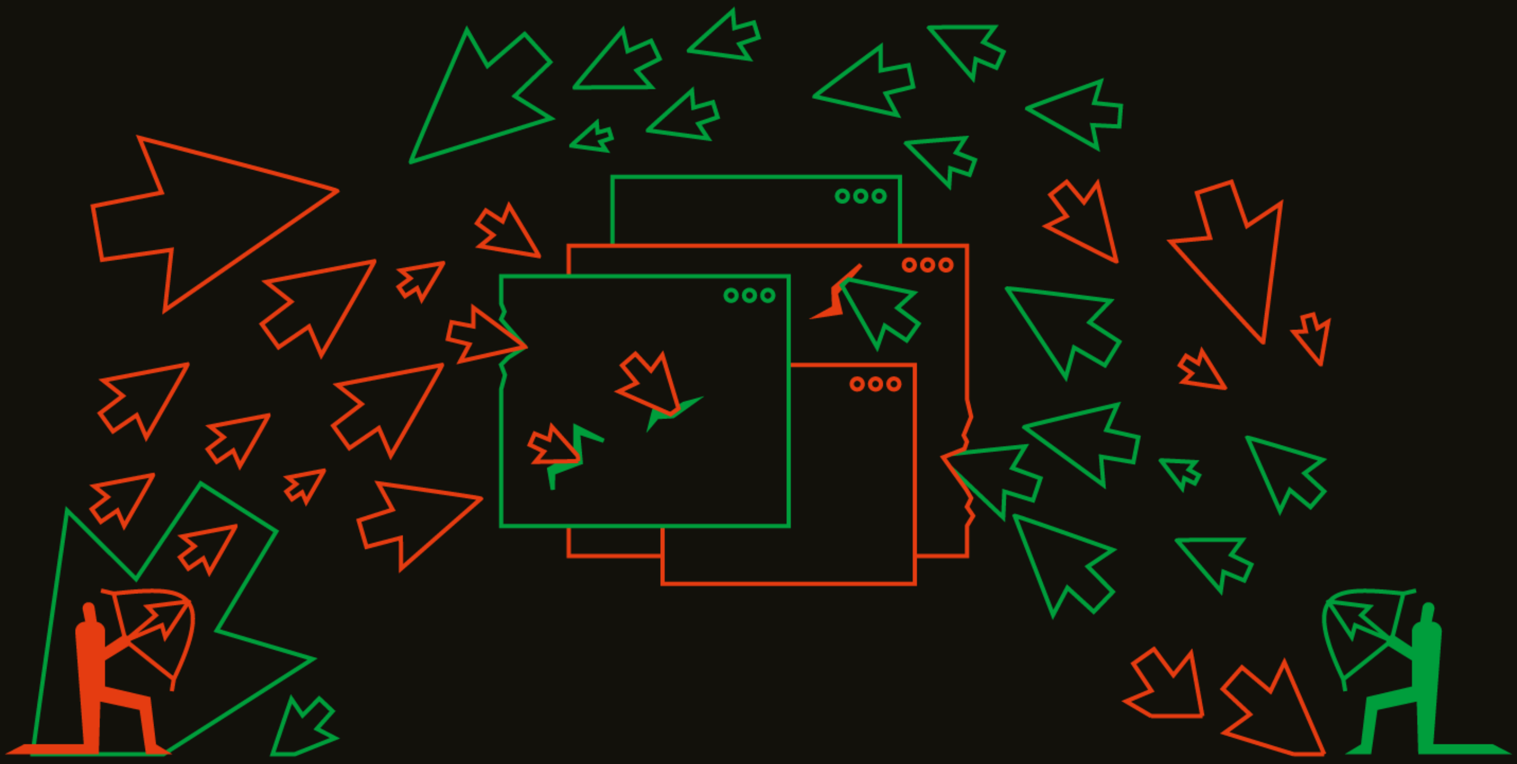


HackerWatch Roundup

Shadow Cyber War Between Iran and Israel Has Consequences for Digital Rights

Filterwatch

January-June 2022

Over the past year, tensions over Iran’s nuclear program have permeated into cyberspace at an unprecedented rate, prompting an unending wave of tit-for-tats with Israel. Ostensibly anonymous hacktivist groups presenting as dissidents have repeatedly targeted Iran’s public sector with espionage and sabotage attacks. It is not just that each side accuses the other of orchestrating these attacks. Thus far, the New York Times has confirmed with two U.S. officials that Israel was behind at least one of these events that targeted gas pumps in Iran last October.[1] There is also speculations about the

[1] https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html

Iranian origin of cyber activities against Israeli entities.[2] The growing pace of these incidents is bringing decades of hostility between the two regional rivals into broad daylight in and through the cyber domain.

The recent attacks have shed new light on Iran’s vulnerability against cyber attacks. FilterWatch has obtained a threat intelligence document prepared for Tehran municipality that elaborates on the details of a malware that targeted the institution. While such a report indicates progress toward investigating and responding to cyber attacks within government bodies, it still lacks key qualities that shows compelling competence on the part of the government in analysis and strategic defense against cyber attacks.

New questions have emerged about the Islamic Republic’s ability to address the existing gaps in cybersecurity technology and policy. These events have also highlighted the consequences of vastly unequal investment into the National Information Network (NIN) and offensive cyber capabilities,[3] compared to that of defensive capacity for protecting domestic networks, infrastructure, and the privacy and security of users.

