



"Iron Swords" War in Cyber Sphere: Insights, Recommendations and Mitigations

TLP:CLEAR

Israel National Cyber Directorate (INCD)

January 7th, 2024

V1.0



INCD
Israel National
Cyber Directorate

Executive Summary..... 3

The Nature of the Threat Actors Activities 4

Israeli Organizations on the Cyber Front 5

Asset Types under Attack..... 6

Attack tools and methods used by attackers..... 6

Cyber Crime..... 7

Countering Terrorist Funds - the Economic Campaign 8

Insights 9

Mitigations and Recommendations..... 11

Appendix A | List of vulnerabilities commonly used by attack groups..... 14

Executive Summary

Since the beginning of the "Iron Swords" war, the Israel National Cyber Directorate (INCD) has detected a gradually intensifying activity from various types of attackers against organizations in the Israeli cyber space.

The attackers deploy wide range of methods and techniques, starting from simple, unsophisticated attacks, such as defacing websites or denial of service attacks, to targeted attacks against organizations that constitute a supply chain for many organizations in the economy, in order to achieve widespread effect.

In this report, the INCD reviews the cyber activity perpetrated against cyber space in Israel during the war, and addresses several insights derived from the first two months of the war.

The Nature of the Threat Actors Activities

1. During the war, attack activities altered significantly, over time and gradually. At this stage of the war, most of the attacks are targeted at conducting destructive attacks (CNA), in contrast to the targeting detected before and at the beginning of the war, which was characterized by attacks aimed at espionage and information theft (CNE).
2. During this period, the use of techniques, tactics and procedures (TTPs) used around the world, such as at the Ukraine-Russia war, was frequently observed. Two key issues indicate the similarities between the wars, as we will elaborate later:
 - Use of psychological warfare or influence operations (CNI) to amplify cyber-attacks, mainly by using social networks to enhance the impact.
 - Use of ransomware and destructive tools such as Wiper malware.
3. The main activities of attackers against the Israeli cyberspace during the war are:
 1. **Broad spraying attack activity** - Numerous attempts were made to abuse known vulnerabilities and human error in the application of configuration settings (Misconfiguration), such as using weak passwords and lack of setting a threshold and account lockout due to failed authentication attempts.
 2. **Extensive use of distributed denial of service attacks - (DDoS)** at the application level (Layer7) and at the communication level (Layers3-4), as well as website defacement.
 3. **Many attempts to penetrate various assets** - to obtain foothold and affect information leakage and/or deletion (Wiper operation).
 4. **Attacks against Linux systems** - in addition to common attacks against Windows-based systems, activities against Linux systems were detected, including activation of Wipers as part of a CNA attack. Use of various techniques for privilege elevation and persistence through built-in scheduling mechanisms such as Scheduled Tasks or Cron jobs has been documented¹
².
 5. **Security cameras accessible over the internet were attacked** - in order to impair or prevent their usage for monitoring physical space, as well as an espionage tool to collect intelligence from the areas observed by the cameras.
 6. Various IoT devices were attacked.

¹ T1053 - Scheduled Task/Job
<https://attack.mitre.org/techniques/T1053/>

² TA0004 - Privilege Escalation
<https://attack.mitre.org/tactics/TA0004/>

7. **Influence Operations** – mainly over social networks. Using various channels and impersonating profiles, publication of false information (Fake News or Disinformation), publication of technically correct information without relevant context, all with the aim of misleading, harming or manipulating public opinion (Malinformation).
8. **Phishing attacks** - using social engineering, both by email and SMS messages, in order to increase credibility. Sometimes an element of the recipient's personal information was added, in order to persuade the recipient to click on a link or an attachment. Though this method of attack is prominent during routine times as well, this type of campaign has significantly increased in numbers during the war.
9. **Attacking mobile applications** (smartphone applications) - or their infrastructures, by publishing impersonating applications, exploiting security gaps in application infrastructure, etc.³
10. **Attacks against organizations part of the MSP sector** – these organizations constitute a substantial supply chain for many organizations in the economy. In this category we have Web hosting companies as well as ICT integration and IT services companies.
11. **15 main attack groups** have been observed operating against the Israeli cyberspace during the war. **These groups were identified as associated with Iran, Hamas and Hezbollah**, and most of them collaborate and share intelligence information, methods and tools, in order to carry out various attacks against Israeli assets.
12. Attempts were made to encourage various target audiences, such as anti-Israel activists, to participate in the offensive activity against Israel, by supplying targets for attack or simple tools to carry out denial-of-service attacks.

