Cyber ✶ Chaos

Volume 1

By: Dr Malvika Mehta

Israel-Hamas war’s digital frontline

Israel-Hamas war's digital frontline

INTELLIGENCE & INVESTIGATIONS | By: Dr Malvika Mehta | DATE: 11/10/2023

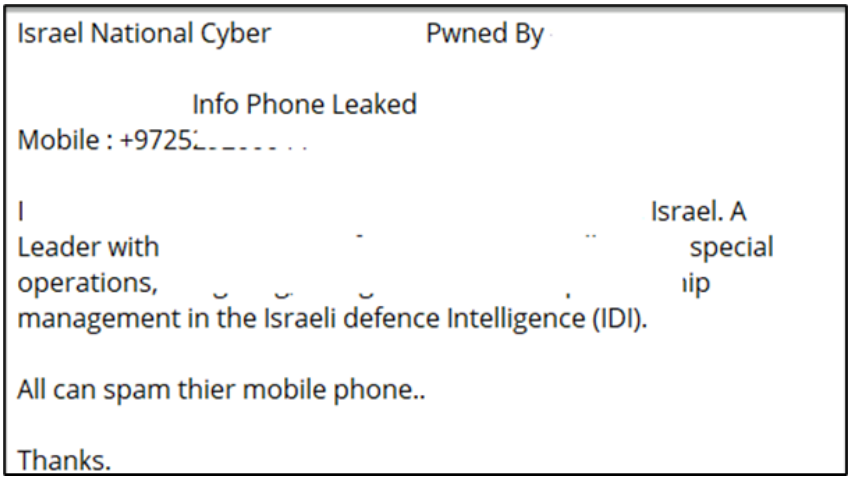
Cyber attacks on Israel's government and private digital assets have added to the ongoing conflict by Pro-Hamas hacktivist groups. Reporters have noted a discernible shift in the focus of cybercrime groups from the conflict in Ukraine to the Middle East. Over at least 15 known cybercriminals and threat groups, including KillNet, Anonymous Sudan, AnonGhost, have announced their plans to carry out disruptive attacks against Israel and those supporting them.

> "*Government of Israel, you are to blame for this bloodshed. Back in 2022, you supported the terrorist regime of Ukraine. You betrayed Russia. Today Killnet officially informs you about it! All Israeli government systems will be subject to our attacks*"- Killnet said on its Telegram channel.

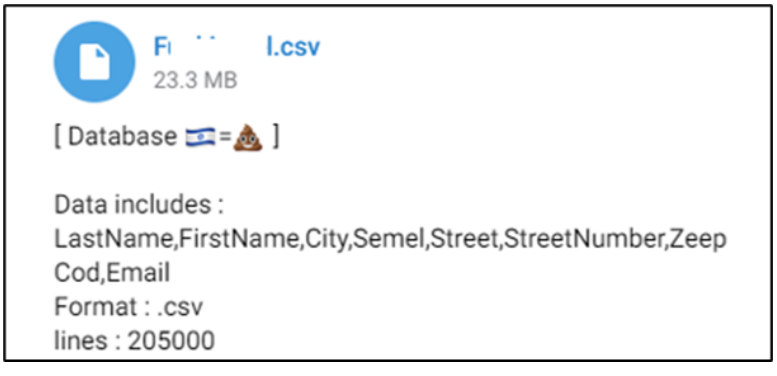
Notably, both The Jerusalem Post and the Tel Aviv Sourasky Medical Center (Ichilov) have already experienced targeted attacks that resulted in operational disruptions. Researchers have cautioned that these operations by these groups can serve various purposes, including **providing tactical advantages, acting as distractions, or even serving as a means for strategic intelligence gathering**.

Pro Hamas hacking groups have claimed that they disrupted an Israeli emergency alert application.

Phone numbers of Israeli high profile- key decision makers from the government are being leaked and broadcasted on Telegram channels encouraging users to spam them.



Leaked databases containing personal information about Israeli army officials, government officials and citizens have been circulating across Telegram and darknet channels.



And so are they attacking countries that are supporting Israel.

32,315,298 USA Citizen Leaked !
https://t.me/
Name,Address,Phone,Status,FB ID
HELLo USA Goverment !
STOP FUNDING ISRAEL TERROR !
NONE OF US ARE FREE UNTILL PALESTINE IS !
WE STAND WITH PALESTINE !
LONG LIVE PALESTINE !
VIVA HAMAS !

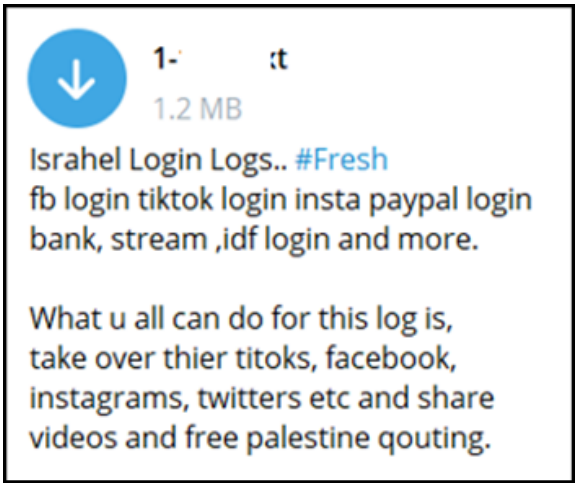
"We are
we are watching you.
we are everywhere."

Claims have been made by hacking groups that they have parked their vision in the computers & CCTV cameras in the government offices of Israel, monitoring the movements of the employees and officers.

Here we have hacked Israel's biggest System used to spy on All Countries.
This CCTV is also used by various Agencies.
📌All Government CCtv.
📌All Private CCtv.
📌All Public CCtv.

Hundreds of websites have been temporarily disrupted through DDoS attacks or defaced completely. In a report released by Microsoft last week, it was documented that a Gaza-based hacker group named Storm-1133 had intensified its cyber espionage activities targeting Israeli companies in the telecommunications, defence, and energy sectors earlier this year.

Social media logs of users from Israel- Facebook, Tiktok, Instagram, Paypal etc are being disseminated via public channels on chat applications encouraging users to take over those accounts and post ‘free Palestine’ quotes.



We saw a similar phase of ‘Cyber-war’ during the Russia-Ukraine war. The same is happening to Palestine, its government and its cyber infrastructure from Pro Israeli hacking groups.

Last few years, it has led us to believe that Cyber warfare is for real, the threats are emerging at an alarming rate. It not only serves as a force multiplier for traditional military operations but also allows state and non-state threat actors engage across borders to use their advanced cyber capabilities to achieve their strategic goals.

Espionage activities are at the rise, intelligence is being gathered during conflicts like these. State actors target their adversary's military, government and industrial systems to gain a tactical advantage. It also includes dissemination of propaganda, spread of disinformation to influence public opinion and create confusion. It is essential to bear in mind that these tactics are used to support psychological operations in times of war and elections too!

Critical infrastructure, such as power plants, water supplies, and transportation systems, is vulnerable to cyberattacks. Disrupting these systems can have a significant impact on a country's ability to function during a conflict. There is a risk of cyber operations escalating into traditional armed conflicts. A cyberattack with severe consequences could trigger a military response.

The international community is still developing legal frameworks and norms governing cyber warfare. The application of existing international law, such as the laws of armed conflict, to cyber operations is an ongoing debate.

Gravest threats of cyber warfare?