Issue Brief

March 2026
No : 493

The Ashen Lepus Playbook: Hybrid Warfare,Digital Psyops, & India's Emerging Security Challenge

Govind Nelika

The Ashen Lepus Playbook: Hybrid Warfare, Digital Psyops, and India's Emerging Security Challenge

Govind Nelika

Abstract

The evolution of hybrid warfare tactics has emerged as a serious and rapidly expanding threat in the even growing modern cyber landscape, the paper analyses the "Tactics, Techniques, Procedures" employed by non-state threat Actors like Hamas, the new Psyops measures employed and how countries like The Republic of India should be concerned about such develiopments.

Read more: Hybrid Warfare, Ashen Lepus, WIRTE, Molerats, Gaza Cybergang, Psyops

Introduction

In the new day and age of Hybrid Warfare, the cyberspace stands as a key playground, with Offence and Defence being the core of the argument. While Threat Actor's sponsored by Sovereign Countries are one thing, even smaller entities, such as **Harakat al-Muqāwamah al-ʾIslāmiyyah** or **Hamas**, as it popularly known. The actions of such groups change the dynamics, because not only is the group utilising the cyberspace to collect information on diplomatic envoys, it has also utilises advanced malware to conduct psyops on targets.

The fact that Hamas in itself is capable on conducting such operations, raise's grave concern for countries all over, while India does not classify Hamas as a Terrorist organization, its activity before the Pahalgam Attacks, notably of April 2025 is of concern. According to the "Times of India" report (ET, 2025) two months before the Pahalgam Terror Attacks, senior Hamas officials had travelled to Pakistan Occupied Kashmir (PoK) namely Khalid Qaddoumi, Naji Zaheer, accompanied by leaders Mufti Azam and Bilal Alsallat, they attended the rally **"Kashmir Solidarity and Hamas Operation Al Aqsa Flood",** to be noted further it is said by security officials that as a deliberate move to link Pakistan's Jihadi campaign in Kashmir with Hamas's struggle against Israel, portraying both as **"resistance against occupation."**

Now we will dive into the analysis of Ashen Lepus, please bear in mind while the "Ashen Lepus" classification is of Unit 42 of Palo Alto Networks the Threat Actor is also tracked as

WIRTE group, and is linked to the Gaza Cybergang, a suspected Hamas-aligned cluster said to identified as the Cyber Arm of Hamas.

Ashen Lepus Campaign – Modus Operandi

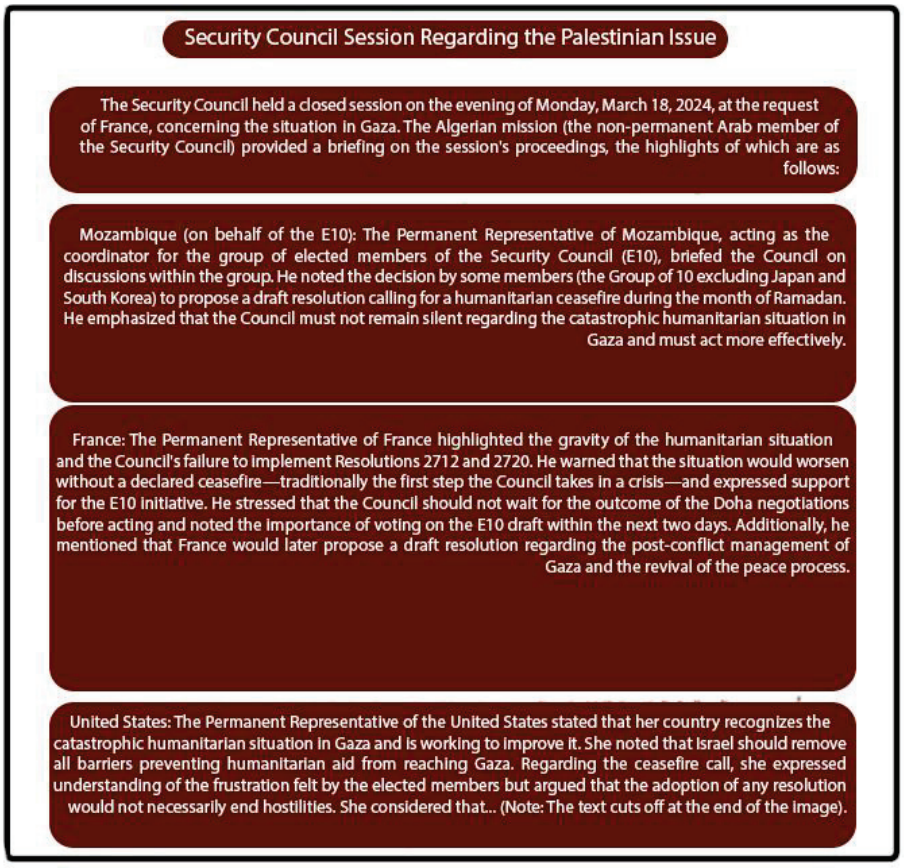
Tracked as WIRTE/Molerat , the Ashen Lepus campaign is identified by Unit42 of Palo Alto Networks(Unit 42, 2025) and attributed to Hamas, the threat Actor is considered to be a division of the Gaza Cyber Gang,(Milenkoski, 2023) the supposed cyber division of Hamas, and is known to be active as far back as 2018, first tracked by LAB52 (Lab52, 2019a), they were initially identified and tracked as WIRTE, the group utilises social engineering tactics (Lab52, 2019b) to acquire initial access, Lures, written in Arabic with subject matter containing political, economic, diplomatic and military developments in the Middle East/West Asia, samples are identified as under:

