

Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks

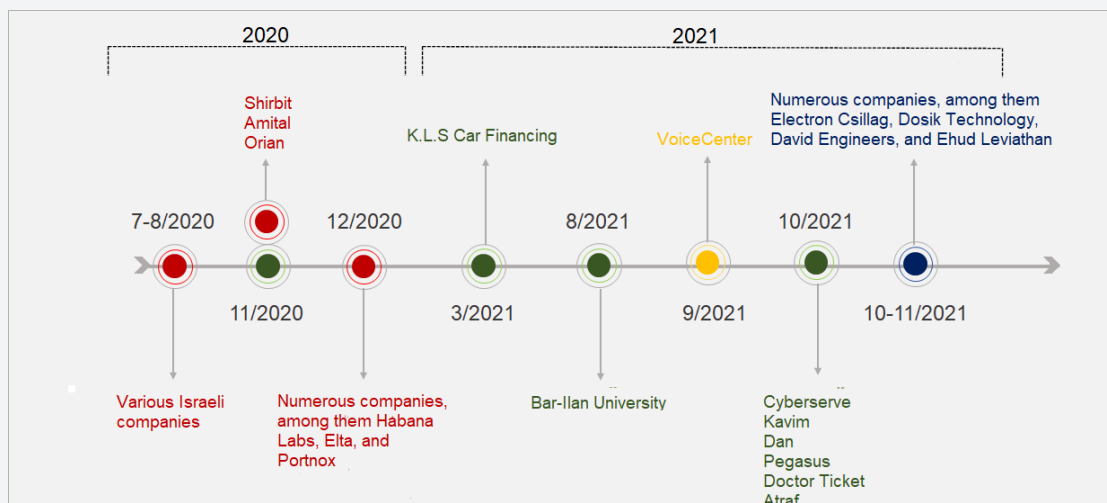
Boaz Dolev and David Siman-Tov | January 27, 2022

The past two years have witnessed cyberattacks attributed to Iran targeting companies and organizations in Israel that are ostensibly ransomware, but in fact are undertaken as influence operations. Notably, ransomware attacks have been very common in recent years, and have been defined by the White House as a central cyber threat. Still, the use of ransomware attacks for the purpose of influence operations rather than for an economic purpose is a singular phenomenon. This phenomenon is unique to the framework of the conflict between Israel and Iran or its supporters. The following article describes the results of research on ransomware attacks from the past two years that targeted the Israeli private sector with an influence operations purpose. The basis of attributing the attacks to an organized Iranian array will be elaborated, as well as methods of distinguishing imitated ransomware attacks, the Iranian groups involved alongside their tools, strategic insights, and possible ways of coping with the phenomenon. The described research was carried out by the ClearSky Cyber Security company for the Institute for National Security Studies (INSS). ClearSky cooperated with researchers from the field of psychological operations warfare and from the Iran program at INSS.

The year 2020 was a turning point regarding the nature of Iranian activity in the Israeli cyber realm. Over the previous decade, the Iranians mainly carried out operations for the purpose of espionage, while psychological operations like fake news sites were seldom observed. Cyberattacks with destructive purposes attributed to Iran were mostly carried out against other countries, including Saudi Arabia. In an unusual event, such an attack was also carried out against Israel in 2020, targeting water facilities. 2020 was the first year in which ransomware attacks began for an influence operations purpose. It appears that companies are targeted when opportunities present themselves, rather than according to a set plan.

Once an attack is made public, and as a function of the Israeli media's response, the Iranians leverage the stolen information in accordance with Israeli characteristics and contexts. For example, the attack on the Shirbit insurance company was leveraged with regard to privacy, with an emphasis on connections to the security establishment; the centrality of the website Atraf was leveraged with regard to the privacy of the LGBT community; the attack targeting Habana Labs, associated with Intel, was leveraged with regard to technological superiority, as were the attacks targeting companies from the security sector such as Israel Aerospace Industries.

The timeline below presents the dates of the attacks, the names of the attack groups, and the organizations that were attacked and publicized by the attackers. Clearly the attacks are consistent and carried out in waves. The period of time between the attacks is apparently used to learn from experience and develop new tools.



