Hamas Leadership Assassination Explainer - CYFIRMA

Archived: 2026-04-05 18:43:09 UTC

Published On : 2024-08-05

The death of Hamas leader Ismail Haniyeh in Tehran and the announcement of the death of Hamas military wing commander Muhhamad Daif occurred on the same day, almost ten months after Hamas attacked Israel on 7 October. Haniyeh was in Tehran to attend the inauguration of the new Iranian president, Massoud Pesekhian, who pledged support to Hezbollah and various anti-Israeli Iranian-backed groups. Prime Minister Netanyahu has not commented on the attack itself, warning instead of “difficult days ahead”, implying potential retaliation from Iran.

The assassination on such a high-profile day is arguably embarrassing for Iran, even though Haniyeh was not Iranian (or even Shiite). Moreover, it follows the killing of senior Iranian Revolutionary Guard officers at the Iranian Embassy in Damascus earlier this year, and demonstrates Israel's ability to carry out effective intelligence-led operations in Iran. Other notable events include the killing of Iranian nuclear scientists; the public shooting of Al-Qaeda's number two, Abu Muhammad Al-Masri; the theft of Iran's nuclear archive in 2018; the Stuxnet cyber-attack on the Natanz nuclear facility (which was not even connected to the internet); the drone attack on drone factories last year, and the destruction of air defenses around nuclear facilities in April of this year.

There are unconfirmed reports that from Iranian officials that Iran's Supreme Leader Ayatollah Ali Khamenei has ordered a direct strike on Israel in retaliation for the assassination, with combined drone and ballistic missile strike on military targets around Tel Aviv and Haifa reportedly being considered.

In the past ten months of the Gaza conflict Iran has been trying to strike a balance between applying pressure on Israel by increasing the number of attacks by its proxy forces and allies in the region supplemented by cyber-attacks and AI-enabled disinformation campaigns, while at the same time avoiding an all-out war between the two countries which they are trying to avoid due to domestic instability.

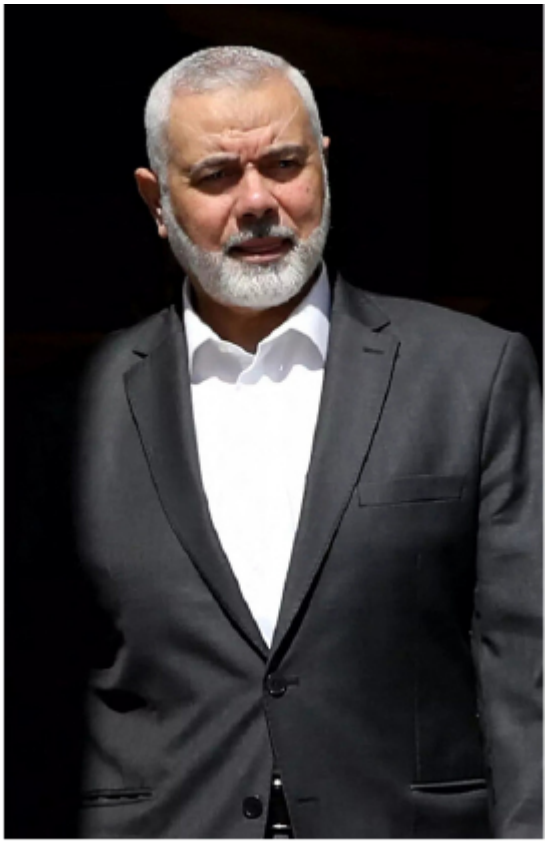
In April, Iran launched the largest and most open attack on Israel in decades, launching hundreds of missiles and drones in retaliation for an Israeli attack on its embassy compound in Damascus that killed several Iranian military commanders tasked with controlling terrorists and proxy forces in Syria. However, even this show of force was 'telegraphed' well in advance, and almost all the missiles and drones were shot down by Israel and its allies, causing minimal ultimate damage.

Iran is fighting Israel on several fronts – through Hamas in Gaza, and Hezbollah in Lebanon. At the beginning of July, Israeli fighter jets bombed a port in Yemen controlled by Houthi militias in retaliation for a drone strike that hit Tel Aviv. Iraqi Shiite militias linked to Iran sporadically join attacks on Israel, but the damage they have inflicted is arguably minimal, and their participation is seen as symbolic.