م/ جلسة مجلس الامن بشأن القضية الفلسطينية

عقد مجلس الامن جلسة مغلقة مساء الاثنين 2024/3/18، بناءة على طلب فرنسا، بشأن الوضع في غزة، وقدمت بعثة الجزائر (العضو العربي غير الدائم في مجلس الامن) إحاطة عن مجريات الجلسة وفي ادناه أهم ما جاء فيها:

- قدم الممثل الدائم لموزمبيق، بصفته منسقاً لمجموعة الأعضاء المنتخبين في مجلس الأمن (E10)، إحاطة للمجلس بشأن مضمون المناقشات التي دارت داخل المجموعة وقرار بعض أعضائها (مجموعة 10 ناقص اليابان وجمهورية كوريا) بعرض مشروع قرار يدعو إلى وقف إطلاق النار لأسباب إنسانية خلال شهر رمضان. وذكر بتوجب على المجلس ألا يلتزم الصمت إزاء الحالة الإنسانية الكارثية في غزة؛ بل يجب أن يكون أكثر فعالية.
- أشار الممثل الدائم لفرنسا بخطورة الوضع الإنساني، وإلى فشل مجلس الأمن في ضمان تنفيذ قراريه 2712 و2720. وإن الوضع سيزداد تدهوراً إذا لم يتم إعلان وقف إطلاق النار، الخطوة الأولى التي يدعو إليها مجلس الأمن عادة في حالة حدوث أزمة. وأعرب عن تأييد بلاده لمبادرة E10. وشدد على أنه ينبغي لمجلس الأمن ألا ينتظر العملية الجارية في الدوحة قبل أن يتصرف. وفي هذا الصدد، أشار إلى أهمية التصويت على مشروع E10 خلال اليومين المقبلين مع مقارنته بالمفاوضات حول مشروع القرار الذي دعا إلى وقف إطلاق النار في السودان. وإن بلاده ستقترح لاحقاً مشروع قرار بشأن إدارة غزة بعد انتهاء الصراع وإحياء عملية السلام.
- أوضحت الممثلة الدائمة للولايات المتحدة إن بلادها تدرك الحالة الإنسانية الكارثية في غزة ولا تدخر جهداً لتحسينها. وعلى هذا النحو، ينبغي على (إسرائيل) أن تزيل جميع الحواجز التي تحول دون وصول المساعدات الإنسانية إلى غزة. وفيما يتعلق بالدعوة إلى وقف إطلاق النار، ذكرت بأنها تتفهم إحباط الأعضاء المنتخبين، لكن اعتماد أي قرار لن يدفع الأعمال العدائية. واعتبرت أن

Sample Figure 0.1 – Original text Lure Utilized in the Campaign



Security Council Session Regarding the Palestinian Issue

The Security Council held a closed session on the evening of Monday, March 18, 2024, at the request of France, concerning the situation in Gaza. The Algerian mission (the non-permanent Arab member of the Security Council) provided a briefing on the session's proceedings, the highlights of which are as follows:

Mozambique (on behalf of the E10): The Permanent Representative of Mozambique, acting as the coordinator for the group of elected members of the Security Council (E10), briefed the Council on discussions within the group. He noted the decision by some members (the Group of 10 excluding Japan and South Korea) to propose a draft resolution calling for a humanitarian ceasefire during the month of Ramadan. He emphasized that the Council must not remain silent regarding the catastrophic humanitarian situation in Gaza and must act more effectively.

France: The Permanent Representative of France highlighted the gravity of the humanitarian situation and the Council's failure to implement Resolutions 2712 and 2720. He warned that the situation would worsen without a declared ceasefire—traditionally the first step the Council takes in a crisis—and expressed support for the E10 initiative. He stressed that the Council should not wait for the outcome of the Doha negotiations before acting and noted the importance of voting on the E10 draft within the next two days. Additionally, he mentioned that France would later propose a draft resolution regarding the post-conflict management of Gaza and the revival of the peace process.

United States: The Permanent Representative of the United States stated that her country recognizes the catastrophic humanitarian situation in Gaza and is working to improve it. She noted that Israel should remove all barriers preventing humanitarian aid from reaching Gaza. Regarding the ceasefire call, she expressed understanding of the frustration felt by the elected members but argued that the adoption of any resolution would not necessarily end hostilities. She considered that... (Note: The text cuts off at the end of the image).