The strategic change is that attacks are intended to pressure the public, and thereby influence decision makers and the conflict underway between Israel and Iran in several contexts. These include the campaign between wars against Iranian elements in Syria, the maritime arena, or cyberattacks attributed to Israel and the West on civilian governmental sectors in Iran. The rise in cyberattacks for ransomware purposes also harms the country's economy and citizens' confidence in leading companies. In light of the information leaked after Shirbit was breached, the chairman of the Capital Market Authority decided to impose a fine of over 10 million shekels on the insurance company due to significant violations by the supervisor of cyber risk management.

It seems that Iran has identified a soft underbelly in Israel – the cyber security systems of the private/business sector. Attacking private business organizations

enables Iran to operate relatively freely and score a dual achievement – one with respect to Israel's citizens and decision makers; the other internal, as a demonstrated response to the cyberattacks that disrupted daily life in Iran. Even though the Iranian attacks are not technically sophisticated, some of them are successful enough to represent influence operations. Their success stems from a low level of security and insufficient awareness of the need to invest in cyber defense of the civilian private sector in Israel, as well as the considerable attention in the Israeli media to the attacks.

The proliferation of ransomware attacks worldwide and their recurrence in recent years has prompted the US administration to define such attacks as a central threat that must be addressed. The White House announced the establishment of a task force to coordinate defensive and offensive measures against ransomware attacks, and it is responsible for continuously updating the White House on the implementation of a national campaign against ransomware operations. Another effort in dealing with the phenomenon is the decision by the US State Department to pay a \$10 million reward for information that leads to identifying cybercrimes.

Overview of the Attacks

In early 2021, one of the biggest espionage systems carried out by the Iranian attack group called Fox Kitten was exposed. In the cyberattack, which lasted for about two years, the Iranians succeeded in penetrating the computer networks of a large number of companies in Israel, pervading internal networks, and gathering sensitive information of various levels of interest. After the system was exposed, the group changed its approach in two ways: first it tried to sell the access to the victims that it achieved in Israel and the world on the darknet, and afterwards began a new pattern of attack: ransomware attacks for influence operations purposes.

Over the past two years this group penetrated dozens of companies in Israel with a singular ransomware attack, working as a "classic" ransomware group: computers were encrypted, emails for the purpose of extortion were sent, money was transferred, and keys for opening the encryption (which did not always work) were provided. The only deviation from the expected behavior of a ransomware group was the incendiary language that the attacker used with the attacked.

In November 2020, the group began to combine ransomware attacks with influence operations attacks. In these attacks, the group broke into and encrypted networks and computers in many organizations, while leaking documents from previous and current attacks on its Twitter and Telegram accounts. The group repeatedly made threats to Israel on social media, and even created a special

website for leaking materials from Israeli companies, saying, "Winter is coming for Israel." As a result, the attack was publicized in the Israeli media and received considerable attention on social media.

Since November 2020, there have been a wave of different cyberattacks that incorporated all the previous capabilities and trends: the goal of the attack was influence operations, while using ransomware methods, with the leaked files sometimes indicating that the attackers had penetrated the computers of the attacked organizations for the purpose of espionage much earlier. These attacks have a high media and internet profile: the attacks are characterized by a determined attempt to command headlines in central media outlets in Israel, with the aim in part of sowing fear and embarrassment in the public consciousness.

The attacks are carried out by several groups disguising themselves as ransomware groups and calling themselves changing names, such as Pay2Key, BlackShadow, and NetWorm. The attackers penetrate companies and organizations and steal information, after having entrenched themselves in these targets over the course of many months. But unlike in the past, in addition to stealing information, the attacks also include leaking, encrypting, or deleting information and engaging in negotiations with the victim that are as publicized as much as possible, demanding ransom in return for the release of the encryption and/or in order to prevent additional stolen information from being leaked to the internet.

The information leaks are routed mainly to the Twitter and Telegram social networks, and to darknet leak sites under Onion. The attack that received the most extensive media coverage in this wave was against Shirbit, in which the personal information of many customers was leaked. The attackers tagged media outlets abroad and contacted media outlets directly so that they would make contact with them. Later, the attackers published embarrassing materials from the negotiations that took place with the Shirbit management. While disguised as ransomware attacks, the behavior of the attackers indicates that money does not seem to have been their top priority, and they are especially interested in the psychological effect.

Linking the Attackers to Iran

Identifying the attackers and their affiliation is done by examining the following parameters – behavior, attack targets, tools, infrastructure and language.¹

Behavior:

The behavior of the Iranian "ostensible ransomware" groups differentiates them from regular ransomware groups, and indicates that the essential aim is influence operations and not profit.