Both sides have the capacity to strike in a way that would unleash a major regional war, but so far both Israel and Hamas have opted for less direct tactics that have allowed them to claim retaliation. Israeli Defense Minister Yoav

Gallant commented: “We don’t want war, but we are preparing for all possibilities.”

THE DEATH OF THE HAMAS CHIEF SOLVES NOTHING



Ismail Haniyeh was the top figure in charge of Hamas’ international relations and one of the group’s best-known faces. From his base in Doha, he helped Hamas negotiate the terms of the Gaza ceasefire and delivered fiery speeches broadcast throughout the Arab world. However, his killing is unlikely to destabilise the organisation in the long term because, as has been shown many times, the group has recovered from previous assassinations of political and military leaders. More broadly, the Hamas leadership can clearly see how far Israel is willing to go to fulfil its promise to kill all those it holds responsible for the October 7 attack: the group’s top leaders are safe only in the tunnels under Gaza, or in countries with which Israel has formal or informal ties that it cannot afford to jeopardize (such as Qatar, where Haniyeh lived).

Hamas may have overestimated the reaction of his allies in Iran and the Lebanese militia Hezbollah. When Haniyeh and his deputy, Arouri, went to Tehran in November to meet with Iran’s supreme leader, they received public praise and expressions of rhetorical support, but Tehran declared that it would not enter the conflict directly.

Hamas was thus abandoned in the early months and found few immediate supporters, but as time went on with the Israeli operation – and as Palestinian civilian casualties began to mount – Israel has arguably suffered global reputational damage, and even charged with war crimes at The Hague.

According to the UN, 80% of Gaza's population has been displaced, nearly 40,000 civilians killed, and most of the buildings on the strip damaged. By contrast, fewer than 690 Israeli soldiers have died in Gaza since the invasion began.

That said, it could be argued that the civilian bloodshed in Gaza has helped Hamas fulfil its strategy of exacerbating divisions in Israeli society, causing disagreements over how or if Israel should even try defeat Hamas, which most analysts agree is not possible by military means. Most importantly, the war has returned the issue of Palestinian statehood to the global discourse, leading several countries to recognize Palestine as a state and making peace agreements between Israel and Arab states temporarily impossible.

Hamas's tunnel-based infrastructure will likely enable it to survive: the organisation's leader in Gaza and many of its top military commanders are still alive, and even through Israel claims to have killed approximately half of the estimated 30,000 Hamas fighters, Hamas would still have ten times more gunmen at its disposal than took part in the 7 October attack. Moreover, the tens of thousands of civilian deaths have produced many new recruits from the relatives of the deceased (indeed, the U.S. experience in Iraq is that each person killed produces 5-10 more militants).

An opinion poll conducted by a Palestinian agency in the West Bank in March 2024 showed that nearly three-quarters of Palestinians living in Gaza still support Hamas's decision to launch an attack on October 7 (compared to 57% in December 2023). However, when asked who they would prefer to control Gaza after the war, only 52% support Hamas, while 40% prefer the Palestinian Authority and 5% would prefer governance through Arab countries.

WHAT NEXT

Benjamin Netanyahu reiterated before the US Congress last week that Israel will fight in Gaza until it achieves “total victory”. Meanwhile,100 Israeli hostages are still being held in Gaza, and fighting has returned to areas in the north that Israel has previously said have been completely cleared of Hamas. Several attempts to broker peace have failed, while tensions with Hezbollah in Lebanon and Houthis in Yemen are threatening to spark a wider regional conflagration, the consequences of which would be immeasurable.

The United States remains vigorously active diplomatically, this week trying to broker a ceasefire and hostage agreement between Israel and Hamas in Rome with the help of Egypt and Qatar. Hezbollah, meanwhile, has said that if the deal goes through, it will stop its attacks on Israel’s northern border. However, despite widespread support for the deal from the Israeli public and many security officials, Netanyahu appears intransigent.

If Iran and Hezbollah do not correctly calculate retaliation for the death of Ismail Haniyeh, we may see an extension of the conflict into Lebanon instead of a ceasefire in Gaza.