Sample Figure 0.1 – Machine Translated (done by Author)

الأمانة العامة
امانة شؤون مجلس الجامعة

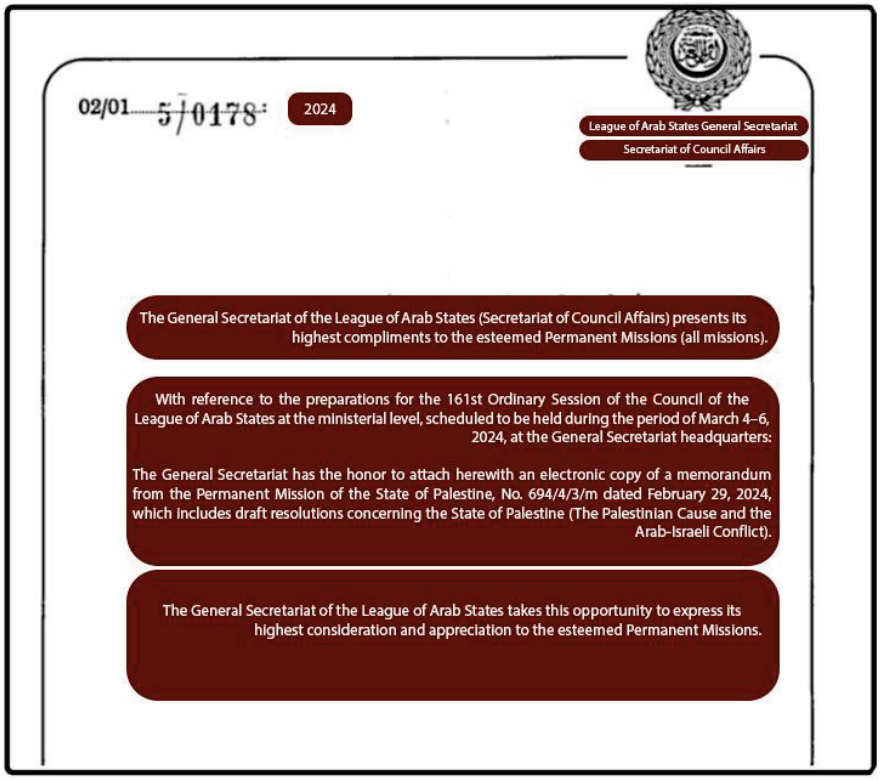
الرقم: 5/0178 02/01

تهدي الأمانة العامة لجامعة الدول العربية (أمانة شؤون مجلس الجامعة) أطيب تحياتها إلى المندوبية الموقرة (جميع المندوبيات)،

بالإشارة الى الاعداد والتحضير للدورة العادية (161) لمجلس جامعة الدول العربية على المستوى الوزاري المقرر عقدها خلال الفترة 4-2024/3/6 بمقر الأمانة العامة، تتشرف بأن ترفق-مع هذا- نسخة الكترونية من مذكرة المندوبية الدائمة لدولة فلسطين رقم م/694/4/3 بتاريخ 2024/2/29، المرفق بها مشاريع القرارات الخاصة بدولة فلسطين (القضية الفلسطينية والصراع العربي الإسرائيلي).

وتغتنم الأمانة العامة لجامعة الدول العربية هذه المناسبة لتعرب للمندوبية الموقرة عن فائق الاعتبار والتقدير.

Sample Figure 0.2 – Original text Lure Utilized in the Campaign



Sample Figure 0.2 – Machine Translated (done by Author)

Modus Operandi

The above lures, set by **Ashen Lepus** are a textbook example of how **social engineering** tactics are utilised to bypass modern security. Rather than using generic **"clickbait,"** these attackers have crafted highly specific lures tailored to the interests of diplomats and politicians, persons of interest and stakeholders following the Israel-Hamas conflict. This is a deliberate strategy: by choosing a topic of intense professional focus, they significantly increase the likelihood that a busy official will overlook the usual subtle technical red flag.

The technical deception works like a digital shell game. A victim receives a PDF that appears legitimate but contains a link to a file-sharing service. When they click to view the document, they unknowingly trigger the download of a hidden "binary" file. As the PDF opens for the user, a secondary piece of code a "**DLL file**" s side-loaded in the background. This technique is particularly effective because it hitches a ride on standard, trusted computer processes to avoid detection. Once this foothold is established, the system connects to the attackers "command and control" server to install **AshTag**, a surveillance suite designed to sit silently on the network. To ensure they aren't removed when the computer restarts, the malware schedules itself as a recurring system task, effectively hiding in plain sight.

While it mirrors an aspect of surveillance capabilities similar to Pegasus, the end goal may well be different. This isn't just about a quick data theft; it is about "**persistence"** maintaining a long-term presence within designated diplomatic circles, the APT monitors internal discussions. In the world of diplomacy & counterintelligence, having a permanent "fly on the wall" provides a massive advantage, allowing one to anticipate their opponent's moves or gain leverage in critical negotiations long before formal meetings ever begin.