- a. The names of the entities: the names of the entities appear, disappear, and change in almost every operation. It is very important to professional ransomware groups to maintain their reputation, and thus they keep their names so that people will know what their "portfolio" includes.
- b. Not maintaining a reputation: financial ransomware groups build and maintain their reputations in several spheres – negotiations protocol and fairness toward those paying the ransom; an encryption key that really works; deleting the stolen files and not publicizing them; technical support if necessary. None of these take place during an attack by a group with an influence operations motive.
- c. Lack of discretion: professional ransomware groups first contact their victims for the purpose of discreet negotiations, usually through a ransom letter that includes how to contact them. Only if the negotiations break down or if contact is not made do they publicize the breach and leak stolen documents. In the Iranian ostensible ransomware influence operations campaigns, the attackers first publicize the hack and the stolen items on the internet before they contact the victim for the purpose of financial negotiation.
- d. Involving the media: in addition to the timing of publication, the Iranian influence operations attackers tag media outlets, and it seems that they desire primarily maximum media exposure. It is the media exposure that is significant and not the money.
- e. Flexibility in negotiations: the Iranian attackers are not willing to negotiate prices, present uncompromising ultimatums, and publicize stolen materials without waiting for the ransom. This contrasts with professional ransomware groups, which engage in discreet, serious negotiations with some flexibility, as long as the victim communicates, in order to increase the chances of profit.

¹ This is a version and extension of the TTP model used for identifying attackers and their affiliation in the professional literature: analyzing and comparing tactics, techniques, and procedures is used to characterize the behavior of attackers in both the physical world and in the cyber realm.

- f. Credibility: at least in some of the cases in the Iranian campaigns, the victims transferred money and the encrypted information was not restored. This behavior does not characterize professional ransomware groups, as it damages their reputation and sabotages their chances of receiving the ransom in future attacks.
- g. Communication style: when a professional ransomware group negotiates, the whole conversation takes place in an even and service-provider tone, as if it was customer service (often the attackers also refer to themselves as "support"). In the ostensible ransomware attacks attributed to Iran, the tone of speech is callous, forceful, and condescending.
- h. The timeliness of the leaked information: financial ransomware groups attack an organization at a certain point in time. The documents that they leak if the ransom is not paid belong to that time. The Iranian ostensible ransomware groups leaked old documents that sometimes belong to information stolen up to two years before they were publicized. This means that materials were used from attacks whose aim was espionage, and when the aim became influence operations, they were publicized in order to bring about considerable media exposure. An example of this is the leak of information from Israel Aerospace Industries.

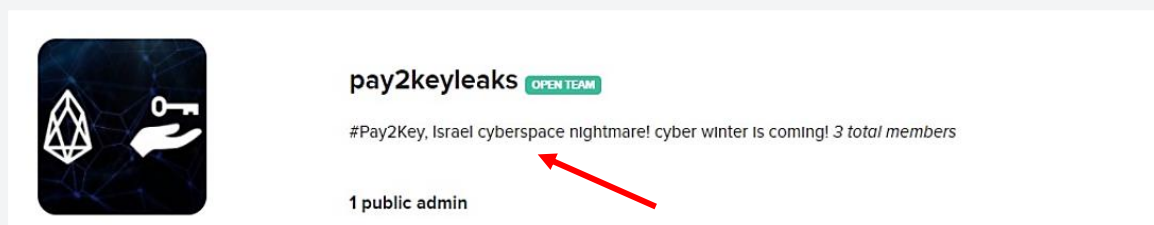


Screen shot publicized by the group Pay2Key: The language is informal and not businesslike – the language of waging an internet campaign and not the language of a ransom deal

Attack Targets

Professional ransomware groups usually focus on a certain sector: e.g., banks, hospitals, financial institutions – regardless of geography. Certain groups refrain from attacking a specific geographical region, for example, Russian ransomware groups that attack only countries that are not former Soviet countries. In terms of the target of the attack, it seems that the attack targets of the ransomware groups are identified in advance, in order to receive the maximum profit from them.