CYBER PERSPECTIVE

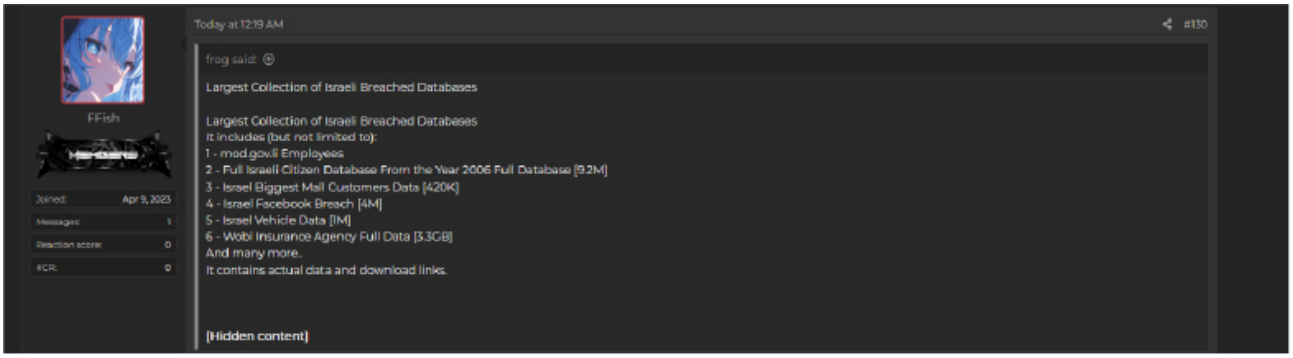
After a lull in online activity, the killing of two Hamas leaders and important Hezbollah commander in Lebanon by Israel on the same day, sparked a storm of strong reactions on social media with many threats to carry out retaliatory hacktivist activities.

Moreover, some cyber activity can lead to personalized physical attacks. Security around Israel’s athletes at the 2024 Olympic Games in Paris (on which we issued a separate report which you can find here) was upped on Wednesday as authorities investigate a cyber-attack leading to leakage of athletes’ personal information on social media, with hacker group “Zeus” posting their military status, blood test results, and login credentials. Meanwhile Iran has utilized the leak to organize a cyber campaign to send social media threats to intimidate the Israeli delegation.

Many more personal details and confidential files have been stolen by various hacktivists and threat actors in the recent months. This spring, a group called “Anonymous for Justice” claimed responsibility for the breach, which

allegedly included the retrieval of nearly 300 gigabytes of data stolen from Israel's Justice Ministry. The group published files that it said it obtained in the breach, such as legal documents including drafts of bilateral agreements, and contracts marked as confidential.

This data could potentially be cross-referenced with numerous databases that have recently appeared on the internet. These include government employee information, a citizen database with millions of entries, data from large insurance agency, data on Israeli-registered vehicles, data of the customers of the biggest Israeli mall and also social media details from Facebook.



Pro-Palestine hacktivist groups are highly likely to significantly ramp up DDoS attacks on organizations in Israel – and those with perceived links to Israel – in the coming weeks, and while Iran might have some capacity to pursue government services, energy, banking, finance and telecommunications, Iran is not ready for potential cyber retaliation from Israel, and might prefer to outsource some of its cyber campaigns to smaller groups outside its territory.

Most hacktivists will likely continue to mount mainly DDoS or website defacement attacks based on our monitoring of their channels. However, amid the myriad DDoS, wipers, espionage, and more peppering Israel's various public and private industries in recent months, some hacktivist have focused on spreading political messaging to civilians in the streets: to that end, we should expect campaigns like the one conducted by the group "MeshSec", which targeted the popular Lev Cinemas in Tel Aviv, posting threats to Israel. Hacktivist intent to share their political views with the wider public to stoke fear in societies considered hostile, as well as disrupting public order in Arab countries, where there is typically a much more radical approach to the issue than the government. Psychological operations thus might be the new front in the ongoing latent cyber war between Israel and its adversaries.

