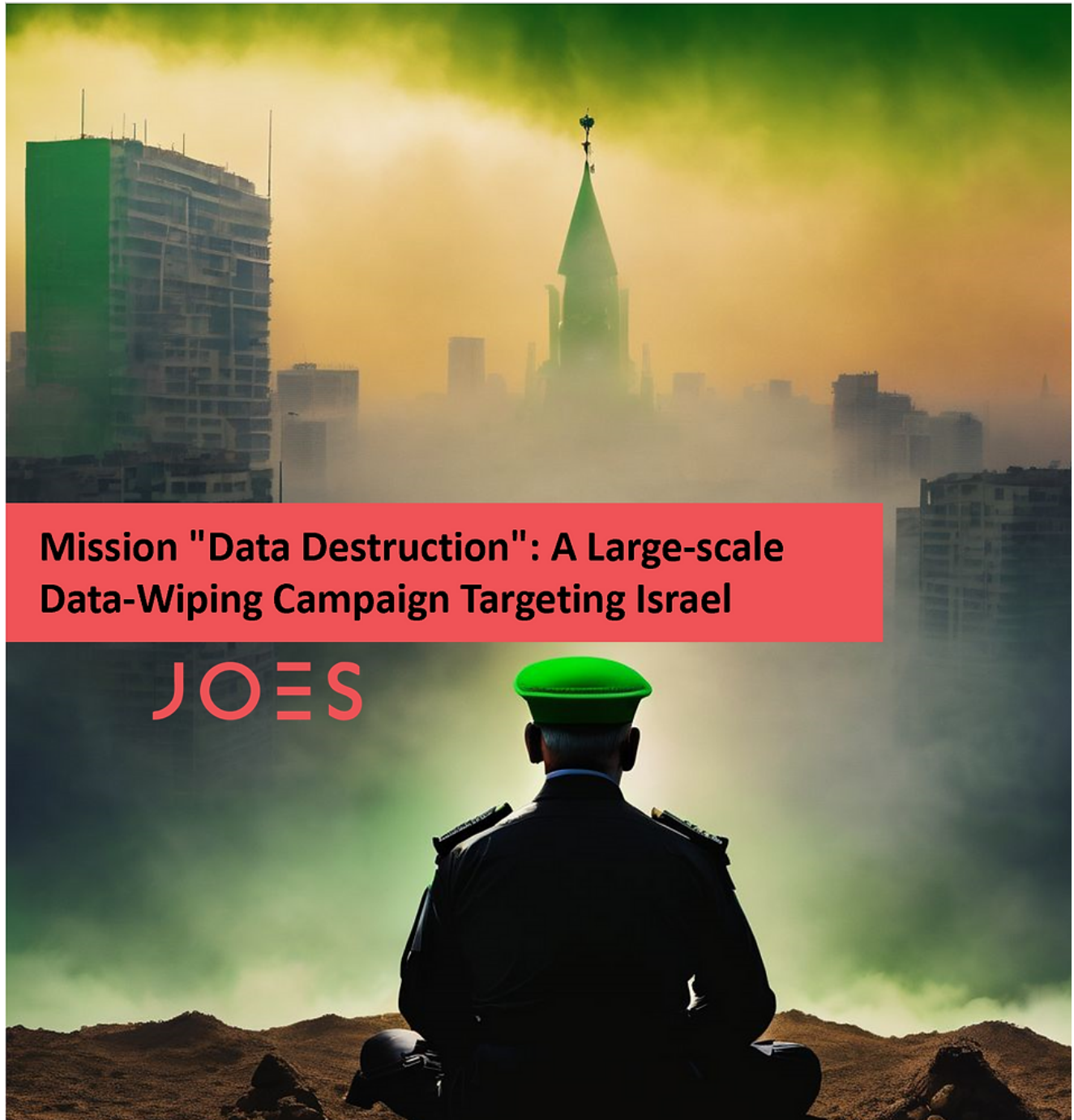
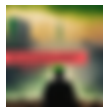


Mission "Data Destruction": A Large-scale Data-Wiping Campaign Targeting Israel

 securityjoes.com/post/mission-data-destruction-a-large-scale-data-wiping-campaign-targeting-israel

November 10, 2023





Since the conflict escalated on October 7, 2023, with an aggressive stance from Hamas towards Israel, cyber-threats have surged. For example, many Pro-Hamas and Pro-Palestine hacktivists, alongside state-backed aggressors, have launched cyber-attacks on Israeli businesses, aiming not just to disrupt but to devastate the nation's economy. In response, victim companies sought assistance from the Israeli CERT and law enforcement agencies, who in turn engaged with our Incident Response team in an attempt to recover from the breaches.