Most of the victims affected by the influence operations campaign are Israeli medium and small companies. The attack method used by the Iranians in order to locate these companies and penetrate them is at first a wide scan of a range of Israeli internet addresses for the purpose of locating their servers, through which the networks of these companies can be hacked. Next the attackers maintain a list of IP addresses and organizations that can be penetrated by exploiting the weakness. They plant tools in the vulnerable systems ("back doors") through which they will be able to attack the companies again. This pattern indicates that the attackers do not usually mark a target and attack it, but rather exploit opportunities. In some cases the attackers choose to carry out quiet espionage activity, without publicity. At the same time, they select and attack organizations that they believe will help attract widespread media attention. The ability of the organizations to pay the ransom is not a central factor, as the profit that they seek is influence operations currency and not financial.



Example of an overt statement against Israel on the leak website of the group Pay2Key on the social network KeyBase

Tools

Cyber attackers use a variety of tools for penetrating an organization, achieving a foothold and consolidating their grip, and later for using spyware or ransomware, in accordance with the purpose of the attack. Some of these tools are well-known, based on open, public, and legitimate code; some are illegal tools that are available on the internet; and some are developed by the attackers.

The public tools based on open code are less unique to a specific attacker, but here too one can see a tendency of a specific attacker to use certain tools more than others. Independently developed unique tools serve as a strong indication of

a campaign's affiliation with a certain attacker. These tools constitute the attacker's fingerprint. Tracking independently-developed unique tools enables comparing tools, code snippets, text chains, and unique names of variables that recur from one campaign to another. Sometimes it is possible to track the upgrades of the tool between different attack operations and thus to attribute several attacks to one attacker. In each attack there is the possibility of using new, different, or unique tools, but developing or using new tools requires training on the new tools and thus a need for greater resources, in both time and money. Consequently, attackers reuse the same tools and thus one can track them and attribute campaigns to them with high probability.

To attribute the influence operations campaign in question to a certain attacker, the tools used during the attacks are mapped. Analyzing the tools in most attacks helps assess that those behind the attacks are Iranian. The map of the tools used and their attribution to attack groups appears in Table 1.

In order to demonstrate how the attribution is made via attack tools, we chose to focus on one tool – a malware program called IPSecHelper, which enables "back door" access to the attacked server and through it remote management of the attack. The tool was operated by a group called BlackShadow. Other tools of the group were analyzed in reports by the companies SentinelOne and Cyberpunkleigh.² Another study including an analysis of the tools and infrastructure of another group that operated as part of the campaign, called Kitten Fox, can be found on a blog on the website ClearSky.³

The SentinelOne report documents the Wiper malware program called DEADWOOD that was found in Shirbit systems as well as in the fuel company of the United Arab Emirates in an older version a year ago. The report describes the direct connection between the malware programs and the changes made in the versions. The SentinelOne report does not describe the changes made in the malware program IPSecHelper. Version 1.5 of IPSecHelper appeared on VirusTotal in August 2019:

² <https://assets.sentinelone.com/sentinellabs/evol-agrius>
<https://cyberpunkleigh.wordpress.com/2021/05/27/apostle-ransomware-analysis/>

³ <https://www.clearskysec.com/pay2kitten/>

History ⓘ	
Creation Time	2019-03-11 12:21:50
First Submission	2019-08-24 10:15:41
Last Submission	2019-08-24 10:15:41
Last Analysis	2021-05-30 20:32:48

The Wiper found in the United Arab Emirates appeared on VirusTotal in June 2019:

History ⓘ	
Creation Time	2019-06-20 11:58:42
First Seen In The Wild	2018-07-07 00:50:33
First Submission	2019-06-22 07:33:43
Last Submission	2019-06-22 07:33:43
Last Analysis	2021-05-30 19:15:31

The file appears in a report⁴ by CERT from the United Arab Emirates under the name DEADWOOD WIPER. The report was published in July 2019:

Advanced Notification of Wiper Malware DEADWOOD

CERT Computer Emergency Response Team

Security Advisory: ADV-19-34 Criticality: High ○○○○●

Advisory Released On: 09 July 2019

Impact

Due to the understanding that the attackers use the DEADWOOD malware along with IPsecHelper, a possible link was examined between the dates the files were uploaded to VirusTotal and the CERT publications from the United Arab Emirates. The proximity of the dates also matches the version updates. It is estimated with medium probability that the version IPsecHelper 1.5-xml is the first version of the attackers that was used in the attack on the oil company in the United Arab Emirates. The version viewed on Shirbit is an update of the first version.