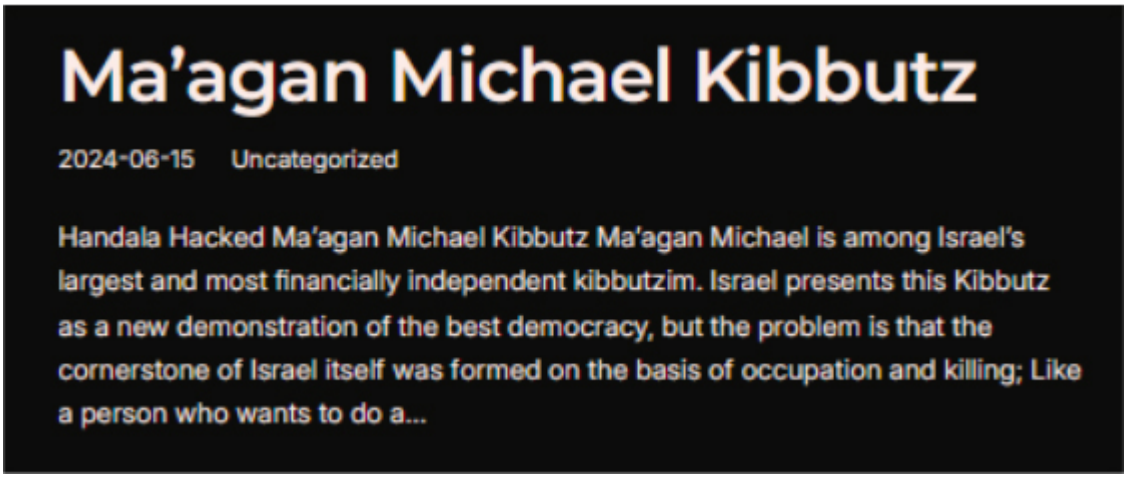
Other attacks may employ a scattershot approach, targeting anything within digital reach – for instance hospitals, universities, banks and newspapers.

HACKTVISM KICKS INTO GEAR AND GETS MORE SOPHISTICATED

Below are samples of recent hacktivist campaigns, which appear to get more sophisticated over time, now also including well-targeted phishing or devasting wipers.

RANSOMWARE ATTACK ON MA'AGAN MICHAEL KIBBUTZ

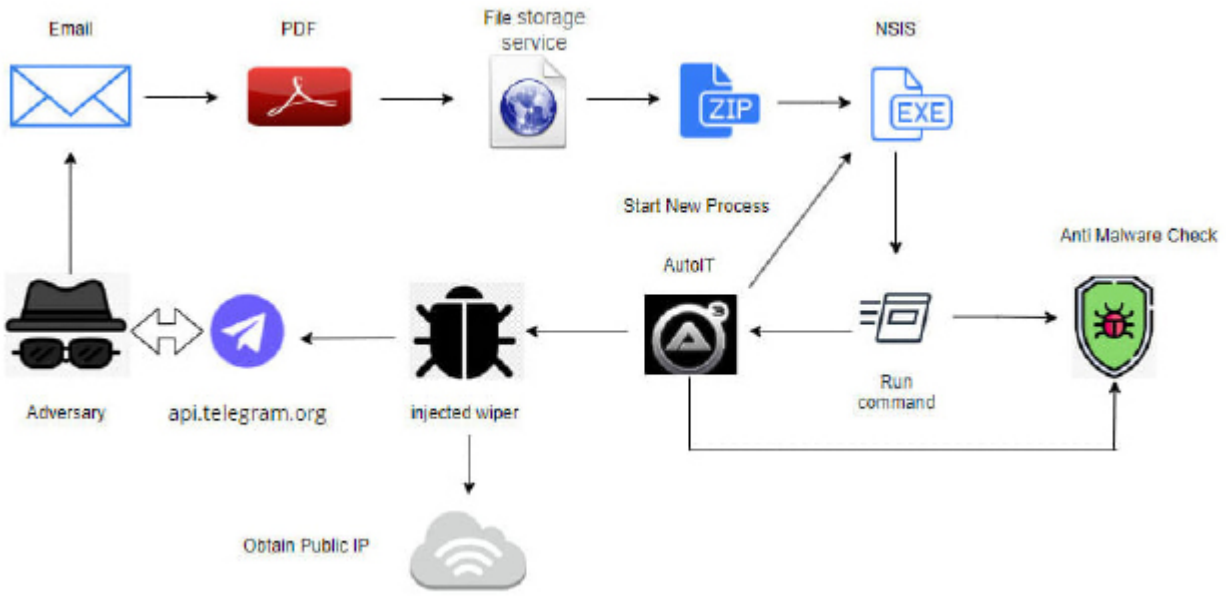
On June 15, 2024, the hacker group Handala claimed responsibility for a ransomware attack on Ma'agan Michael Kibbutz, exfiltrating 22GB of data and sending over 5,000 warning SMS messages. The ransom note criticized both the kibbutz and Israel, revealing the group's political motivations. Ma'agan Michael is one of Israel's largest and most financially independent Kibbutz, is known for its diverse economic activities and advanced technological use in agriculture and industry. Handala likely employed sophisticated phishing campaigns and malware with advanced obfuscation techniques to gain access.