With over $6 billion invested, the NIN is the most costly national telecommunications project in the history of the Islamic Republic.[4] Its overarching goal is to substantially cut reliance on international platforms and global Internet gateways and to centralize Internet access within the country as much as possible. To this end, Iran has spent over $1.5 billion on a domestic search engines project and hundreds of thousands more in additional subsidies to go toward mature development of a host of software for instant messaging, streaming, and banking, among other services. Thus far, none of these platforms have substituted the more popular and secure international peers.

The recent cyber attacks on Iranian infrastructure put this investment to test and underscored the challenges of overemphasis on centralization without properly addressing the cybersecurity needs of such a network – and its impact on people’s daily lives.

[2] https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

[3] In over a decade, Iran has become one of the key threat actors in cyberspace along with China, Russia, and North Korea. Between 2009 and 2019, Iran targeted 7 countries in 31 cyberattacks, with 42% aimed at the United States. Read more at: https://www.privacyaffairs.com/geopolitical-attacks/

[4] https://cyber.harvard.edu/node/100145

Much of the criticisms about the NIN thus far have revolved around its implications for freedom of expression and access to information. However, recent incidents highlight the significant yet under-researched issues of human rights and digital governance against the backdrop of major cybersecurity holes in the domestic network.

Iran's Civilian Defense Organization (CDO) was established in the early 2000s to guard the security of civilian networks and pursue non-military defensive measures. Since its inception, however, the organization has come under criticism for major security breaches like the Stuxnet attack on the Natanz nuclear plant in 2010 and a series of unexplained fires[5] in oil and petroleum refineries in 2016. While these criticisms remain unaddressed, the head of CDO, General Gholamreza Jalali, has instead advocated for the development of a national intranet (aka NIN)[6] and has suggested the use of cryptocurrencies for bypassing the U.S.-imposed economic sanctions.[7]

After suffering multiple blows allegedly from Israel, in June 2022 the parliament proposed structural changes to the CDO[8] as well as new budgetary requirements to improve the resilience of critical infrastructure and civilian networks. Under this proposal every public agency is required to dedicate 1% of its revenue to the CDO.[9] While this legislative proposal signals Iran's changing approach to cybersecurity, there seems to be a long way to achieving this goal. CDO, in particular, seems ill-equipped to take the lead on these issues given its past performance and lack of interest in a rights-based approach to civil defense and security.

A July 2022 report by the Russian cybersecurity firm Kaspersky[10] only hints at Iran's current state of cyber defensive capacity. According to the report, with over 35% of users attacked by mobile malware, Iran tops the list of countries with the largest share of mobile infections even before China.

In addition to deprioritizing network security in favor of censorship and centralization, Iran also suffers from a lack of expertise in the

[5] https://www.radiofarda.com/a/f35_oil_indu_fire_ladan_salami/28057862.html

[6] https://www.alef.ir/news/3980918054.html?show=text

[7] https://en.mehrnews.com/news/139158/Iran-could-turn-to-cryptocurrencies-to-evade-some-sanctions

[8] https://bit.ly/3zgOsiJ

[9] https://bit.ly/3Je7jj2

[10] https://securelist.com/it-threat-evolution-in-q1-2022-mobile-statistics/106589/

	COUNTRIES	%
1	**Iran**	**35.25**
2	**China**	**26.85**
3	**Yemen**	**21.23**
4	**Oman**	**19.01**
5	**Saudi Arabia**	**15.81**
6	**Algeria**	**13.89**
7	**Argentina**	**13.59**
8	**Brazil**	**10.80**
9	**Ecuador**	**10.64**
10	**Morocco**	**10.56**

cybersecurity field. There are a combination of factors at play, from the government agencies› challenge to compete with the private sector in attracting talents and a significant brain drain of the IT and cybersecurity fields over the past decade.[11] According to informed sources, the turnover rate within the private sector is so increasingly high that many of the best known brands have gone through three generations of engineers in just over two years. They continue to lose talent to companies in Europe, North America, and Australia.

As the nuclear negotiations between Iran and major world powers continue, the current geopolitical climate is likely to intensify. Iran's espionage and sabotage priorities (mostly against Israel) are unlikely to change significantly. But the contention between Iran and Israel will increasingly reflect in the shadow cyberwar, and civilian networks are expected to pay the price. The lack of investment and expertise in Iranian public sector will continue to make civilian networks and critical infrastructure susceptible to further blows unless structural changes are made to cybersecurity policy and practices.

These circumstances undermine Iran's long-standing promise of digital governance that can facilitate governmental affairs and serve citizens more effectively. Among the recent attacks, targeting of government agencies that deal with the media doubles the pressure

[11] https://asreertebat.com/?p=33699

on the civil society by extending wait times for licenses or approvals for cultural productions. Attacks on civilian networks – such as the one on gas stations – also exacerbate an already dire economic situation that has pushed many Iranians over the poverty line. Cyberattacks have never been so closely tied to economic and other human rights.

The Iranian government could address the situation by investing in cybersecurity and enhancing the resilience of civilian networks. However, much of the public investment has thus far gone to offensive capabilities to target the regime's adversaries and developing the National Information Network without much consideration for cybersecurity. Unless priorities are realigned, civilian networks and human rights will continue to suffer from extended hostilities between Iran and its rivals.

What is HackerWatch?