Israeli Organizations on the Cyber Front

1. Attackers activity was detected against organizations having the following characteristics:
 - 1) Organizations that constitute hubs of activity as supply chain of various organizations in the Israeli economy.
 - 2) Organizations in the health sector.
 - 3) Organizations in the water and waste water sector.
 - 4) Organizations in the academic sector.
 - 5) Organizations in the energy and fuel supply sectors.
 - 6) Organizations in the transportation sector.
 - 7) Organizations engaged in maritime shipping and customs brokerage.

³ Mobile Techniques

<https://attack.mitre.org/techniques/mobile/>

2. The abovementioned organizations sometimes provide services such as shared applications used by most/all of the sector's organizations. The common theme for attacks against these organizations is the possibility for larger impact on other organizations in the sector, or on those that use the services of the organization under attack.

Asset Types under Attack

1. Attackers activity has been detected against many common assets such as:
 1. Physical security systems, mainly security cameras.
 2. Exposed management interfaces, such as a remotely managed controller (PLC) interfaces.
 3. Communication equipment that exposes management interfaces to the Internet, for example equipment by Cisco or Juniper managed over the internet.
 4. Remote monitoring and management systems exposed directly to the Internet⁴.
 5. Remote access tools such as VPNs by Fortinet, Citrix, F5 etc.
 6. Webmail servers such as Roundcube and Exchange OWA with or without EWS interfaces.
 7. Content management systems (CMS) such as WordPress, Drupal, Joomla.
 8. IoT devices.
 9. API interfaces accessible from the internet, such as REST/SOAP interfaces.

Attack tools and methods used by attackers

1. Attack methods based on tools already installed on the target of the attack as part of the operating system or applications LOLBAS⁵ (Living Off the Land Binaries, Scripts and Libraries).
2. Supplying attack tools for use by actors with no technical knowledge. For example, supplying access to a website that includes a Denial of Service (DDoS) attack script where the attacker only has to enter the address of the target.
3. Exploiting file sharing services for running an attack tool or using a legitimate user for initial access to an organization's network, while bypassing security measures, and used as a **channel for leaking information**. Services such as: Microsoft OneDrive, Google Drive, Dropbox, Discord Servers.
4. Using open source tools modified by the attackers, such as DCOMpotato, where some of these tools misuse WinAPI.

⁴ CISA Releases JCDC Remote Monitoring and Management (RMM) Cyber Defense Plan
<https://www.cisa.gov/news-events/alerts/2023/08/16/cisa-releases-jcdc-remote-monitoring-and-management-rmm-cyber-defense-plan>

⁵ A sample list of tools is available at: Living Off The Land Binaries, Scripts and Libraries
<https://lolbas-project.github.io/>

5. Using free and commercial Proxy and VPN infrastructures, or endpoints attacked to cause them to act as a Dedicated Proxy, for the purpose of bypassing restrictions such as using Geo-Location to prevent access from abroad.
6. Abuse of legitimate functionality of a corporate email system, after taking over the mailbox of a user in the organization. For example, setting Outlook/OWA/Office365 rules to send a copy of an email to the attacker and deleting the sent message.
7. Using Reverse Shell to contact the management server (C&C) and leak information⁶.
8. Use of website hosting and hosting services (Hosting Services/VPS) as an infrastructure for carrying out attacks.
9. A list of vulnerabilities used by various threat groups is included in Appendix A.