HANDALA HACKERS TARGET ISRAEL WITH DEVASTATING WIPER MALWARE

The Handala Hacking Team has initiated a new wiper malware campaign targeting Israeli organizations, capitalizing on the global disruption caused by the CrowdStrike Falcon agent outage. This malware is designed to erase files from infected systems and exfiltrate data using Telegram.

The attack began with a phishing email themed around CrowdStrike, exploiting the recent Falcon agent outage. The email contained a PDF with a link to an "update.zip" file, which included a malicious NSIS installer disguised as "CrowdStrike.exe." Once executed, this installer unpacked and ran files designed to bypass anti-malware measures and deployed an AutoIT script that launched the wiper.



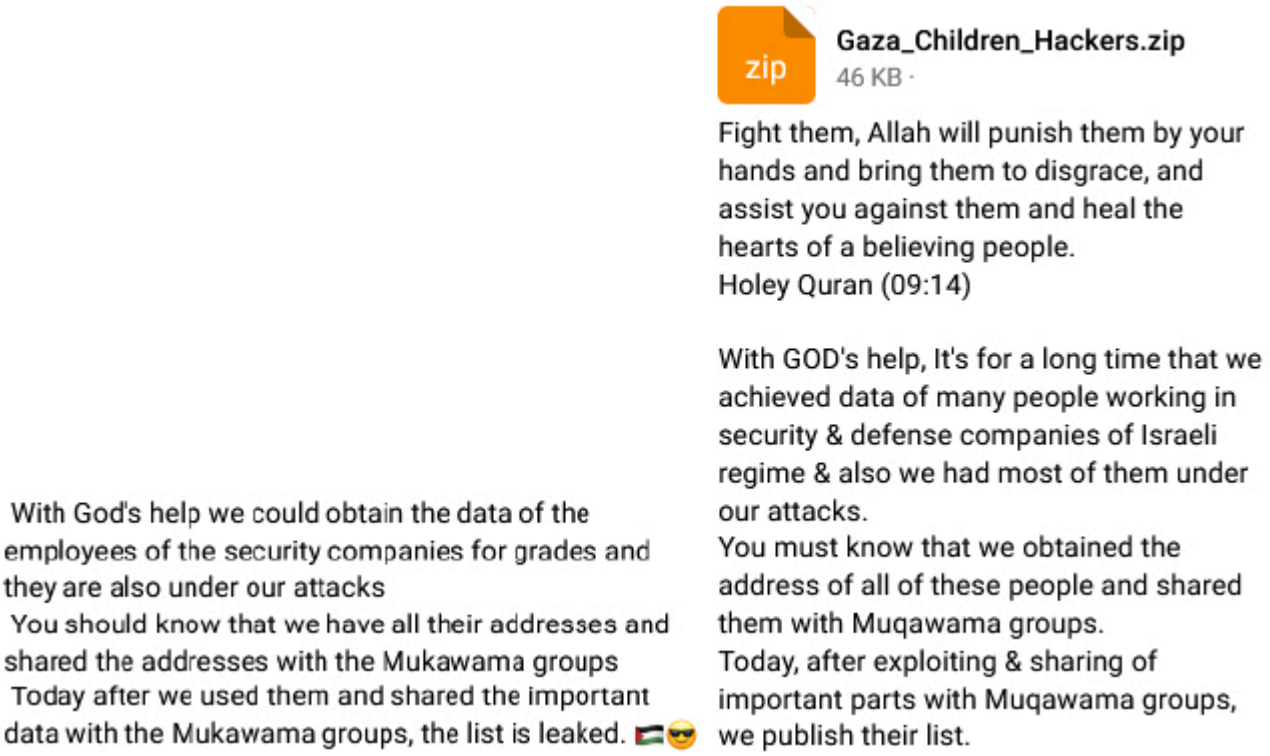
The malware's complex execution flow involves multiple stages designed to evade detection. Initially, an NSIS installer deploys a batch script named "Carrol," which checks for security software. If such software is detected, the script introduces delays to avoid triggering defenses. Next, the malware executes a PowerShell script hidden within a JPEG file, which ultimately launches the wiper.

