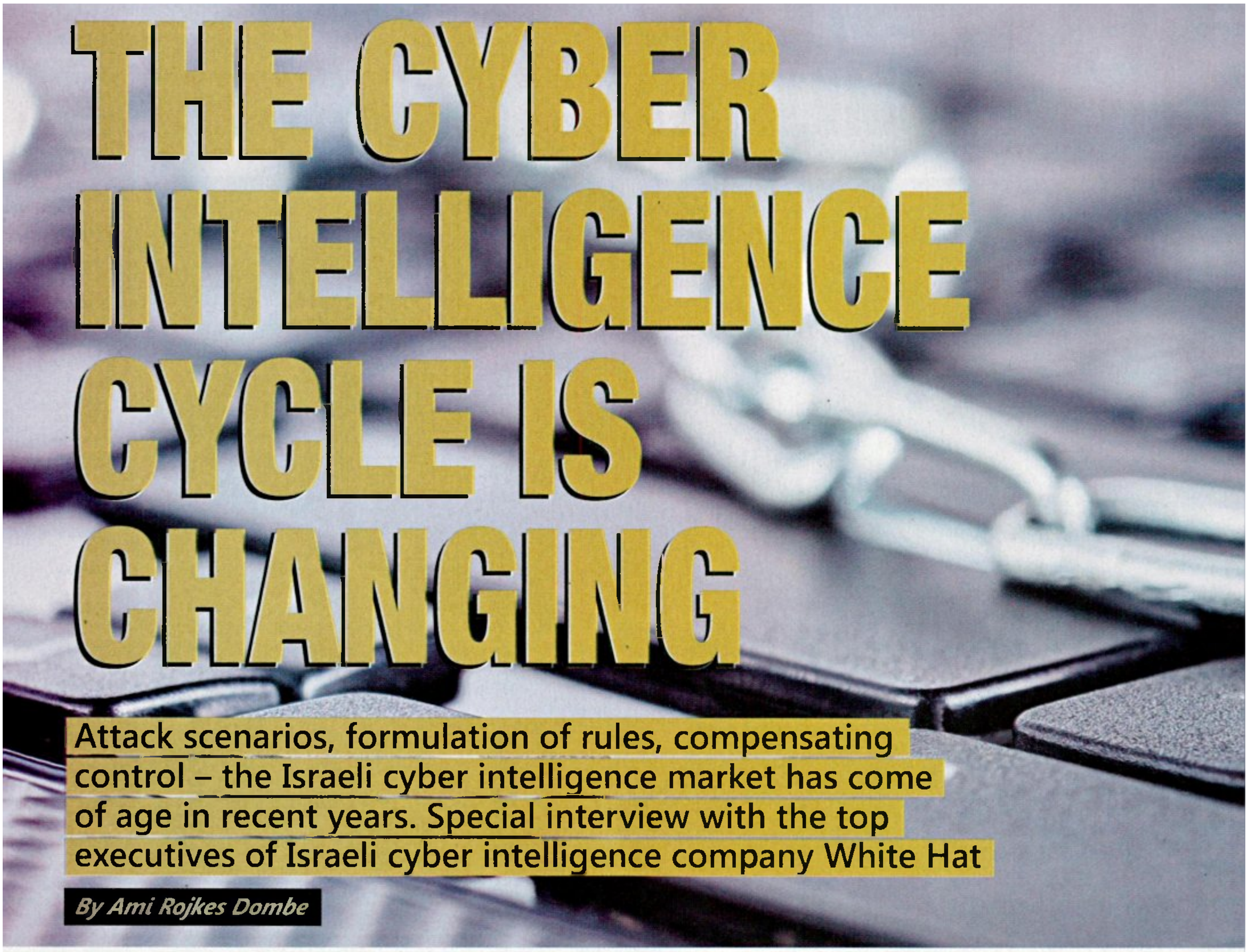


THE CYBER INTELLIGENCE CYCLE IS CHANGING

Attack scenarios, formulation of rules, compensating control – the Israeli cyber intelligence market has come of age in recent years. Special interview with the top executives of Israeli cyber intelligence company White Hat

By Ami Rojkes Dombe

How has the Israeli cyber intelligence market matured in recent years? Well, to answer this question, I applied for an interview with Sharon Nimirovski, owner and CEO of the White Hat cyber intelligence company. We had a similar chat a few years ago, and I expected the current chat would enable me to understand the processes this market has gone through in recent years.