Cyber Crime

1. So far, we have focused on the cyber-attacks observed in the Israeli cyberspace during the war, driven by an overarching motive of harming business continuity and productivity.
2. During the war we have witnessed another type of attacks, motivated to provide economic gain.
3. In the shadow of the war, there was an increasing trend in the frequency of ransomware attacks in Israel. The choice of ransom as an offensive tool is not surprising and even natural at this time, when warfare of influence and perception is a significant instrument in the battle. The effect caused by a successful ransomware attack may cause fear and paralysis to the attacked, as well as for those that learn about the attack. These attacks are carried by simple to operate tools, accessible to an average user, and do not require much technical knowledge for their implementation. A number of insights has emerged from analyzing reports received by INCD:
 1. **An increasing trend in the use of Wiper type “ransomware”** – attack tools characterized by wiping all information on the network. Sometimes this action is accompanied by data exfiltration (for the purpose of negotiating over the publication of the information, humiliating the victim, or bragging on the part of the attacker) or simply by erasing it to cause damage to the victim and its functional continuity.
 2. **Ransomware type tools operated by criminal groups using the RaaS (ransom-as-a-service) business model** - this model, which offers a subscription mode of operation, allows any user to purchase a product at a monthly cost and use it for his purposes while sharing in the profits obtained from the payment of ransom by the victims. The use of ransom-as-a-service is

⁶ Reverse Shell

T1059 – Command and Scripting Interpreter

<https://attack.mitre.org/techniques/T1059/%D7%A9>

particularly convenient, since the purchased product comes with full technical support, does not require a high level of technical understanding; it causes damage with minimal effort, and guarantees income and anonymity to the user. The ransomware is not unique per victim thus making it difficult in most cases to associate one with a specific subscriber.

3. **First time usage of Wiper attack tools targeting Linux-based servers** - this trend converges with global reports about extortion and crime groups, together with state attack groups that streamline technological effort towards developing harmful tools against various Linux-based distributions. The expansion of malicious actors in cyberspace towards other operating systems besides Windows requires defending organizations to understand the risks and provide a solution against the strengthening of these malicious actions (BIBI, LOLBIN).
4. The attackers recognize the human factor as the weak element to be leveraged in a cyber-attack. A significant percentage of cyber incidents handled by the INCD originated from a human agent who opened a phishing email, clicked on an unknown link or downloaded an unknown file to their system. It is true that this is not a unique trend in times of war only - but this vector is preferred by attackers at this time.
5. **Sharp increase in the use of N-Day vulnerabilities as an initial access vector** - it seems that threat groups avidly monitor publications of vulnerabilities, and find windows of opportunity to use these vulnerabilities in very short periods of time. Using such vulnerabilities is not unique to one group, and widespread use of these vulnerabilities can be seen by state sponsored APTs and cybercrime groups.

Countering Terrorist Funds - the Economic Campaign

1. For many years, the State of Israel has been conducting, in parallel with the physical and cyber war, a persistent economic campaign against terrorist organizations and the funding sources for these organizations around the world.
2. Hamas, like other terrorist organizations in the world, has resorted to the use of crypto currencies to make it more difficult to thwart its funding sources, primarily Iran. The transition from conventional currency (FIAT money) to crypto helped Hamas receive a lot of funds on an ongoing basis from Iran during the two years leading up to the "Iron Swords" war.
3. Initially, Hamas used crypto to receive small amount donations from supporters around the world, but soon moved to extensive crowdfunding campaigns using social networks, with revenues reaching millions of dollars.
4. According to the National Headquarters for Combating Terrorism Economy (MATAL), crypto has become an essential part of operational activities for Hamas. The transferred funds are used,

among other things, to purchase weapons and ammunition, and to finance other terrorist activities.

5. As part of the economic war on terrorist organizations, various partners in Israeli IC identified and seized digital wallets that contained dozens of millions of dollars in a wide variety of tokens (cryptographic currencies), the prominent ones being: Bitcoin (BTC), Ethereum (ETH) and Tron (TRX).
6. INCD joined as a partner in the economic campaign from the beginning of the war. As part of this activity, the INCD has developed technological tools and methods, enabling detection of dozens of terrorist financing campaigns, worth millions of dollars.
7. The developed tools and methods were built to respond the challenges of the Israeli IC, as reflected to INCD by its partners, to assist with collecting, locating, and processing OSINT data on terrorist financing campaigns. Technological tools were deployed on as wide a variety of platforms possible, where the fundraisers for terror organizations operate, focusing on crowdfunding platforms, social networks, etc.