The wiper initiates its attack by extracting files and gathering system information, which it then sends to Telegram. Following this, it begins the file destruction process. It uses the "OverwriteFileBlockSize4096" function to overwrite files in 4096-byte chunks with random data, and then attempts to delete them. If a file is in use, the malware employs an open-source project to identify and terminate the process holding the file before proceeding with the deletion.

```
public static bool OverwriteFileBlockSize4096(string path)
{
    decimal num = 0m;
    num = new FileInfo(path).Length;
    FileStream fileStream = new FileStream(path, FileMode.Open);
    StreamWriter streamWriter = new StreamWriter(fileStream);
    byte[] array = new byte[4096];
    new Random().NextBytes(array);
    decimal num2 = Math.Floor(num / array.Length);
    decimal num3 = 0m;
    int num4 = 0;
    while (num4 <= num2)
    {
        bool flag = num4 == num2;
        if (flag)
        {
            decimal num5 = num - 4096m * num3;
            array = new byte[(int)num5];
            streamWriter.BaseStream.Write(array, 0, array.Length);
        }
        else
        {
            streamWriter.BaseStream.Write(array, 0, array.Length);
            num3 += 1m;
        }
        num4++;
    }
    streamWriter.Close();
    return true;
}
```

GAZA CHILDREN'S GROUP HACKTIVIST GROUP LEAK

On July 21st the hacktivist collective known as Gaza_Children_Hackers leaked data belonging to Israeli defense companies, exposing their employees' data.



313 TEAM HACKTIVIST COLLECTIVE LEAKS ENERGY COMPANY DATA

On 29th July, the Hacktivist collective known as Iraqi Cyber Army (also going by the name “313 team”) has leaked the data of Israeli company, Y.R.T Energy, after posting propaganda denouncing Israel.

We are on the brink of a world war

The Russians, Iranians, and Turks are uniting in their rhetoric against Israel.

copy

That is why we are here, gathered in this union that currently includes more than 80 teams, so that we may have an important share in this war.

Let all flags unite and let all fronts open for a noble and lofty goal, which is to liberate all of Palestine from the filth of the occupying Zionists and their agents in NATO.

God is victorious over their affair, even if most of them do not know. And that jihad is a victory or martyrdom.

#IsraelLeaks - Leak Second - Y.R.T Energy (yrt-energy.co.il) - #Op313Team #7_October_Union #Holy_League #OpIsrael

Bismillah

In line with the Holy League's Alliance organized attack campaign against Israel, our team decided to continue its operations to infiltrate and destroy Israel's infrastructure as part of this campaign in support of Palestine. Our team is responsible for the hacking of the Israeli company (Y.R.T Energy), which specializes in the latest energy innovations in Israel. The hacking operation took place a few weeks ago and the hacking was recorded at that time, and today we leak the entire databases of the Israeli company, noting that we distorted the home page of the site and leaked their systems and databases and then Delete backups and encrypt the entire system.
As usual after the Israeli company failed to recover their encrypted website servers, they transferred the remainder of their systems and created a new website domain that did not contain il in the domain (yrt-energy.com) to avoid the bad reputation that might befall their company as a result of the cyber attack that our team launched on their systems. Note that the company's previous server and domain have been under the control of our team for weeks until this moment, and the main page of the site is decorated with our team's logo with #FreePalestine , and today we will leak its complete databases.