The present document is the first in a forthcoming series of HackerWatch reports in which we at Filterwatch aim to track malicious cyber activities of Iran as well as any blows to the country from other threat actors.

By following these developments, we hope to analyze Iran's ever-changing landscape of cyberspace, its rationality for related offensive and defensive activities, and the big picture of cyber escalation in the Middle East.

HackerWatch will be published biannually and present the most important developments of the preceding six months. The first report focuses on the first half of 2022.

The two major themes between last December and June 2022 include (1) Iran's continuation of targeting of diaspora organizations through phishing, impersonation, and defacements, and (2) escalation of hacktivist attacks targeting Iran and Israel, with each country accusing the other of orchestrating these activities.

As Iran continues to negotiate with world major powers over its nuclear program – and Israel remains in fierce opposition to any settlement with Iran– malicious cyber activities are on the rise as an extension of the geopolitical tensions between the two states.

Dec 2021

In December 2021, only days after Apache's warning about the Log4j vulnerability[12] – a coding framework used in various software applications and services – Iranian state hackers were detected to be exploiting Log4j against a variety of targets.[13] In particular, Advanced Persistent Threat (APT) 35,[14] also known as Charming Kitten, TA453, or Phosphorus, was actively using only basic open-source tools for the exploitation, suggesting that the group had rushed to leverage the vulnerability.

Filterwatch's research shows that civil society organizations were most susceptible to APT35 exploits, in particular those running older versions of VMWare (a cloud computing service) and web servers that were affected by the log4j vulnerability.

APT35 has a long history of using spyware, spear phishing, and social engineering for surveillance purposes. The group is affiliated with the Islamic Revolutionary Guard Corps (IRGC), Iran's revolutionary military organization with extensive power in almost all sectors of the country. While this was not the first time that Iranian threat actors attempted to undermine networks of civil society organizations, it indicates their agility to exploit even the most widely known vulnerabilities to their benefit.

Jan 2022

On January 27, an unknown hacking group briefly disrupted the broadcast of Channel1 of the state-owned broadcaster (IRIB)[15] to play images of leaders of Mujahedin-e-Khalq (MEK), an exiled opposition group that backs the overthrow of the Islamic Republic with a history of armed resistance. MEK has not officially claimed responsibility for the disruption. While it remained limited in scope and the media attention it garnered, it might have motivated the events that followed and affected an Iranian diaspora civil society organization.

On January 28, at least three websites affiliated with the

[12] https://logging.apache.org/log4j/2.x/security.html

[13] https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/

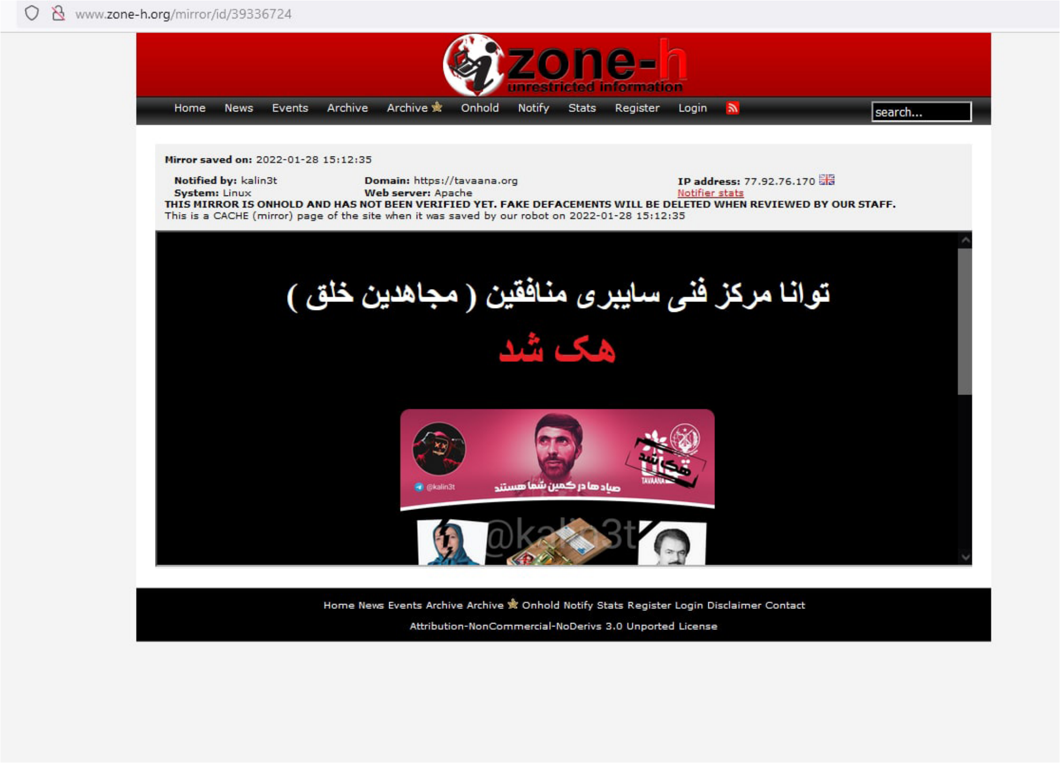
[14] https://www.cfr.org/cyber-operations/charming-kitten

[15] https://twitter.com/radiofarda_/status/1486679822856245250?s=21&t=LoFLjKLn6JM1-xBwdEjuhg

E-Collaborative for Civic Education (otherwise known as Tavaana) were defaced and displayed disparaging images of MEK leaders. The defacement announcement labeled Tavaana as the “technical center of MEK’s cyber operations,” claiming a link between Tavaana and the disruption in the national broadcast the day before. The announcement was also posted to Zone-H, a defacement forum, and promised to disclose identifying information about members of Tavaana (image 1). On February 6, a hacker who identified as Kalin3t posted on his Telegram channel[16] (kalin3t hacker) a minute-long video of registered Tavaana members. Their previous post from February 5 derided a MEK gathering and hinted at an upcoming MEK-linked data dump, which turned out to be personal information of Tavaana users.