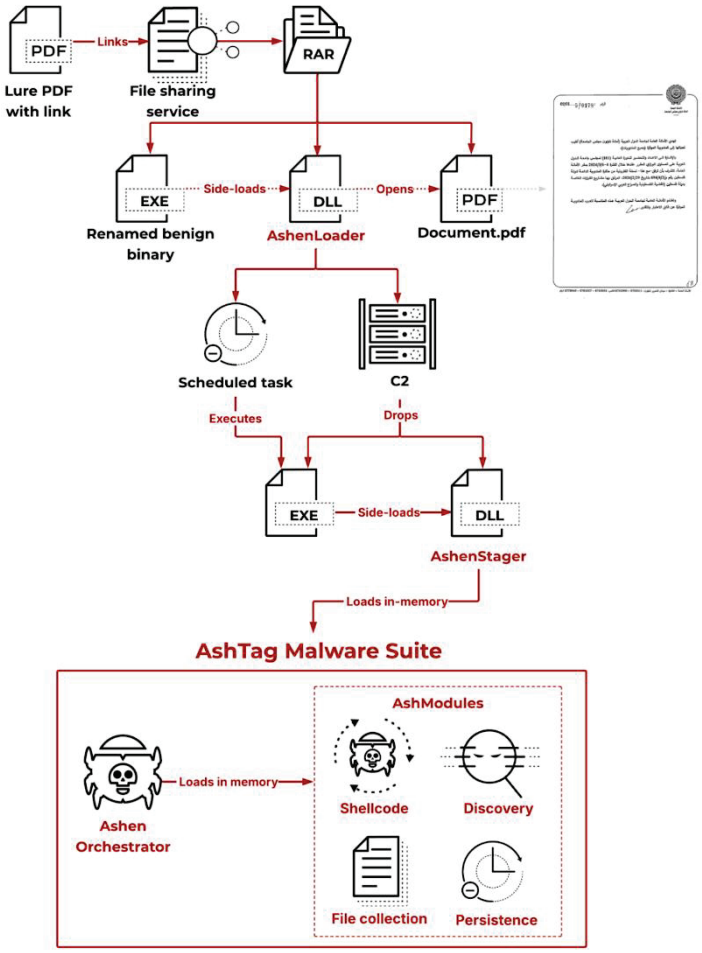


Figure 0.3 Ashen Lepus Modus Operandi (Unit 42, 2025)

As one seen above from the figure 0.3 the emergence of the AshTag campaign represents a shift from the traditional tactics of used Ashen Lepus. In earlier efforts, the group's activities seemed unfinished, they would start an operation but shut it down before delivering their main software tools. This new pattern suggests those previous attempts were likely trial runs, where the actors were essentially practicing their techniques in the real world to see what worked on which architecture with the AshTag Campaign, they have since, moved beyond practice to a fully functional, modular toolkit that allows them to steal files, download new instructions, and run malicious code directly in a computer's memory to avoid detection.

The system is essentially tricked into loading a series of hidden files, loaders and stagers that act like a digital "bridge," gradually bringing the full AshTag malware into the system. Once the breach is complete, the software schedules itself to run automatically, ensuring persistence is maintained. Over the last two years, the APT has maintained a relentless pace of intelligence gathering. Their approach is prioritizing a **"low-cost, high impact"** philosophy over technical flashiness. The group's latest toolkit, a flexible system nicknamed **"AshTag,"** identified by Unit 42 provides them with a modular way to steal sensitive information and take control of systems remotely. One must be aware of the threat that is increasingly adept at hiding in plain sight by exploiting the very systems we trust (Unit 42, 2025).

Use of Psyops in Grey Zone

For decades, Psychological Operations, in warfare often called **"PsyOps"** for short, was utilised almost exclusively by the world's most powerful nations. Major military powers, such as the United States and the United Kingdom, had specialized units throughout the 20th century specifically to master the craft of information warfare and counterintelligence i.e the PSYWAR School of U.S Army, (United States Army, n.d.) the 77th Brigade Information Operations of the British Army (The British Army, n.d.). However, the digital revolution has fundamentally shattered this monopoly, the rise of social media and artificial intelligence has set the stage, even relatively small organizations are presently capable of launching sophisticated influence campaigns with minimal efforts and in some instances these campaigns rival countries, especially in case of Hamas there was no shortage of funds or resources i.e support from **Islamic Republic of Iran** for example. These actors operate in the **"Grey zone,"** where accountability and attribution to a particular entity can only be inferred or at best guessed. The line between Political tension and open military conflict are intentionally blurred to create confusion. Instance of such are abundant by blending technical cyber-attacks with psychological tactics during the Hamas-Israel conflict, the WIRTE Threat actor has demonstrated how modern digital tools can be used to incite social chaos and deepen existing divisions. This represents a significant turning point: the power to destabilize a region through information is no longer reserved for superpowers, we will examine a specific case that that showcases this very phenomenon.