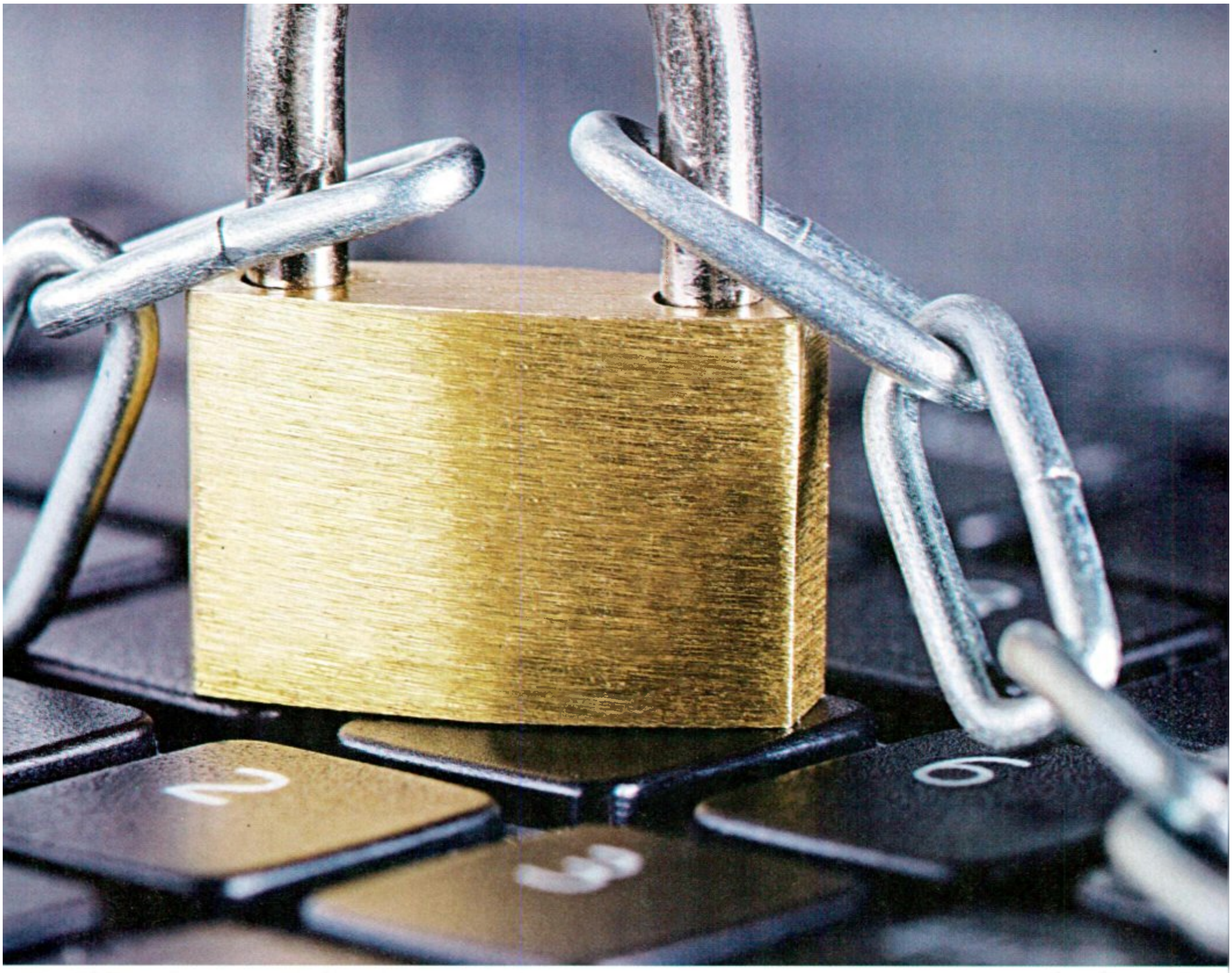
"Cyber intelligence had started out as a collection of messages in WhatsApp groups, progressed to feeds purchased from intelligence companies and today there is also intelligence that comes from the national cyber layout," explains Nimirovski. "The problem with cyber intelligence in these configurations is that it does not provide the organization with the full picture as to which threats are aimed at it. To understand the value of cyber intelligence, the question one should ask is who initiates a focused attack against the organization. In most cases, the initiators are criminal, terrorist or intelligence organizations.