For years, Iran has labeled most opposition groups as MEK regardless of their political orientation, activities, and history. Labeling Tavaana as MEK fits the same pattern.

Filterwatch’s research shows that in the runup to the Tavaana defacement and data leak at least two employees of the organization had gone public about being impersonated on Skype.


www.zone-h.org/mirror/id/39336724
zone-h
unrestricted information
Home News Events Archive Archive Onhold Notify Stats Register Login
search...
@kalin3t
صیاد ها در کمین شما هستند
هک شد
TAVAANA
@kalin3t
Home News Events Archive Archive Onhold Notify Stats Register Login Disclaimer Contact
Attribution-NonCommercial-NoDerivs 3.0 Unported License

Mirror saved on: 2022-01-28 15:12:35

Notified by: kalin3t
System: Linux
Domain: https://tavaana.org
Web server: Apache
IP address: 77.92.76.170
Notifier stats

THIS MIRROR IS ONHOLD AND HAS NOT BEEN VERIFIED YET. FAKE DEFACEMENTS WILL BE DELETED WHEN REVIEWED BY OUR STAFF.
This is a CACHE (mirror) page of the site when it was saved by our robot on 2022-01-28 15:12:35

توانا مرکز فنی سایبری منافقین (مجاهدین خلق)

هک شد

Image 1. Tavaana defacement announcement on Zone-H, January 28, 2022.

[16] https://t.me/kalin3t

They warned about fake accounts that were befriending their contacts, seeking to collect phone numbers and/or bank account information and distributing malicious files. It is unclear if these incidents were linked to the Tavaana hack that followed, nor is there sufficient information to link these impersonations and Kalin3t and his Telegram channel.

Tavaana was not the only target of Iranian hackers on January 28. A hacking group called Moses Staff published video footage of street CCTV cameras from around Israel on their website.[17] The announcement, titled “We see you with your eyes...,” claimed that the footage was but one part of a larger surveillance operation targeting the Israeli security apparatus. It went on to reiterate an old Iranian threat to strike Israel with a surprise attack. Fars News Agency, a news outlet affiliated with the IRGC, published an article about the incident and attributed it to Moses Staff with no further information about the hacking group, its structure, or affiliation.[18]

In November, Fars News had covered other hacking activities of Moses Staff, including the hacking of 3D maps and images of Israel’s critical infrastructure, the leak of financial documents of three Israeli engineering firms,[19] and the alleged breach of Israel’s Defense

Image 2. Moses Staff announced the hacking of Israeli CCTV cameras.

[17] https://moses-staff.se/we-see-with-your-eyes/

[18] https://bit.ly/3IAr4ka

[19] https://bit.ly/3z14VIQ

Ministry and leak of personal information of military personnel and other confidential correspondence.[20]

Israeli cybersecurity firm Cybereason has speculated about the Iranian origin of Moses Staff due to the ideological cues and its alignment with the geopolitical interests of the Islamic Republic.[21]

March 2022

On March 14, only a week before the Iranian new year holidays, a self-proclaimed hacktivist group titled قیام تا سرنگونی (Persian for Revolt To Overthrow, hereafter R2O) announced on Twitter that it had defaced 62 domains affiliated with Iran's Ministry of Culture and Islamic Guidance, and shut down 77 web servers and 280 computer devices.[22]

Similar to the brief hack of IRIB's Channel 1 in January, these domains displayed pictures of MEK leaders with derogatory language toward Ayatollah Khamenei, Iran's Supreme Leader. Iranian Student News Agency (ISNA) was first to publicize the attack but said that no Ministry official had confirmed the incident yet.[23]

On the same day, a wave of Distributed Denial of Service (DDoS) attacks hit a number of Israeli government websites using the «.gov.il» domain, including ministries of health, justice, welfare, and the prime minister's office.[24]

A hacking group called BlackShadow, with previous attempts at ransomware,[25] claimed responsibility for the attack. The group had previously struck Israeli companies, including a web hosting site and a LGBTQ dating application,[26] in alleged retaliation for hacking of Iran's gas pumps in October 2021 that paralyzed the country's 4,300 gas stations and took a dozen days to have service fully restored. That

[20] https://bit.ly/3o1YwH6

[21] https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations#:~:text=Over%20the%20past%20months%2C%20the,by%20leaking%20sensitive%2C%20stolen%20data.