We will take the case of the malware campaign tracked as same coin, identified in 2024, by "**IntezerLab"** (Nicole, 2024) the initial point of infection as published by Intezerlabs is an email impersonating as the "**Israel National Cyber Directorate"**

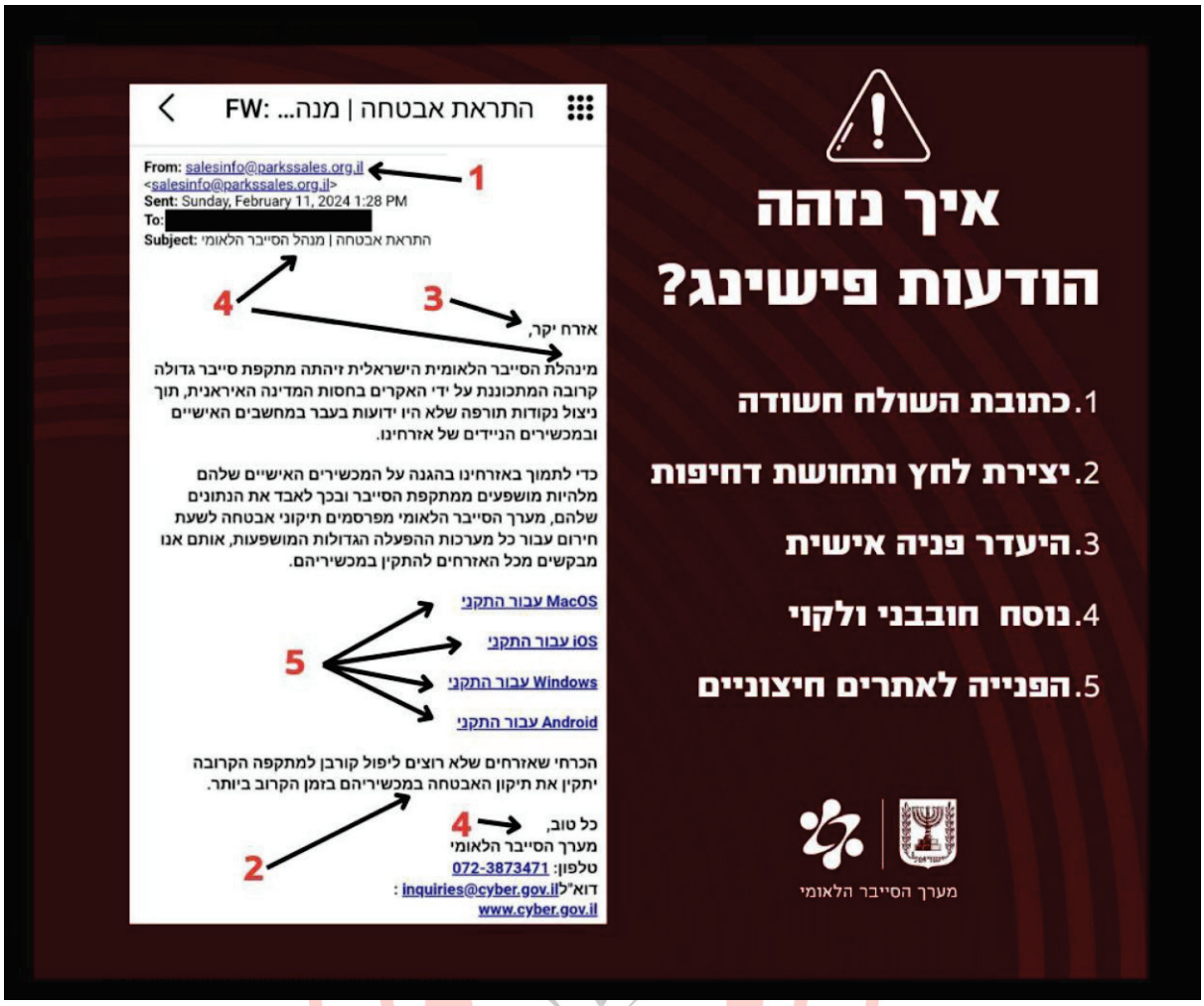


Figure 0.4 (Nicole, 2024) The sample provided by **IntezerLab**

The sample provided above has a specific lure, the identified markers 1 to 5, the rough translation of the email is

"The Israeli National Cyber Directorate has issued an urgent warning regarding an imminent, state-sponsored cyberattack originating from Iran. This sophisticated campaign targets previously unknown vulnerabilities in both personal computers and mobile devices to compromise citizen data. To mitigate this threat, the Directorate has released emergency security patches for major operating systems, including MacOS and Android. It is highly recommended that all users install these updates immediately via the official government portal at ***www.cyber.gov.il*** *to secure their devices against potential exploitation."*

The email urges the recipient to download and update patches to their systems, while some of the links, are genuine, the MacOS and Android applications links in the malicious emails are infected with a wiper. The malware dubbed "Samecoin" was analysed by Harfanglabs is a Paris-based cybersecurity company founded in 2018 by former ANSSI and French Ministry of Armed Forces experts. Their detailed analysis brought out the sophistication

of malware, their analysis found that the malicious files were made available through Gofile a legitimate public files hosting service. The Virus total graph of the SHA-256 556b5101e0e8aee004bed89f1686ce781a075fde5a8a86fa5409fe34a2d1b6d9 is as under for reference.