Download Y.R.T Energy data:
https://t.me/x313xTeamLeak/10

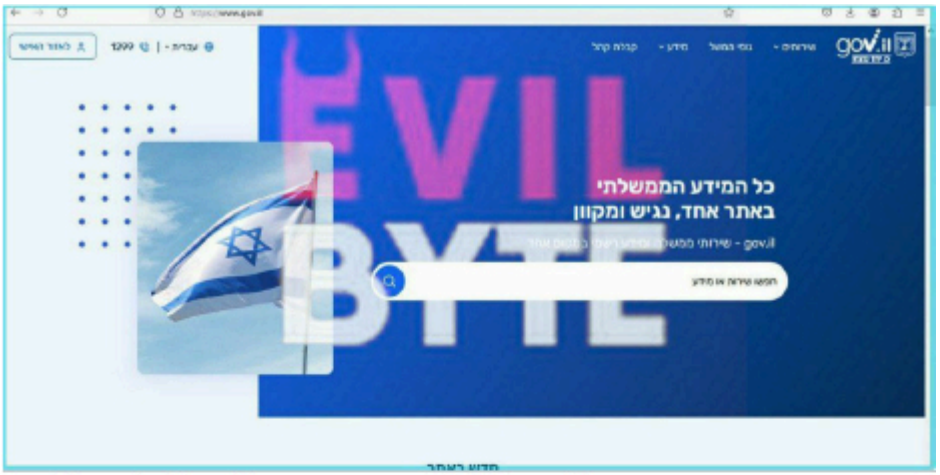
Password: @x313xTeam
SHA-1: 1aeeb8a1d7960d3c3ed8b267cb19b982cb272b6e

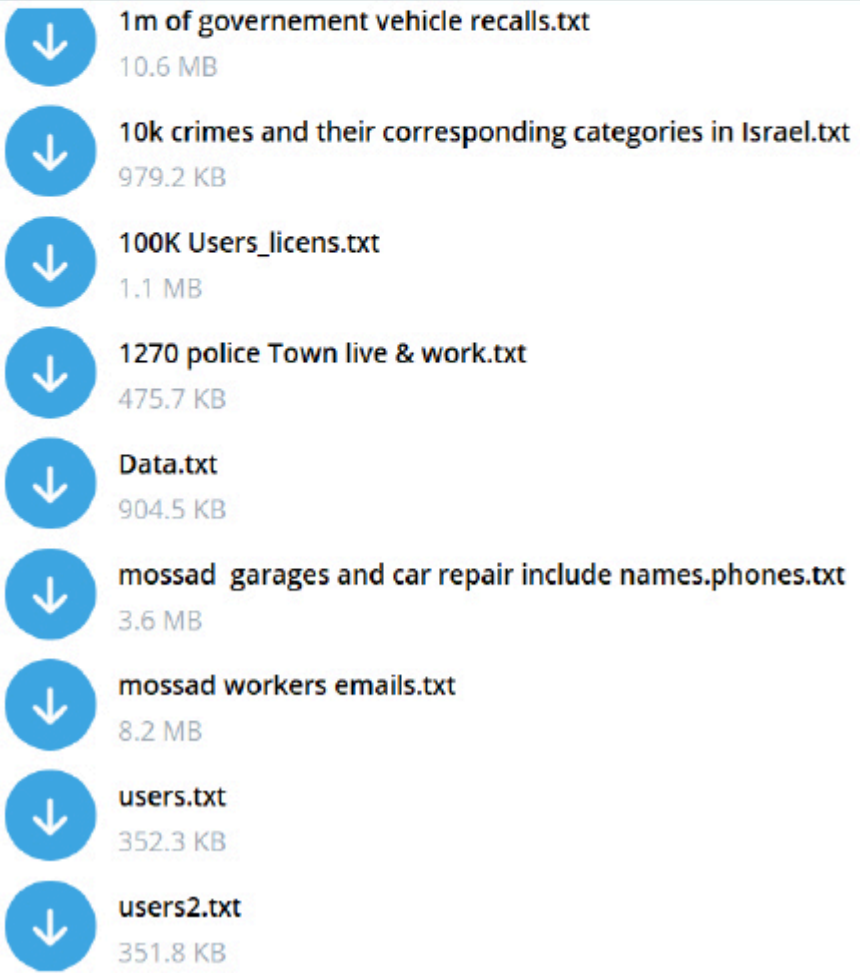
Op313Team-Opls...RT-Energy.zip
3.1 MB ·

#IsraelLeaks
Leak Second - Y.R.T Energy (yrt-energy.co.il)
Password: @x313xTeam
SHA-1:
1aeeb8a1d7960d3c3ed8b267cb19b982cb
272b6e
#Op313Team
#7_October_Union
#Holy_League
#OpIsrael
@x313xTeam
@x313xTeamLeak
@x313xTeamBackup

EVILBYTE TARGETED ISRAELI GOVERNMENT

On Aug 1st, the hacktivist collective EvilByte targeted Israeli government websites (gov.il/data.gov.il) and claimed leaking data of government employees and details linked to intelligence agencies.