[22] https://twitter.com/GhiamSarnegouni/status/1503259362944507907

[23] https://bit.ly/3NYK4dq

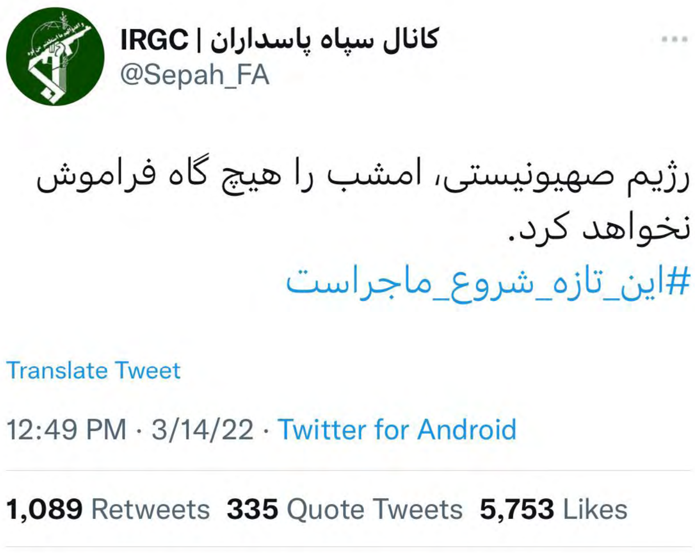
[24] https://www.haaretz.com/israel-news/tech-news/2022-03-15/ty-article/.premium/cyber-attack-on-israel-biggest-attack-ever-or-iranian-propaganda/00000180-5bba-db1e-a1d4-dffbfa970000

[25] https://securityaffairs.co/wordpress/124000/hacking/black-shadow-hacked-cyberserve.html

[26] https://www.cyberscoop.com/hack-and-leak-group-black-shadow-keeps-targeting-israeli-victims/

attack was attributed to Israel by two U.S. defense officials.[27]

Shortly before the .il websites hack was announced, the Twitter account of IRGC cryptically threatened that “the Zionist regime would never forget this night,” followed by an intimidating sounding hashtag #ThisIsJustTheBeginning. Within minutes, pro-IRGC accounts started promoting that tweet, announcing the hacking of .il domain websites even before the Israeli government went public with it. These pro-IRGC accounts referred to the hacking incident as “the first blow,” suggesting that there was more to expect.[28] That same night, the IRGC announced the arrest of a Mossad ring leader that was allegedly plotting a sabotage operation in the Fordow facility, one of Iran’s main nuclear sites.[29]



IRGC | کانال سپاه پاسداران
@Sepah_FA

رژیم صهیونیستی، امشب را هیچ گاه فراموش
نخواهد کرد.
#این_تازه_شروع_ماجراست

Translate Tweet

12:49 PM · 3/14/22 · Twitter for Android

1,089 Retweets 335 Quote Tweets 5,753 Likes

Image 3. IRGC’s tweet on the night of .il websites hacking

April 2022

On April 25, for the first time since it hacked Iran’s Ministry of Culture in March, Revolt to Overthrow (R2O) made a comeback. This time it targeted over 49 domains affiliated with Iran’s Ministry of Agriculture. Defaced websites showed, once again, images of MEK leaders and wished Khamenei dead.[30] Furthermore, R2O started to

[27] cf1.

[28] https://twitter.com/matinmoraveji/status/1503428748418375683?s=21&t=ylr8F37pYsiE4MB4tjRmDQ

[29] https://twitter.com/sepah_fa/status/1503432110404784134?s=21&t=ylr8F37pYsiE4MB4tjRmDQ

[30] https://twitter.com/ghiamsarnegouni/status/1518500745406029825?s=21&t=u-ib7_STQ6XC7zLASdUNYQ

leak documents that were reportedly obtained from the breached networks of the Ministry of Agriculture.[31]

The attack was allegedly in reaction to the suppression of farmer protesters in Isfahan province. The peaceful protests first emerged in November 2021 and were met with violence by the state's security forces. In April 2022, at least two rounds of protests were reported demanding accountability for local authorities for mismanagement of water resources that has affected agriculture across the province.

June 2022

R2O marched on in June. This time the group targeted the website and SMS portal of Tehran municipality and over 50,000 CCTV cameras from around the city,[32] including the shrine of Rouhollah Khomeini, the founder of the Islamic Revolution.[33] These attacks happened on the public holiday of June 2nd, the passing anniversary of Khomeini. Similar to the two previous attacks, the announcement showed images of MEK leaders and subversive anti-regime messages.

Iranian media covered the incident, some quoting the municipality officials accusing the Mossad for the hack.[34] Two weeks later, Fars News Agency claimed that at least one individual with alleged affiliations with foreign intelligence services was arrested in connection to the municipality hack.[35] FilterWatch has obtained a threat intelligence document prepared for Tehran municipality in the aftermath of this attack that elaborates on the details of a wiper malware.

It should be noted that the repeated use of MEK as cover in the past few incidents has been unconvincing. This is in large part due to the group's limited known cyber capabilities, lack of history of causing similar disruptions, and the scope of recent exploitations. MEK itself has not claimed credit for these attacks.

