space of a separate process (Process Injection), masquerading its artifacts to appear legitimate (Masquerading), and modifying file timestamps (last modified, last accessed, created, and last changed) (T1070.006) to make altered files less conspicuous to forensic analysts.

Recommendations for government and business organizations

To protect government organizations from cyberthreats, it is important to consider insider threats, as security measures aimed at external cyberthreats will not stop an insider who has no need to hack the system and can collect data directly.

At a basic level, it is recommended to apply organizational and technical measures, including a comprehensive security audit of the information infrastructure; the introduction of strict policies for managing accounts and passwords, as well as access, both virtual and physical, to the infrastructure; building a comprehensive information security infrastructure using a multi-vendor approach, and cybertesting and cyber exercises to ensure cyber-resilience.

A much greater effect in protecting government agencies from cyberthreats can be achieved by cooperating with governments that face similar cyberthreats and engineering challenges.

Using an effective cybersecurity methodology can significantly improve the cyber-resilience of organizations of any size and ensure the protection of sensitive data in the face of destructive cyberattacks by:

- Identifying non-tolerable events and scenarios for their implementation
- Conducting comprehensive cyber-transformation by reinforcing the protection of IT infrastructure components
- Regularly auditing the cyber-resilience of organizations

For organizations involved in implementing technological and business processes, it is crucial to identify specific non-tolerable events and the critical infrastructure components that could be targeted. Due to the regional characteristics, remote access settings, particularly those for RDP and VNC, require careful attention. A poorly configured system can be exploited by attackers to launch cyberattacks. For industrial facilities equipped with IoT devices—inherently one of the most vulnerable parts of the infrastructure—a list of non-tolerable events would directly correlate with common IoT cybersecurity issues, including the following:

- A lack of specialized hardware protection. As of 2023, 66% of IoT devices lacked this, and 29% had no security features at all.
- Administrators' lack of awareness about the full range of IoT devices in use. According to the Ponemon Institute, companies often lack a full understanding of all connected devices, which results in around 48% of devices being at risk because they are either no longer detected by the company's IT department or run outdated software.
- Lack of encryption for IoT traffic. According to a study by Palo Alto Networks, 98% of IoT devices have this issue.

Recommendations for individuals

Key cyberthreat trends affecting individuals in Iran include the following:

- A persistent rise in cybercrimes perpetrated via cyberattacks targeting Android mobile devices, particularly those exploiting the mimicry of VPN services.
- An increasing percentage of cyberattacks on banking apps and legitimate VPN apps.
- A growing interest among cybercriminals in cryptocurrency apps.
- The emergence of more complex cyberattacks that utilize social engineering methods combined with AI.

Although it is premature to declare a full-scale wave of cyberattacks on cryptocurrency exchanges and mobile apps, the emergence of malware targeting crypto apps, a recent data breach due to misconfigured security settings on an exchange, and dark web listings offering blockchain-related data point toward a growing threat.

Common scenarios of cyberattacks using social engineering:

- Fake business proposals targeting popular content creators.
- Posting videos, in particular AI generated, with descriptions that contain malicious links disguised as popular software downloads.
- Setting up fake domains that mimic legitimate software companies and using them to distribute malware.

Recommendations for individuals include increasing cybersecurity literacy through public education on digital hygiene and safe online behavior. Digital hygiene generally implies that apps must only be installed from trusted sources, and mobile devices should have antivirus software.

Training users will also enable them to effectively resist social engineering attacks by ignoring potentially dangerous attachments in emails and chats, and suspicious links.