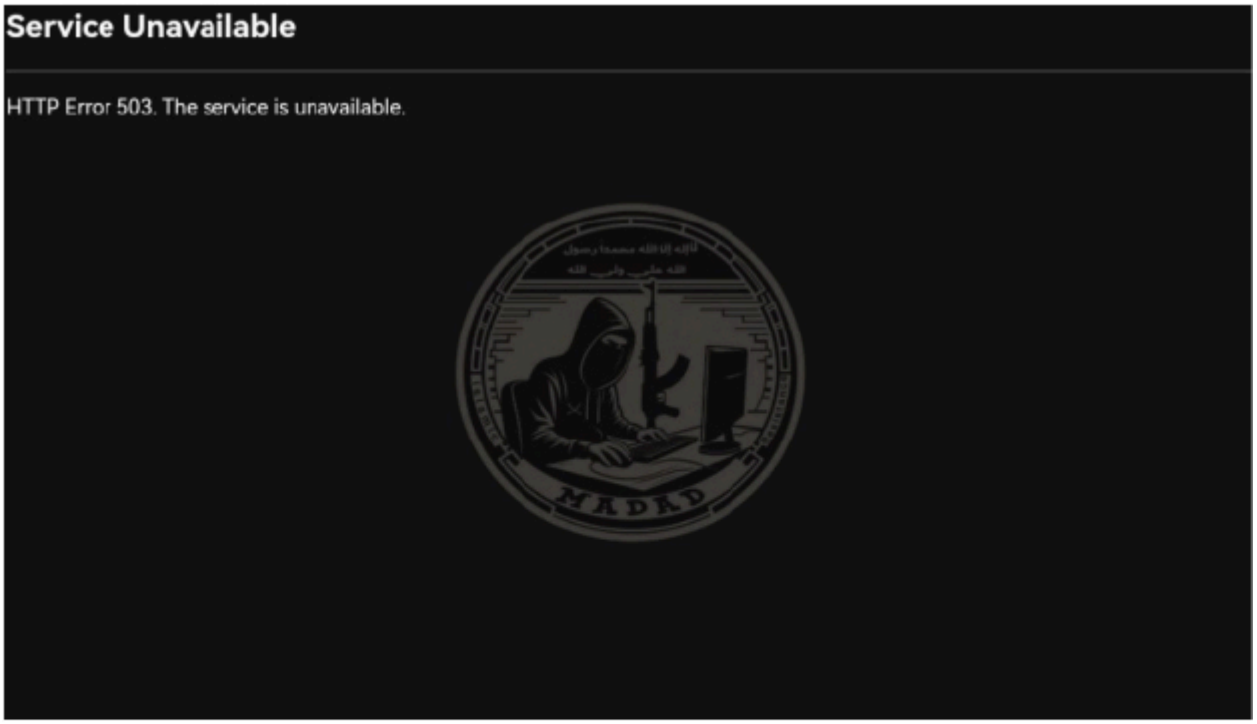




MADAD TARGETING MICROSOFT

Microsoft Israel R&D Center is one of Microsoft's three strategic regional development centers. Microsoft has recently agreed to provide "unlimited products" to the Israeli Ministry of Defense, and to "broadly exchange

‘knowledge’ with the army”: its subsidiary’s website has been now victim of DDOS attack by the Madad hacktivist collective.



microsoftrnd Israel

target:
https://www.microsoftrnd.co.il/

CONCLUSION

The cyber war is likely to escalate further as Iran vows revenge for the assassination of Hamas and Hezbollah leaders. The Israeli pressure on Gaza and the dire humanitarian situation there will continue to fuel pro-Palestinian sentiment and inspire further hacktivist action, while the actors in the international arena are weighing their options for escalation. Our researchers will continue to watch this space and bring your fresh analysis in the coming weeks and months.

Source: https://www.cyfirma.com/research/hamas-leadership-assassination-explainer/