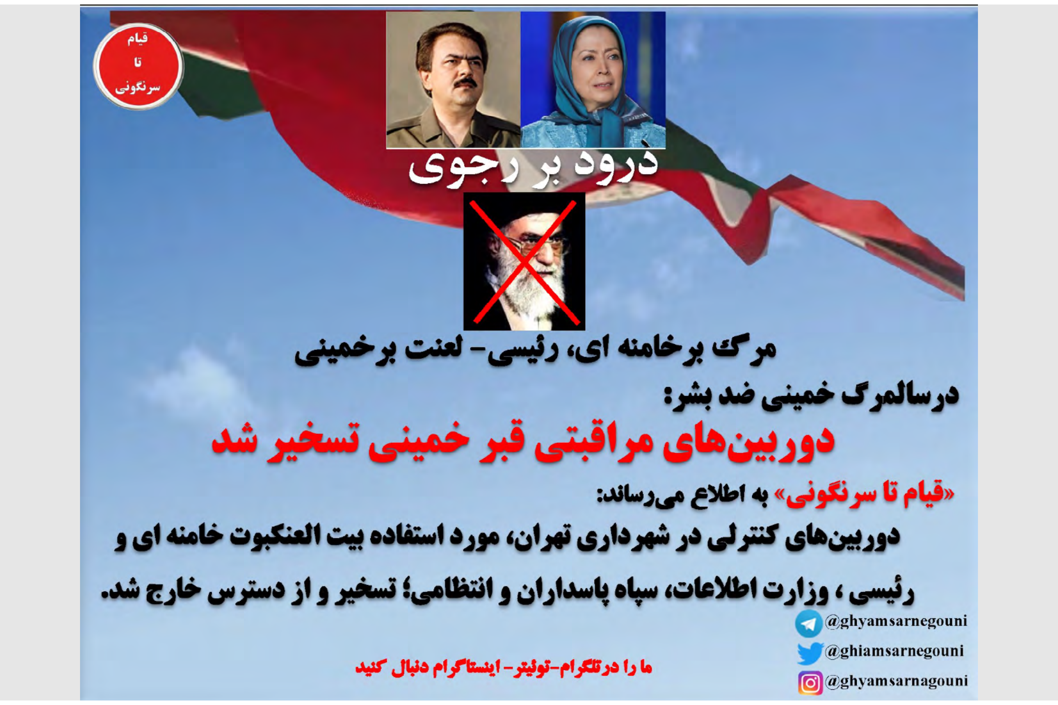
[31] https://twitter.com/GhiamSarnegouni/status/1518544409268211713

[32] https://twitter.com/ghiamsarnegouni/status/1532396522171777027?s=21&t=uwHhq95PmXaBvQFFR17qeg

[33] https://twitter.com/ghiamsarnegouni/status/1532276891100532738?s=21&t=R860snG2h_T-sAzvCbiiVg

[34] https://bit.ly/3zjedjH

[35] https://bit.ly/3cf8PEX



مرگ برخامنه ای، رئیسی- لعنت برخمینی

درسالمرگ خمینی ضد بشر:

دوربین‌های مراقبتی قبر خمینی تسخیر شد

«قیام تا سرنگونی» به اطلاع می‌رساند:

دوربین‌های کنترلی در شهرداری تهران، مورد استفاده بیت العنکبوت خامنه ای و
رئیسی ، وزارت اطلاعات، سپاه پاسداران و انتظامی؛ تسخیر و از دسترس خارج شد.

@ghyamsarnegouni
@ghiamsarnegouni
@ghyamsarnagouni

ما را درتلگرام-توئیتر- اینستاگرام دنبال کنید

Image 4. Hacking announcement of Tehran municipality, June 2.
Source: Twitter account of R2O.