Insights

1. Following detection of various attack patterns and the developing trends during the war, several insights can be pointed out:
 1. **As the war continues, the boldness and creativity of attackers increases** - evidenced from the transition from CNE attacks to CNA attacks, and raising the bar to attack high-end targets, such as attacking a hospital, putting human lives at risk.
 2. **Targeting "Hub" organizations that provide services to many dependent customers** - the more services an organization delivers to external entities, whether within a specific sector or as a service provider, the more attractive this organization becomes as a target in the eyes of a potential attacker.
 3. **Pervasiveness of disruption attacks** – the growing number of ransom or destructive deletion (Wiper) attacks, emphasizes the crucial task of being able to recover from such an attack.
 4. **Keeping multiple backups** - preferably using different technologies, with at least one backup copy kept offline and off premise at all times, which is critical for recovery.
 5. **Recoverability** – an organization should ensure its ability to successfully recover all cyber assets and information, from the hardware level up, in an alternative environment based on new hardware and/or utilizing public cloud environment, even if an attacker succeeds in violating the integrity of used hardware, such as disrupting/deleting the UEFI/BIOS.
 6. **Using Geo-location to prevent access by attackers from abroad** – this is not considered an airtight defense against attacks from outside the country, since some attackers are able to

bypass it, using free or commercial services or attacking intermediate servers in the target country. However, it is still recommended to implement this mechanism in the organizational network, to reduce network exposure and prevent low level attackers from getting access.

7. **Distributed Denial of Service attacks (DDoS)** – defending against this type of attack requires an organization to prepare in advance, through agreements with their Internet provider and/or by employing a dedicated traffic filtering service (network traffic scrubbing center). Organizations should prepare to respond to different levels of attack volume and frequency, with an emphasis on the Application and Networking layers.
8. **Exposing security cameras to the Internet** - cameras are an important security measure in an organization's service, therefore exposing them directly to the Internet should be avoided, while reinforcing their security by setting a strong password (and if possible, MFA authentication) and restricting access to relevant and specific users only. During installation of cameras, it should be verified that they are not directed at sensitive areas or security facilities.
9. **Human resources during a cyber emergency** – the possible absence of key professionals during a national emergency should be anticipated in advance; thus, it is recommended to prepare for it utilizing alternative sources through service contracts or by hiring manpower, even for short terms.
10. **Raising alertness in emergency** – examine methods for proactive alert raising in the event of a national emergency, including considering taking proactive actions such as quickly disconnecting interfaces from the Internet, preventing access to services and servers that are not essential or establishing a strict Internet browsing policy.
11. **Employee awareness** - sharpen employee awareness of common attack patterns, especially phishing attacks, and acceptable coping methods, including understanding of the importance of reporting a suspected cyber incident.
12. **Physical security of server rooms** - the war raised the importance of the physical and environmental security of server rooms and work areas to preserve business continuity in case of intrusion into the facility or physical damage because of rocket fire.

Mitigations and Recommendations

1. Reducing attack surface

1. Reduce the organization's external attack surface by continuously mapping and monitoring its changes, while taking actions to reduce the attack surface. For example, disable access to sensitive ports (management interfaces) or those that are not necessary for business activity, and reduce the number and variety of corporate services accessible from the Internet as much as possible.

2. Information security updates

1. Many manufacturers allow subscribing to email distribution lists to receive notifications about security updates by email. Leverage this option and monitor vendors of equipment or software operated by your organization vigilantly.
2. Consider installation of security updates, particularly those classified as critical and high, within a reasonable period of time from the date of their publication, since attackers manage to exploit vulnerabilities sometimes within hours from publication. For assets directly exposed to the Internet, installing updates as fast as possible is imperative and should be considered mandatory.

3. Access to management interfaces from the Internet

1. Avoid providing access to management interfaces over the Internet. Use services such as a VPN or a ZTNA with an appropriate MFA, as well as cellular APN or MPLS infrastructure, to isolate access to these critical interfaces.
2. Set up each and every remote access user, in particular those with administrator privileges, with strong authentication (MFA).
3. Implement a Geo-Velocity mechanism to detect anomalies in the identification process and session management.
4. Examine the possibility of restricting remote access by using a Deny List approach, based on continuously updated Threat Intelligence, and with reference to the following data:
 1. IP addresses of free and commercial proxy services, such as: TOR, Freenet, I2P, ZeroNet, KPROXY, CroxyProxy.
 2. IP addresses of free and commercial VPN services.
 3. IP addresses associated with known attack systems used by threat actors.
 4. IP addresses associated with notorious countries.