"Our team's expertise spans a wide range of incident response & crisis management aspects, with negotiation being one of our key strategies to formulate a recovery and business continuity plan. However, we quickly realized that dialogue was futile against adversaries whose intent was sabotage rather than extortion.", said Security Joes Threat Researcher, Jasmine Sukary-Navarro. "Their goal is unambiguous: to undermine Israel's economic stability by targeting its corporate infrastructure.", she concluded.

Volunteering our services, we found ourselves at the forefront of Israel's cyber-defence, thwarting a destructive data-wiping onslaught orchestrated by these malicious actors. Given that the impact of recent security breaches in Israel is fairly broad and manifests in various forms, this article will zero in on our discovery of a new Wiper malware - "[Bibi-Linux](#)" and its surrounding evidence. The aim is to profile the hacker coalitions behind this menacing campaign, delineating their roles and techniques within this concerted effort to compromise Israeli organizations.

Unravelling The Campaign

In October, our Incident Response team voluntarily addressed a complex security breach that led to significant data destruction effecting numerous companies. The targets included an Israeli data-hosting company and defence contractors. During our forensics investigation, we uncovered a new data-wiping malware, which we are tracking as **BiBi-Linux**. We've

published a comprehensive analysis of this Wiper on our blog, along with other concerning attack characteristics. Corroborating our findings, security firms such as ESET have identified and shared detailed about the Wiper's Windows variant, named bibi.exe.



Figure 1. ESET discloses bibi.exe, the Windows version of BiBi-Linux Wiper

According to a LinkedIn post by Senior Director of CTI at BlackBerry, Dmitry Bestuzhev, the Windows version found by ESET was compiled on Benjamin Netanyahu's birthday, October 21st. An interesting fact.



Figure 2. LinkedIn article by Dmitry Bestuzhev showing the Wiper's compiler timestamp

As a response to these discoveries and in light of the ongoing conflict, we decided to launch a research mission aimed at unravelling the threat actor responsible for these attacks.

Our investigation not only led us to a new and suspicious hacktivist group but also exposed a larger campaign targeting Israeli companies with the deliberate intent to disrupt their day-to-day operations using data destruction. The alleged primary goal appears to be undermining Israel's cybersecurity and identifying defence contractors. We have reason to believe that these groups may have links with previously attributed Iranian hacker groups due to several overlaps in recent TTPs.

To initiate the investigation, our team searched for key pieces of evidence related to the attacks, including mentions by various anti-Israeli hacktivist groups of an IP address that had been flagged by us as a potential entry point in one security breach we volunteered to assist in. Following the trail of shared messages, we traced back to the first group that published the incriminating details, a new Telegram channel named Karma.

Karma Is A [Hacktivist Group]

The Telegram channels of the group, who refer to themselves as “Karma”, surfaced on Saturday, October 7, 2023, coinciding with the tragic events experienced by Israel when Hamas terrorists infiltrated the Gaza Strip. The hacktivist group used the slogan "Bibi will shatter our dream of turning 80", likely in reference to Israel's current Prime Minister, Benjamin Netanyahu ("Bibi"), and the country's upcoming 80th anniversary in 2028. While

the slogan appears to be written from a subjective view ("our dream"), the breach revealing the Bibi-Linux Wiper began at the same day, inside the offices of one of the data hosting's clients. Servers were wiped, rendered unbootable, machine names altered to "NO2BIBI", and even printers were sent instructions to mass-print the group's logo and slogan. Two main channels were covering these breaches, both of which had the name of the group, but were recently deleted. Our team was able to copy the entire contents of these channels, along with information collected from the breach and build a hypothesis around the attacker's profile.

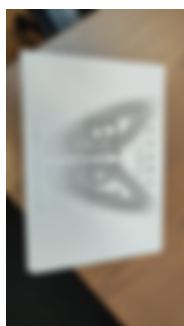


Figure 3. Printers received instruction to mass-print the logo and slogan of Karma

This association suggests pro-Palestinian motivations, further supported by the group's open claims of responsibility for multiple attacks targeting Israeli organizations. We have reasons to believe that Karma did the maximum efforts to camouflage themselves as an Israeli hacktivist group motivated at disinformation about Israel's Prime Minister.



Figure 4. Telegram channel message declaring a data-wiping campaign

Zooming In On Similarities

While the investigated attack using Bibi-Linux primarily focused on spreading a Wiper within the victim's network, some of the Karma self-published attacks involved manual data deletion. Interestingly, Karma is not the only group employing such wiping methods. Our team's in-depth open-source intelligence (OSINT) investigation also revealed similar modus operandi used by other hacktivist groups, notably the Iranian-linked APT - [Moses Staff](#).