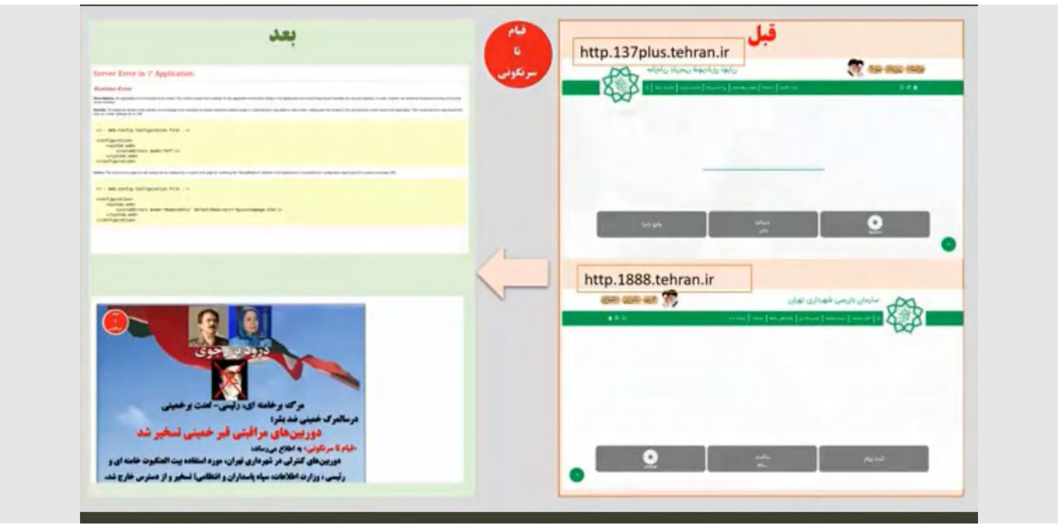
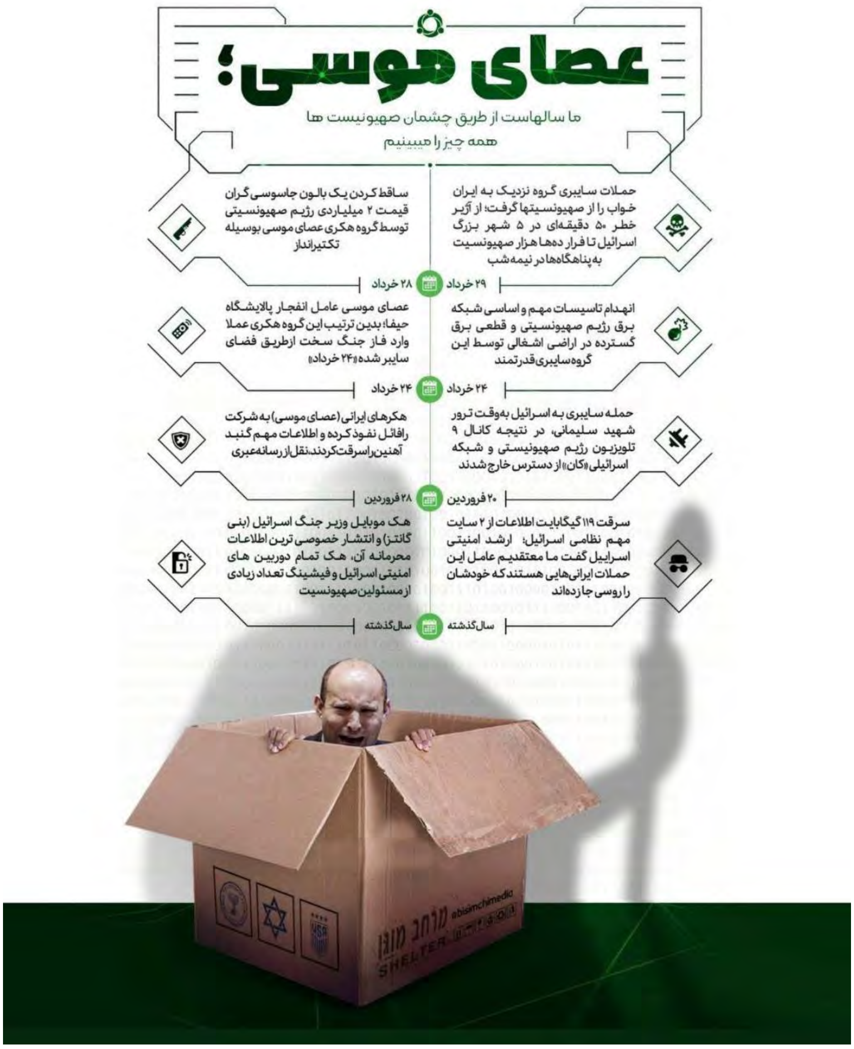


Image 5. The website of Tehran municipality before and after the R2O hack
Source: R2O on Twitter.

In response, Moses Staff returned with a new attack on at least three Israeli power and energy companies, including Israel Electric Corporation (IEC).[36]

On June 15, the group which had previously hacked Israel’s CCTV cameras, announced that the attack was “just the beginning,”

[36] https://moses-staff.se/israeli-power-companies/



عصای موسی؛

ما سالهاست از طریق چشمان صهیونیست ها

همه چیز را میبینیم

۲۹ خرداد

حملات سایبری گروه نزدیک به ایران
خواب را از صهیونسیتها گرفت؛ از آژیر
خطر ۵۰ دقیقه‌ای در ۵ شهر بزرگ
اسرائیل تا فرار ده‌ها هزار صهیونسیت
به‌پناهگاه‌ها در نیمه‌شب

۲۸ خرداد

ساقط کردن یک بالون جاسوسی گران
قیمت ۲ میلیاردی رژیم صهیونسیتی
توسط گروه هکری عصای موسی بوسیله
تکتیرانداز

۲۴ خرداد

انهدام تاسیسات مهم و اساسی شبکه
برق رژیم صهیونسیتی و قطعی برق
گسترده در اراضی اشغالی توسط این
گروه‌سایبری‌قدرتمند

۲۴ خرداد

عصای موسی عامل انفجار پالایشگاه
حیفا؛ بدین ترتیب این گروه هکری عملا
وارد فاز جنگ سخت ازطریق فضای
سایبر شده«۲۴ خرداد»

۲۰ فروردین

حمله سایبری به اسرائیل به‌وقت ترور
شهید سلیمانی، در نتیجه کانال ۹
تلویزیون رژیم صهیونیستی و شبکه
اسرائیلی«کان» از دسترس خارج شدند

۲۸ فروردین

هکرهای ایرانی (عصای موسی) به شرکت
رافائل نفوذ کرده و اطلاعات مهم گنبد
آهنین‌را‌سرقت‌کردند.نقل‌از‌رسانه‌عبری

سال‌گذشته

سرقت ۱۱۹ گیگابایت اطلاعات از ۲ سایت
مهم نظامی اسرائیل؛ ارشد امنیتی
اسراییل گفت ما معتقدیم عامل این
حملات ایرانی‌هایی هستند که خودشان
را روسی جا زده‌اند

سال‌گذشته

هک موبایل وزیر جنگ اسرائیل (بنی
گانتز) و انتشار خصوصی ترین اطلاعات
محرمانه آن، هک تمام دوربین های
امنیتی اسرائیل و فیشینگ تعداد زیادی
از مسئولین صهیونسیت