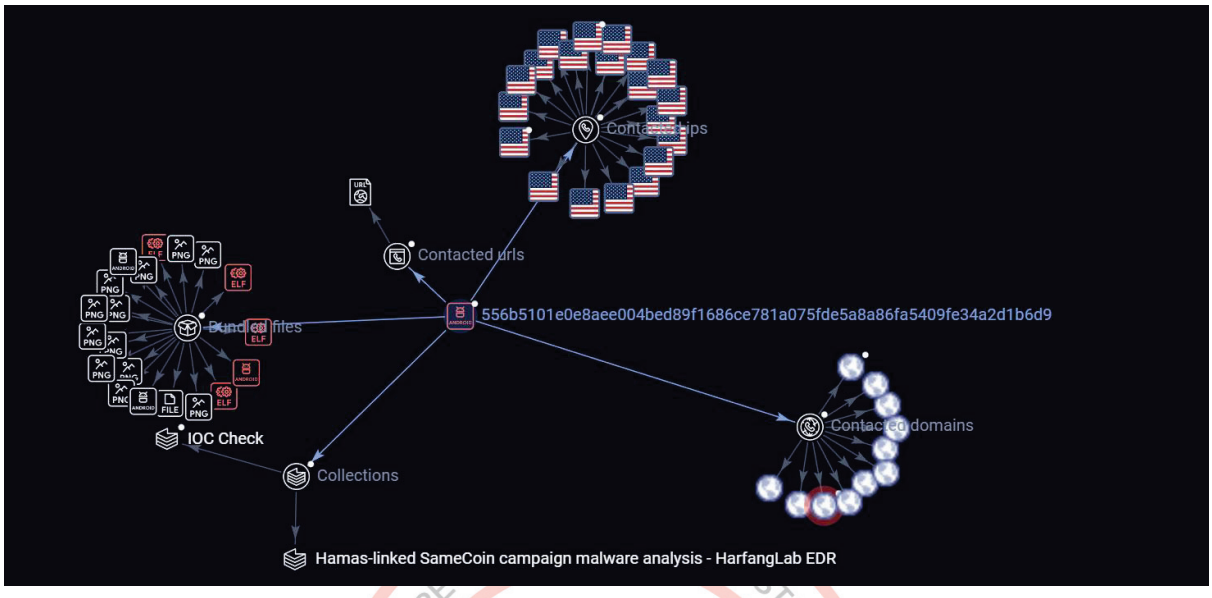


Figure 0.5 (VirusTotal, n.d.)

The above graph is available on Virus Total

The analysis done by Harfanglabs, gives a detailed analysis of the conditions required for malware to activate, which makes it more interesting and dangerous.

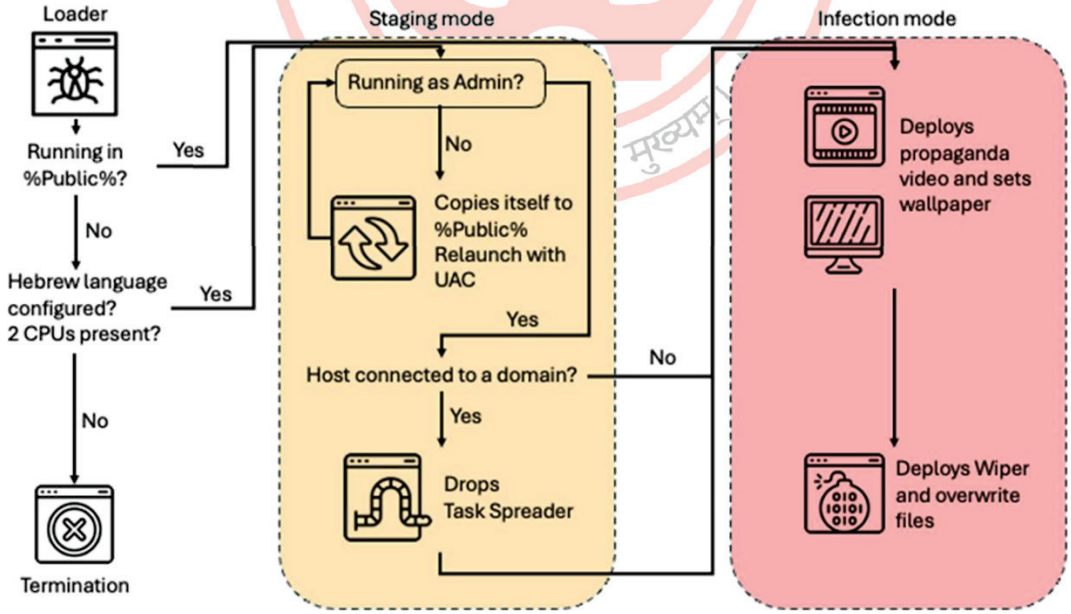


Figure 0.6 (HarfangLab, 2024)

Once the malware stages itself, it checks if the system is viable in terms of functional CPU's to ensure, it hasn't landed in a security researchers' sandbox, however as seen above it also check for registry keys if one of the configured keyboard layouts corresponds to Hebrew,

making sure it's the intended victim. Once confirmed, it hijacks administrator privileges to deploy a data-destroying "wiper," spreads through the network, and creates a chaotic scene by maxing out the system volume, playing propaganda, and forcing a specific desktop wallpaper. Compiled on October 7, 2023, the malware was designed to combine focused cyber-attack with psyops tactics. The wallpaper is altered for one which showcase's warning of Hamas to IDF.