Figure 5. Mass-deletion of Government email data by hackers

Much like Karma, this group voluntarily published a video claiming responsibility for an attack on a different Israeli data-hosting company, demonstrating threat actors manually deleting disks from iDRAC servers, which were also involved in the Bibi-Linux incident, albeit for lateral movement rather than being the primary target. Moses Staff labelled this operation as "Mission: Data Destruction".

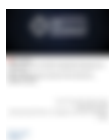


Figure 6. Moses Staff labelling their campaign as "Mission Data Destruction"

Reviewing Karma's social media activity, it is evident that their Telegram channel is currently their sole means of public communication, unlike many other hacktivist groups that maintain websites / Tor-sites, forums, paste-bins, and more. Similarly, Moses Staff's website appears inactive, with operations listed up to the Hamas-Israel war of 2023. This approach has proven challenging for hacktivist groups like Moses Staff, as their Telegram channels and groups frequently get taken down by the platform. In a similar manner, Karma has seen several versions of their channels - all using variations of the handle "KarmaBelow80" - removed multiple times, relying heavily on a single Telegram user to forward messages to new versions of their channels in this unstable form of public communication. The use of a single user raises questions around the identity behind the user and their link to other groups.

Besides their notable presence on social media and the other above-mentioned, these two groups exhibit several shared characteristics that underscore their similarities. They both share the objective of causing disruption to Israeli operations through data destruction. Their evident pro-Palestinian motivations align their actions with this cause. Additionally, the timing of their current activities coincides with significant events, highlighting a strategic approach. They show similar breach tactics and chose similar hardware management management toolset iDRAC as target, along with other noticeable TTPs.

Here's a brief summary of some of the shared attributes:

Recent Parameters	Karma	Moses Staff
Origin	Unknown	Iran
First Seen	October, 2023	<u>October, 2021</u>
Activity Period	Reinitiated media presence during the Israel-Hamas conflict	Reinitiated media presence during the Israel-Hamas conflict
Communications	Telegram	Telegram (website found inactive)
Motivation	Pose as Anti-Israel right wing, specifically targeting Prime Minister Bibi.	Pro-Palestine, targeting Israel and its government agencies.
Objectives	Harming Israeli operations No demands or extortions No negotiations	Harming Israeli operations No demands or extortions No negotiations
Victimology	Israeli organizations of the following industries: - IT and data-hosting companies - Government / Homeland Security	Israeli organizations of the following industries: - IT and data-hosting companies - Government / Homeland Security

Modus Operandi

- Initial access via publicly-exposed administrative panels
- Leaking their breach to their channels live
- Deploying “Bibi-Linux” Wiper
- Lateral movement towards iDRAC servers
- Wiping data using both Wiper (“Bibi-Linux”) and manual deletion
- Known modus operandi from previous campaigns consists of initial access by exploiting vulnerabilities in publicly-exposed administrative panels
- Leaking their breach to their channels live
- Lateral movement to iDRAC servers, with them being the attack’s main target
- Wiping of servers via iDRAC console
- Previous campaigns have been showing proof of incorporate destruction-driven malware

While no conclusive evidence linking these two groups together has been established thus far, the overarching theme of the narrative is evident that an ongoing campaign involving multiple hacktivist groups openly striving to disrupt the operations of Israeli organizations through the use of data-wiping techniques. Although the campaign has primarily centered around Israeli IT and government sectors up to this point, some of the participating groups, such as Moses Staff, have a history of simultaneously targeting organizations across various business sectors and geographical locations. These discoveries added significance with recent findings of additional data-wiping activities involving Iranian hacking groups.

Recommendations

Recent breaches have underscored the significant impact of data-wiping campaigns amidst political conflicts. With the rise in conflict, hacktivist activity and cyber-attacks have increased, escalating the associated risks. We advise organizations to perform a thorough External Attack Surface Assessment to detect and fix any exposed administrative interfaces. Enabling MFA for all employees and boosting cybersecurity awareness is also paramount.

Security Joes is widely recognized for disclosing technical details of new malware strains. BiBi-Linux (23bae09b5699c2d5c4cb1b8aa908a3af898b00f88f06e021edcb16d7d558efad), among other malicious artifacts, has been documented and is now recognized and blocked by EDR systems. Companies should consult with their EDR providers to ensure that these defenses are actively mitigating threats.



Figure 7. Detections of BiBi-Linux surge since the publication, from 2/63 to 37/63

It is crucial to monitor all security controls 24x7x365 and constantly improve security posture to prevent from such devastating results. Ensure proper continuous threat hunting, asset and vulnerability management, alongside recurring Red Team activities, Compromise Assessment & External Attack Surface assessment.

The abovementioned, and more, could be found in our multi-layered Incident Response plan and comprehensive MDR (Managed Detection (and Response) operations. You may contact us via response@securityjoes.com or fill up the [Get-A-Quote form](#).