Image 6. A summary of the Moses Staff cyber attacks on Israeli targets, distributed by a group of pro-regime Twitter accounts in June 2022.

promising many more attacks to follow.[37] A week later, Moses Staff published alleged phone numbers of three high ranking Israeli defense authorities, including the IDF's spokesperson.[38] A separate attack also targeted municipal alert systems that activated rocket sirens in Jerusalem and Eilat but did not breach essential IDF infrastructure, according to Israeli media.[39]

In a matter of days, it was Iran's turn to suffer a retaliatory blow. On June 27, hacking group Gonjeshk-e-Darandeh claimed responsibility for a sabotage attack on Iran's steel conglomerate, causing physical

[37] https://twitter.com/staffofmoses1/status/1539594882620297216?s=21&t=IXOXImGJRQGEitpUeeJe1Q

[38] https://twitter.com/staffofmoses1/status/1539591537453146112?s=21&t=HZbvjrnfvIGzRy8DseECQQ

[39] https://www.israeltoday.co.il/read/iranian-cyber-attackers-trying-and-so-far-failing-to-create-panic-in-israel/

damage to machines as captured by hacked security cameras.[40]

The group announced that the hack was in retaliation for Iran's aggressions and that targeted companies were operating despite international sanctions on them. Iranian authorities claimed that the damage was limited and to have already contained the threat. The group had previously attacked Iran gas pumps,[41] national railways,[42] and the Ministry of Housing and Urban Design.[43]

On June 28, over 20 Israeli agencies, hotels, and resorts were hacked, including hotels4u.co.il, hotels.co.il, isrotel.com, minihotel.co.il, trivago.co.il and danhotels.com. An Iranian hacking group Sharp Boys (presumably a play on the American Proud Boys[44]) took responsibility for the attack and leaked the personal information of over 300,000 Israelis that it had obtained through Israeli travel booking sites. This information included ID numbers, addresses, credit card information and more.[45]

Previously in December 2021, Sharp Boys hacked two Israeli hiking websites and leaked personal information of over 100,000 users, including emails, addresses, photos, and phone numbers. The group then offered the information of three more million people for sale, without specifically asking for ransom.[46]

Conclusion

The first half of 2022 brimmed with so-called hacktivist cyber attacks aligned with the geopolitical interests of two Middle Eastern rivals: Iran and Israel. The increasing frequency, scope, and variety of targets of these attacks stand out. While each state has accused the other for these subversive activities, no official attribution has been made. However, technical analyses point to Iran for the activities of

[40] https://t.me/GonjeshkeDarand/20

[41] https://twitter.com/gonjeshkedarand/status/1452992555361214474?s=21&t=h7MR0r1rxV9dUW9utmxHCw

[42] https://twitter.com/gonjeshkedarand/status/1452876401804288001?s=21&t=h7MR0r1rxV9dUW9utmxHCw

[43] https://twitter.com/gonjeshkedarand/status/1452879508214886406?s=21&t=h7MR0r1rxV9dUW9utmxHCw

[44] https://www.splcenter.org/fighting-hate/extremist-files/group/proud-boys

[45] https://m.jpost.com/israel-news/article-710973/amp

[46] https://m.jpost.com/business-and-innovation/tech/hackers-attack-israeli-hiking-websites-leak-personal-information-689128/amp

BlackShadow and Moses Staff hacking groups. Attribution of attacks on Iranian institutions is less clear, but at least two U.S. officials have confirmed, according to The New York Times, that Israel was behind Gonjeshk-e-Darandeh's attack on gas pumps. These cues paint a complex picture of escalatory intelligence and sabotage operations in and through cyberspace that correspond to the growing tension between the two countries.

While the international community seeks a diplomatic solution to Iran's nuclear program, Israel continues to voice concern about the prospect of a nuclear Iran for the region and the world. Iran in response continues to blame Israel for undermining negotiations and threatens to take a 'hard revenge.' These low-level cyber tit-for-tats offer a less costly alternative to the possibility of severely consequential use of force between the two states. For now, the main function of these attacks is signaling or creating some form of deterrence.

Thus far, the attacks on Iranian institutions have been more systematic and coherent. The combination of sabotage and espionage suggests a possible involvement of intelligence agencies in the design and execution of recent events against Iranian agencies. The consistent use of Mujahedin-e-Khalq as a front indicates that whoever is behind these attacks has a well-informed understanding of Iranian opposition and the state's position and propaganda toward them. Yet the unconvincing MEK cover carries severe implications for civil and political liberties in Iran. It perpetuates the state's views of opposition groups as existential threats and perpetuates the cycle of suppression against civil dissent. This in turn prompts Iran's own cyber attacks on civil society organizations, as we have already seen this year with the case of Tavaana.

In contrast, attacks on Israeli networks have indicated less sophistication, mainly focusing on disruption and prompting public panic (e.g. activating sirens, hacking CCTV cameras). However, Iranian state hackers have repeatedly proved persistent in evolving their tactics and finding new vulnerabilities for exploitation in future attacks. As negotiations over Iran's nuclear program continue and tensions with Israel grow, similar retaliatory incidents are likely to expand and evolve. Most importantly, such tit-for-tats in the cyber domain affect average citizens and undermine human rights on different levels. Iran's civilian networks will likely remain susceptible to cyber attacks given the lack of expertise and priority to secure these networks. We will continue to cover these developments in the next issues of HackerWatch.