Sample - Figure 0.7, (HarfangLab, 2024)

While the image itself was widely used well before the malware campaign, (Planet Report HQ, 2023) and the malware goes one step further after altering the wallpaper it then proceeds to show video footage specifically designed to stir internal conflict in Israel by turning the families of hostages against Prime Minister Netanyahu. This campaign is a digital extension of Hamas's propaganda strategy, focused on fuelling tensions further.

Sample - Figure 0.8, (HarfangLab, 2024)

By using consistent branding such as the "Military Media" highlighted in the left-hand side red box and the inverted red triangle emoji (Al Jazeera, 2023) (" 🔻 ") refer figure 0.7, which is

used to symbolize Hamas combat operations and targeting IDF groups, while the Samecoin malware, has not in particular been attributed to a specific entity, the approach used is similar to a threat Actor which has been active tracked by various classification some notable one's are "Desert Falcons, Mantis, Arid Viper, Grey Karkadann, Big Bang, APT-C-23, Two-tailed Scorpion as detailed by Mitre Database. The group is known for its high-quality psychological lures, relatively simple malware, and the ability to target both Android and Windows users simultaneously using techniques established as far back as 2021. The Theat actor in itself has been active for some time, going as far back as 2013, identified as Desert Falcons, by Kaspersky Securelist, (Ghareeb & Mohamad Amin, 2015). The APT utilizes specialized social engineering tactics to further their agenda. Their targets vary but are largely focused on the Middle East, namely Palestine, Egypt, Israel as tracked refer figure 0.9.

Figure 0.9, (Ghareeb & Mohamad Amin, 2015)

The lures, crafted and the overall sophistication of the malware indicate the Threat Actor, behind Samecoin might well be Desert Falcons, however one cannot attribute the malware campaign to them with absolute certainty, but the similarities are clear "**multi-platform payloads**, **language-based activation triggers**, and **highly targeted social engineering"** strongly align with the known TTPs (Tactics, Techniques, and Procedures) of the Desert Falcons or their affiliated subgroups.

How this effects India

While some might wonder how the actions of groups like Hamas any bearing on the Republic of India in any sense have, what's worrying is the Link between groups like Hamas, and Pakistan. At the introduction of the article, I had pointed out the visit of Senior Hamas official's in Pakistan occupied Kashmir (PoK), prior to the Pahalgam Attack, even if some analysts dismiss that statement, the Palestinian BDS National Committee (BNC), the coalition of Palestinian organisations that leads and supports the BDS movement, their own statement likens the Palestinian State's condition and Kashmir and has strong opposition to the abrogation of Article 370 by the Government of India(BDS, 2019a, 2019b).

While the link between the movement in itself may seem harmless, the targeted use of the malware against a specific demographic, is the cause of concern, for a country like India, the targeted use of such malware, designed specifically to propagate information to a target based on the targets native keyboard layout is the all the more alarming.

India while largely holds Hindi (Devanagari script) and English as the official languages for union government proceedings, our nation is home to 22 Base languages and even more dialects, this internal diversity which is our pride in one aspect holds a significant surface area for exploitation. If a localized malware or disinformation campaign were tailored, it could essentially work towards escalating tensions along lines of caste, creed, and community sowing discord and fanning embers. Depending upon the Psyops approach the effects may not even be immediate, a harmless, suggestion on your favourite news app, of a case of communal violence, a seemingly harmless notification of a news article describing a case of a targeted killing of Sect leader or Politician and targeted violence in a district, all of it may contribute to escalating tensions. In an era where AI models functionally allow anyone to manipulate and automate info ops, fabricated content becomes indistinguishable from reality, any digital artifact or medium of communication, be it a podcast, video, or short-form article, can be weaponized to manipulate public perception and erode social cohesion.

Conclusion

The evolution of the **Ashen Lepus** campaign (WIRTE/Molerat) and the **Samecoin** malware represent a fundamental shift in the landscape of modern conflict. The hybrid warfare domain has spilled over to Cyber Grey Zone, The Ashen Lepus approach showcases how non-state actors can now maintain a permanent **"fly on the wall"** presence within high-level

diplomatic circles and weaponize digital media and use Psyops tactics coupled with technical expertise to incite social discord.

For a nation as linguistically and culturally diverse as **India**, this playbook presents a grave security challenge. The potential for malicious actors to exploit internal fault lines through automated, AI-driven disinformation is no longer a **"theoretical"** risk, it is a clear and present danger. By targeting specific communal or linguistic identities, adversaries seek to turn India's digital connectivity into a catalyst for social erosion using our own social structure as a possible vector.

The path forward requires a transition from reactive damage control to a **predictive defence model**. While current administrative measures, such as monitoring social media and enforcing data-sharing compliance for applications, have successfully insulated India from the chaos which was seen recently in our neighbourhood, i.e. Nepal and Bangladesh, the "AI-malware" mix demands a more nuanced approach. The state must deploy **localized Large Language Models (LLMs)** may be sourced such as **"Sarvam"** and several others showcased during the AI Summit. These indigenous tools should be integrated to analyse threat dialogue and dialects, on social media & news platforms. It is essential for neutralizing deepfakes and bot-driven narratives, which spread misinformation, i.e Indias social media handles were filled with deepfakes during Op Sindoor, and we should make an effort to curb them at the sources before it reaches the critical mass. Agencies could employ sentiment and speech, text analysis patterns in such cases.