Attribution to Specific Attack Groups

Table 1 summarizes tools and additional characteristics that help ClearSky researchers attribute Iranian influence operations attacks to known groups. While the attribution to the Iranian influence operations campaign is at a high level of certainty, the internal division is only for our convenience and does not necessarily reflect the organizational structure on the other side.

⁴ <https://www.tra.gov.ae/assets/ZTwpCOI3.pdf.aspx>

Infrastructure

Infrastructure that the attackers use helps attribute the campaigns to the same entity, or at least to see cooperation between different entities. In some cases they can be linked definitively to Iran: IP addresses and servers that belong to Iran; IP addresses, servers, or storage and domain listing services outside of Iran that were used in other Iranian attacks; and so on. In the Pay2Key and NetWorm ransomware attack, Checkpoint checked the wallet number that victims were ordered to transfer the ransom to in the form of a bitcoin payment. This check led to an Iranian cryptocurrency exchange, registration for which requires the presentation of an Iranian ID number and an Iranian phone number.



Graph from a Checkpoint study tracking the path of the money

Language

The language that the attackers use in the negotiations to receive ransom or in statements in various communications media can betray their origin and provide further confirmation of the entity behind the attack.

In the influence operations attacks in the past year, as in real ransomware attacks, the attackers communicated with the attacked in English: in statements received as a Readme file or in the form of a desktop background, and in negotiations over ransom with the representatives of the attacked. In addition they communicate in English on internet sites – both darknet and regular – and on Twitter, Telegram, and other media, in order to take pride in their actions and to locate potential customers for the leaked information.

In some cases there are not enough mistakes in English to figure out the mother tongue of the attackers, but the majority of the attackers in the influence operations campaigns make enough mistakes to enable identifying language mistakes or irregularities that are characteristic of Persian speakers. For example, these include mistakes in definiteness and indefiniteness (the articles "the" and "a," respectively) and singular-plural, with patterns that match Persian syntax.⁵ The use of prepositions in phrasal verbs is the characteristic that most clearly betrays non-native speakers, even in languages that they speak well. The mistaken prepositions can also indicate the source language. Mistakes in other characteristic areas but without mistakes in the use of perfect verb forms in English (e.g., we have encrypted), are also an Iranian characteristic. The level of the English and the number of mistakes (even the kind of mistakes) also vary within the texts of the same attacker, apparently because these are groups in which different members represent it in different media. But in almost all of them the mistakes indicate Persian as the mother tongue.

Sometimes, in fact, there is no need to guess: in attacks on Iran researchers in academia, the attackers sometimes wrote in Persian, which was at a native-speaker level. In making personal contact it was possible to identify a similar style among figures. It was also possible to identify the use of consistent transcription, which indicates a single attacker operating several figures. In one of the Gmail accounts that were hijacked and restored, the attackers changed the interface language of Google to Persian; in a Pay2Key attack by FoxKitten, which was discovered in 2020, infrastructure was found with names in Persian, such as citrix@kharpedar webshel. The meaning of the word kharpedar is "son of a donkey;" in one of the code snippets studied by ClearSky, documentation clips – explanations of the program's code in human language – were discovered in Penglish (Persian in English letters), and in "division of labor" documents that we accessed, typical Iranian names appeared, as well as Penglish spellings of names such as amrica.

⁵ Mistakes in definiteness are also characteristic of speakers of Russian and East Asian languages; the latter also make mistakes in singular-plural. But each has a unique pattern of mistakes. Mistakes in definiteness that are typical of Persian syntax include, for example, omission of the definite article "the" but usually proper use of the indefinite article "a," except in nominal sentences, in which it is omitted (for example "I am professional"). In addition are the use of the singular instead of plural when it comes to a collective noun (whose number is not important), or overcorrection – the use of the plural form in places where English uses the singular with a collective meaning.

Table 1. Breakdown of the attacks on civilian organizations and companies in Israel