"In such organizations, the attacker starts the process by collecting intelligence on the objective. Anything he can find through open sources goes into a collection file. He then moves on to the scanning stage, based on the information he had found regarding the organization in which he is interested: network layout, technologies, officers, chain of supply. Subsequently, he 'scenariorizes' – develops the attack scenario, namely – he actually checks which path of those he had found would get him into the organization. Owing to his preliminary collection effort, he is familiar with the hobbies of the key personnel, and based on this information he can produce a dedicated Phishing campaign with the objective of 'fishing' for a certain individual, targeting only that individual. If he fails to accomplish this through the organizational infrastructure, he will attempt it through the private one. If that fails, he will try the chain of supply and so forth. The moment he has succeeded – the story will come to an end."

Controlling a Network within Minutes

Nimirovski explains that the highlight of the cyber intelligence world is the ability to produce current attack scenarios for a specific organization. "The question an organization asks itself is how a certain scenario can actually occur in my network," explains Nimirovski. "Based on that question, the intelligence sought is what information regarding the organization is readily available on the web? Which attack scenarios are relevant to it? Cyber intelligence should be client-oriented and that is what we do – we see you just as the attacker sees you. "We 'scenariorize' (develop scenarios) for the

17.85x23.19	2/3	עמוד 69	israel defense מהדורה אנגלית	14/08/2018	64792544-1
54561 - WHITE HAT - חברת בטיחות סייב					



client 24/7. If I managed to get to the Twitter password of a public company, I would be able to decrease the value of its stock. If I managed to get to the access details of the Linkedin accounts of the board of directors or the management – I would have practically decreased the value of that company's stock. That is the game today. The attacker can make a lot of money buying 'shorts' on the stock exchange. Until they have adjusted the stock value, he had already made his profit. This is not an intelligence feed where the client has to ask himself what he should do with it, but reliable information – to the maximum extent possible – regarding the actual risk he is facing in cyberspace.

"We also develop usability scenarios for existing weaknesses and established attack methods. The objective, in this case, is to show the organization which weaknesses that had already become public knowledge might damage his computer system. When an organization gives us the authorization, I will control their network within ten minutes, even if they had installed the recommended security products. In today's reality, technology does not stop focused attacks. Our clients invested a fortune in security products. Finance, insurance, government – we can go through anything, and that is not because we are such geniuses, but because we do what the attackers do. We regard the client as an objective through the scenario designer-exploiter cycle."

Formulation of Rules & Compensating Control

The people at White Hat explain that they perform most of their work opposite the organization's Security Operations Center (SOC). Working within the scenario-exploitation cycle enables them to formulate rules that are suitable for real-life attack scenarios. "We identify the loopholes, formulate rules and attempt to enter again," explains Nimirovski. "Conducting such tests on a regular basis significantly decreases the number of loopholes in the organization's security layout, through which an attacker may gain access.

"Our effort is made up of four teams. The intelligence team includes focused intelligence and trend intelligence: new attacks, new weaknesses, the latest from the trade conferences, the latest discussions in the forums. The findings go to the CTO and we use some of them to create a database of current ways to gain access into the organization. The database provides another team with the tools required in order to simulate attackers and examine the loopholes in the organizational security layout. We coordinate all our activities with the client. The objective is not to test the SOC, but rather to review the security layout.