4. Hardening endpoints and servers

1. Verify that operating systems and applications without vendor support (End of Life products) are not used in your environment.

2. Ensure that user accounts with high privileges are not used routinely, and are only used for tasks requiring these privileges.
 3. Test and enable the following security mechanisms on endpoints and servers:
 4. Secure Boot, Windows credential guard, Windows defender device guard, Controlled folder access, Windows sandbox, AppLocker, Windows Firewall.
 5. In a multi-tenant environment, it is recommended to examine the possibility of simultaneously activating several mechanisms for differentiating between environments of various customers, including: a dedicated IAM instance for each customer, encryption of each customer's information by a dedicated encryption key, use of kernel-level tools such as SELinux and/or Chroot, and implementing a dedicated VXLAN for all client traffic.
 6. Make sure that endpoints and servers have the latest version of EDR/XDR installed, and that it is regularly maintained and optimized. Implementing products of this type **have been proved to be effective in mitigating and curbing cyber-attacks.**
5. **Protecting corporate websites**
1. Verify that the website is protected using WAAP⁷, implementing an Allow List at the field and input levels, as it can detect whether the traffic originates from a person or a machine, and block the latter.
 2. Verify that the website is developed and maintained in accordance with accepted requirements for secure development, for example OWASP ASVS⁸.
6. **Protecting corporate mobile applications**
1. Make sure that a corporate mobile application is developed and maintained in accordance with accepted requirements for secure development, such as OWASP MASVS⁹.
7. **Brand Protection**
1. Consider using a Brand Protection service to detect anomalies such as setting up a spoofed counterfeit website or running an impersonating mobile application.
8. **Email Protection**
1. Examine the configuration settings of the email system in relation to an approved baseline periodically, for example Outlook Rules, Transport Rules.
 2. Block access to mail Web interfaces (webmail) from the Internet. If there is a business requirement to allow this, it is recommended to implement MFA and protection using WAF, and access them using VPN or ZTNA.

⁷ WAAP - Web Application and API Protection (WAAP)

⁸ OWASP Application Security Verification Standard

<https://owasp.org/www-project-application-security-verification-standard/>

⁹ OWASP Mobile Application Security <https://mas.owasp.org/>

3. Make sure that the email system allows receiving emails only after completing the following tests:
4. The email is not spam; it was not sent from an IP address/domain with a low reputation.
5. The email does not contain links to IP/Domain addresses of low reputation.
6. The email contains only attachments defined in the Allow List. There is an identity between the file extension, its Header - indicating its type, and the Payload.
7. Ensure the email does not contain malicious links or attachments – check existence of up-to-date signatures and implement sandbox testing to detect suspicious behavior.
8. Ensure the email does not contain a built-in code in the text field. In case there is a code of this type, the email security system shall remove it or perform encoding before it is transmitted to the user, so that it cannot be run.
9. The email system clearly indicates to the user that the email originates from outside the organization.

9. Protecting user Internet Browsing

1. Block access to IP/Domain addresses with low reputation (URL Filtering).
2. Implement means to verify encrypted traffic, to detect and thwart threats.
3. Prevent direct user access to the Internet through the use of RBI or similar technology.
4. Verify that downloading files is possible only after completing the following tests:
 1. The file's type defined in the Allow List and there is an identity between the file extension, the Header indicating its type and the Payload.
 2. The file does not contain malicious content - use of up-to-date signatures, as well as a sandbox testing to detect suspicious behavior.

10. Supply chain security

1. Make sure that suppliers in your supply chain meet the requirements set in the supply chain defense document by the National Cyber Directorate.

11. Physical security

1. Prepare to prevent possible physical damage to the facilities, and to recover from it in cooperation with the physical security elements of the organization.
2. Verify that server farms for the organization meet the requirements of the TIA-942 or Uptime Institute standard, Tier 3 or higher.
3. Ensure that the corporate server rooms and those in alternative site/s (DR) are in different geographical areas and are not adjacent to each other. In the absence of an alternative site, it is recommended to consider establishing such a site, or using a public cloud environment as a substitute.