Ultimately, fostering a robust **Public, Private, Partnership (PPP) approach between the Government** and indigenous tech firms is the way forward. It has become a necessary to ensure that our digital borders are as well-guarded as our physical ones. As the line between code and kinetic conflict continues to blur.

References

Al Jazeera. (2023, November 13). *What's the red triangle being used by pro-Palestinian activists?* Al Jazeera. https://www.aljazeera.com/video/newsfeed/2023/11/13/whats-the-red-triangle-being-used-by-pro-palestinian-activists

BDS. (2019a, August 12). *Solidarity and Unity in Opposing Global Militarization: BNC Statement on Kashmir*. BDS Movement.

https://web.archive.org/web/20260109024858/https://bdsmovement.net/news/solidarity-and-unity-opposing-global-militarization-bnc-statement-kashmir

BDS. (2019b, August 12). *Solidarity and Unity in Opposing Global Militarization: BNC Statement on Kashmir*. BDS Movement. https://web.archive.org/web/20260109024858/https://bdsmovement.net/news/solidarity-and-unity-opposing-global-militarization-bnc-statement-kashmir

ET. (2025, April 27). *Hamas leaders met Pakistani terror groups in PoK before Pahalgam attack, says Israel envoy - The Economic Times*. The Economic Times. https://economictimes.indiatimes.com/news/defence/hamas-leaders-met-pakistani-terror-groups-in-pok-before-pahalgam-attack-says-israel-envoy/articleshow/120660630.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

Ghareeb, S., & Mohamad Amin, H. (2015, February 17). *The Desert Falcons targeted attacks*. Kaspersky. https://securelist.com/the-desert-falcons-targeted-attacks/68817/

HarfangLab, C. T. R. T. (2024, February 14). *Hamas-linked SameCoin campaign malware analysis*. HarfangLab. https://harfanglab.io/insidethelab/samecoin-malware-hamas/#Attribution-and-propaganda-contents

Lab52. (2019a, April 2). *WIRTE Group attacking the Middle East*. Lab52. https://web.archive.org/web/20251129020817/https://lab52.io/blog/wirte-group-attacking-the-middle-east/

Lab52. (2019b, May 24). *WIRTE, Group G0090*. MITRE ATT&CK. https://attack.mitre.org/groups/G0090/

Milenkoski, A. (2023, December 14). *Gaza Cybergang | Unified Front Targeting Hamas Opposition*. SentinelOne. https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/

Nicole. (2024, February 12). *Today, a malicious campaign impersonating the Israeli National Cyber Directorate (@Israel_Cyber)*. X Formerly Twitter. https://x.com/NicoleFishi19/status/1756936902735806644?s=20

Planet Report HQ. (2023, December 9). *Planet Report HQ on X: "PSIL | Hamas to IDF: You entered alive, you will come out torn to pieces!* X Formerly Twitter. https://x.com/PlanetReportHQ/status/1733233812857836020

The British Army. (n.d.). *77th Brigade*. UK MoD. Retrieved January 26, 2026, from https://www.army.mod.uk/learn-and-explore/about-the-army/formations-divisions-and-brigades/field-army-troops/77th-brigade-information-operations/

Unit 42. (2025, December 11). *Hamas-Affiliated Ashen Lepus Targets Middle Eastern Diplomatic Entities With New AshTag Malware Suite*. Palo Alto Networks. https://unit42.paloaltonetworks.com/hamas-affiliate-ashen-lepus-uses-new-malware-suite-ashtag/

United States Army. (n.d.). *PSYWAR School*. Retrieved January 26, 2026, from https://www.swcs.mil/Schools/PSYWAR-School/

VirusTotal. (n.d.). *Samecoin Malware Graph*. Virus Total. Retrieved February 1, 2026, from https://www.virustotal.com/graph/g196243a500e1432481b4c02974e0a4edbdb20939e3d74baeaaa1121c4da171f2

CENTRE FOR LAND WARFARE STUDIES
CLAWS
अन्वेषणं ज्ञानस्य मुख्यम्

About the Author

Govind Nelika is the Web Manager/Researcher at the Centre for Land Warfare Studies (CLAWS). He is an alumnus of Pondicherry Central University with a degree in Political Science complemented by a certification in Data Sciences from IBM. His research approach is multidisciplinary in nature, and his focus area at CLAWS is on emerging challenges and trends in the fields of Cybersecurity, OSINT, and the evolving landscape of Strategic Technology, synergized with Generative AI and LLM. In recognition of his contributions, he was awarded the Chief of Army Staff (COAS) Commendation Card on Army Day 2025 for his work with CLAWS.

All Rights Reserved 2026 Centre for Land Warfare Studies (CLAWS)

No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from CLAWS.

The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.