"If we send an E-Mail message with a contaminated presentation attached to it, the client organization will be informed what the message contains and when it will be received. We ask the client to open it with the intention of gaining access into the organizational system. The client will open the presentation and if we managed to control the network, the SOC would receive the relevant screen printouts. Some organizations want to seal their loopholes on their own, while others ask us to formulate the rules for them. The rules serve all of the security layers – the EDR, FW, SIEM or any other element the client possesses, and they work. We can actually see that an organization that 'scenariorizes' attacks, formulates rules and implements compensating control will experience a decrease in the amount of successful attacks."

The people at the White Hat Company told us that weaknesses are not the only thing that matters, as attack methods matter as well. In the professional jargon, the name of this field of activity is Tactics, Techniques & Procedures (TTP). "If an attacker uses Powershell, which is a task automation and configuration management software framework by Microsoft, what will you do? Will you shut off your Powershell? If you do, you will be rendering your organization inoperable. This problem has no off-the-shelf solution. To cope with it, the client will require a review of scenarios, formulation of rules and compensating control. Attacks that leak information using Domain Name Servers (DNS) are in the same category. What will you do? Will you shut off your DNS? It will be impractical," they explain at White Hat.

On the Brink of Terrorism

Along with the attacks whose objectives are money or information, there are attacks whose objective is terrorism. Attackers planning such attacks normally seek targets where an attack can generate substantial damage and intimidation, like critical infrastructures. "We have identified the emergence of attacks on the brink of terrorism. In one case, the attackers penetrated an industrial plant using a tool that looked like ransomware, but that was not its purpose. The attackers gained control over the network and started moving, left toward the ammonia tank and right toward the formula of some chemical compound. When we examined the 'leftovers' of the attack, like the 5MD files or IP addresses, we discovered a history of attacks against critical infrastructures. Admittedly, this is not an exact science, but you know the attackers were looking for SCADA," explains Nimirovski.

Sharon Nimirovsky *(Photo: Nadav Cohen)*

Ilan Mizrachi *(Photo: Liat Mendel)*

Ilan Mizrachi, formerly the Deputy Head of the Mossad (Special Assignments) and Head of the National Security Council, and currently an external director at the White Hat Company, joined our discussion. Mizrachi pointed to the need for government-business cooperation in order to cope with the terrorist threats in cyberspace. "In the past, we had a problem – some of the critical infrastructure services did not want any help from the National Security Council. Those organizations did not believe they were facing an actual threat and in some cases, we had to prove it to them. Financial organizations were totally against allowing the government into their networks. In some cases, we managed to solve the problem. However, the desirable solution involves legislation. Persuasion and demonstration do not always work," explained Mizrachi.

In addition to the legislation and regulation that should set the cybersecurity market in order, the insurance companies are entering the market as well. Organizations have realized that there is no such thing as hermetic protection, so they want to hedge their risks with money. The insurance companies that offer policies insist on several preliminary conditions prior to the actual underwriting, on-going monitoring and their own response team during an incident. "We are in contact with several insurance companies, in Israel and overseas," Nimirovski told us.

"It is a business need. In today's market, it is preferable to be 'licensed' by the insurance company. When an organization seeks a policy, the insurance company will demand preparations for the actual insurance. Their requirements may include two-stage verification, cloud backup, operating system updates and so forth. The insurance company will also determine which remote access software products the client may use. After purchasing the insurance policy, the insured party will undergo a continuous scan by the insurance company. In the event of anything suspicious, the client will receive an alert and would have to call in a response team on behalf of the insurance company. To provide these services, you will require the seal of approval of the insurance company, indicating that you are qualified and were authorized by the insurance company to perform the operations in question."

The conversation with Nimirovski and Mizrachi has undoubtedly raised the insight that the cybersecurity market is coming of age. On the one hand, there is an abundance of niche-type solutions, each one of which addresses a part of the problem. On the other hand, the attackers regard the organization as a whole and are familiar with all of the security layers. Regulation, legislation and insurance have started to get the market in order and cyber companies that fail to operate along these three axes may not survive in the long run. "There is an overabundance of solutions and organizations do not know what to do with all of those solutions. Which niche should we protect? A situation has emerged, where an organization may purchase dozens of products and still be vulnerable to penetration within ten minutes. Consequently, organizations currently seek an indication of which scenarios they are actually vulnerable to."