Appendix A | List of vulnerabilities commonly used by attack groups

Part one | Vulnerabilities exploited by the 15 attack groups targeting Israel:

CVE	CVSS	Vendor	Product
CVE-2023-4966	7.5	Citrix	NetScaler ADC and NetScaler Gateway
CVE-2023-47246	9.8	SysAid	SysAid Server
CVE-2023-46748	8.8	F5	BIG-IP Configuration Utility
CVE-2023-46747	9.8	F5	BIG-IP Configuration Utility
CVE-2023-43770	6.1	Roundcube	Roundcube webmail
CVE-2023-38831	7.8	RARLAB	WinRAR
CVE-2023-36851	5.3	Juniper	Junos OS
CVE-2023-36847	5.3	Juniper	Junos OS
CVE-2023-36846	5.3	Juniper	Junos OS
CVE-2023-36845	9.8	Juniper	Junos OS
CVE-2023-36844	5.3	Juniper	Junos OS
CVE-2023-34362	9.8	Progress	MOVEit Transfer
CVE-2023-29336	7.8	Microsoft	Win32k
CVE-2023-27997	9.8	Fortinet	FortiOS
CVE-2023-22518	9.8	Atlassian	Confluence Data Center and Server
CVE-2023-22515	9.8	Atlassian	Confluence Data Center and Server
CVE-2023-20198	10.0	Cisco	IOS XE Web UI
CVE-2022-47966	9.8	Zoho	ManageEngine
CVE-2022-41082	8.8	Microsoft	Exchange Server
CVE-2022-26134	9.8	Atlassian	Confluence Server/Data Center
CVE-2022-1388	9.8	F5	BIG-IP
CVE-2021-45046	9.0	Apache	Log4j2
CVE-2021-44223	9.8	WordPress	Wordpress Core
CVE-2021-34473	9.8	Microsoft	Exchange Server
CVE-2021-22986	9.8	F5	BIG-IP and BIG-IQ Centralized Management
CVE-2021-21307	9.8	Lucee Server	Lucee Server
CVE-2020-5902	9.8	F5	BIG-IP
CVE-2020-14882	9.8	Oracle	WebLogic Server
CVE-2020-0796	10.0	Microsoft	SMBv3
CVE-2019-19781	9.8	Citrix	Application Delivery Controller (ADC), Gateway, and SD-WAN WANOP Appliance
CVE-2019-1653	5.3	Cisco	Small Business RV320 and RV325 Routers
CVE-2019-11510	10.0	Ivanti	Pulse Connect Secure
CVE-2018-13379	9.8	Fortinet	FortiOS
CVE-2017-0199	7.8	Microsoft	Office and WordPad
CVE-2017-0143	8.1	Microsoft	Windows

Part two | Vulnerabilities used by cyber criminals in the Israeli cyberspace:

Product	Vendor	CVE	CVSS
IOX XE	Cisco	CVE-2023-20273	7.2
		CVE-2023-20198	10.0
ASA, FTD	Cisco	CVE-2023-20269	9.1
Expressway Series, VCS	Cisco	CVE-2023-20209	7.2
Catalyst SD-WAN Manager	Cisco	CVE-2023-20252	9.8
NetScaler ADC NetScaler Gateway	Citrix	CVE-2023-3519	9.8
		CVE-2023-4966	7.5
		CVE-2023-4967	7.5
SharePoint	Microsoft	CVE-2023-29357	9.8
Webmail	Roundcube	CVE-2023-5631	5.4
		CVE-2020-35730	6.1
		CVE-2020-12641	9.8
		CVE-2021-44026	9.8
Tomcat	Apache	CVE-2023-41080	6.1
ActiveMQ	Apache	CVE-2023-46604	9.8
SSL-VPN	Fortinet	CVE-2023-27997	9.8
vCenter	VMware	CVE-2023-34048	9.8
WS_FTP	Progress	CVE-2023-40044	8.8
		CVE-2023-42657	9.6
Deep Discovery InspectorApex One Worry-Free Business Security	Trend Micro	CVE-2023-3823	7.5
		CVE-2023-3824	9.8
		CVE-2023-41179	7.2
FortiProxy FortiOS FortiWeb	Fortinet	CVE-2023-29183	5.4
		CVE-2023-34984	8.8
ESG	Barracuda	CVE-2023-2868	9.8
Avalanche, Sentry	Ivanti	CVE-2023-32560	9.8
		CVE-2023-38035	9.8

Sources

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>