Attacker	Dates	Targets (victims / objectives)	Characteristic tools used for attribution	
			Public (legitimate or not)	Independent development
Blackshadow(s) / Agrius/ Darkrypt	11-12/2020	Shirbit	Exploiting known weaknesses in VPN servers, Exchange, applicative weaknesses in SQLI, IIS servers	Apostle ransomware
	03/2021	KLS vehicle financing		Remote control malware
	08/2021	Bar-Ilan University		IPSecHelper
	10-11/2021	Various Israeli companies such as: <ul style="list-style-type: none"> • Cyberserve • Kavim • Dan • Pegasus • Doctor Ticket • Atraf 		CryptWrapper-Encryption tool
FoxKitten/ Networm/ Pay2Key	07-08/2020	Various companies in the Israeli economy	Unique Token for configuration of FRPC, including overlap of server addresses, command and	Cobalt.Client ransomware (Pay2Key)
	11/2020	The logistics companies Amital and Orion and through		

		them directly to other companies	control of configuration	
	12/2020	Many companies, including Intel's Habana Labs, Israel Aerospace Industries' ELTA; Portnox – NAC corporation and many others		
Deus	09/2021	Voice Center And through it many Israeli companies	In this attack the tools were not made public, but the attacker's behavior on networks, language, and supply chain method all indicate an Iranian influence operations campaign	
Moses Staff	10-11/2021	Israeli companies and organizations including: <ul style="list-style-type: none"> • Gidel • Electron Csillag • Dosik Technology • Epsilor • David Engineers • Ehud Leviathan Engineering 	Exploiting ProxyLogon weaknesses in Israeli companies that have Exchange servers installed on them, that didn't have security patches installed on them	DiskCryptor ransomware

		<ul style="list-style-type: none"> • H.G.M. Engineering • Artzi ,Hiba, Elmekiesse, Cohen - Tax Solutions • Matitiahu Bruchim Law Office • V-On corporation • CVs of Unit 8200 graduates 		
--	--	--	--	--

Recap

The past two years have witnessed cyberattacks attributed to Iran against companies and business organizations in Israel that are ostensibly ransomware, but in fact are undertaken for influence operations purposes. Ransomware attacks have been very common in recent years and have been defined by the White House as a central cyber threat. At the same time, the use of ransomware attacks as influence operations rather than an economic purpose is a singular phenomenon in the framework of the conflict between Israel and Iran and its supporters.

The strategic change is that attacks are intended to pressure the public, and thereby influence decision makers and the conflict underway between Israel and Iran in several contexts. These include the campaign between wars against Iranian elements in Syria, the maritime arena, or cyberattacks attributed to Israel and the West on civilian governmental sectors in Iran.

It seems that Iran has identified a soft underbelly in Israel – the cyber security systems of the private/business sector. Attacking private business organizations enables Iran to operate relatively freely and score a dual achievement – one with respect to Israel's citizens and decision makers; the other internal, as a demonstrated response to the cyberattacks that disrupted daily life in Iran.

Even though the technical level of the Iranian attacks is not high, they are successful in part and wield an influence operations impact, especially among economic leaders. Their success stems from a low level of security and insufficient awareness of the need to invest in cyber defense of the civilian private sector in Israel, as well as the considerable attention in the Israeli media to the attacks.

Conclusions and Recommendations:

- a. Cyberattacks directed against the business/civilian sector seize on vulnerabilities in the cyber defense systems of these organizations. Consequently, attention is necessary on the national level in order to increase basic cyber security in the business/private sector.
- b. Due to the phenomenon of ransomware attacks for influence operations purposes, it is worth examining which private/business sub-sectors might cause influence operations damage to Israel (for example, the issue of privacy) and to examine how to improve the protection of these sectors. In this context, it is worth providing incentives to the business sector to tighten its cyber defense systems.
- c. Those involved in the protection of privacy – first and foremost the Privacy Protection Authority – need to enforce existing cyber defense regulations on issues of privacy protection, and to update them in accordance with the development of the threats.
- d. Since this is a threat with influence operations purposes, the Israeli media has a significant role in addressing the threat. The relevant national bodies should initiate in-depth discussion with spokespeople and defense and technology correspondents in order to deepen the understanding of the challenge and how to address it in the media sphere, and thereby minimize the achievements of the attacking side.
- e. Israel should examine how to take part in international cooperation efforts led by the United States that focus on addressing ransomware attacks in order to contain the attackers, expose them, and make these kinds of attacks illegitimate.

Boaz Dolev has over 20 years of experience in the field of research, cyber intelligence, building and managing cyber defense systems, and managing governmental cyber defense projects and systems. He is the CEO of ClearSky, a cyber intelligence company that carries out projects for companies and organizations in Israel and abroad. He is head of the cyber and information security committee at the Standards Institute of Israel's, and a former director of the e-Government Unit and Tehilla, Accountant General Department, Ministry of Finance.

David Siman-Tov is a senior research fellow at INSS.