Dark Web Profile: Cyber Toufan Al-aqsa

Published: 2023-12-20 · Archived: 2026-04-02 12:12:13 UTC

On November 16 2023, a new group emerged in the intricate web of modern cyber warfare: Cyber Toufan. This group, shrouded in the digital shadows, has recently gained notoriety for a series of aggressive cyberattacks predominantly targeting Israeli organizations.

Threat Actor card of Cyber Toufan Al-aqsa

Cyber Toufan's rapid escalation in the cyber realm mirrors the intensifying geopolitical tensions in the region, particularly between Israel and Hamas.

Cyber Toufan's first post on their Telegram channel on November 18, 2023.

Cyber Toufan's emergence aligns with an era where cyber warfare is becoming an increasingly prominent aspect of international conflicts.

Background and Emergence of Cyber Toufan

Cyber Toufan's inception is a significant event, particularly in the context of the longstanding Israel-Hamas conflict. This group, initially unknown, has quickly made its presence felt by launching cyberattacks against a range of Israeli organizations. The timing of their emergence is noteworthy, coinciding with heightened tensions and hostilities in the region.

The tactics and scale of Cyber Toufan's operations bear the hallmarks of a sophisticated entity, potentially state-sponsored. Their rapid rise and effective execution of complex cyberattacks suggest a level of support and resources that are not typically available to independent hacker collectives. Cybersecurity experts and intelligence analyses have pointed towards **potential Iranian backing**, given the group's style, targets, and the geopolitical narrative underpinning their attacks.

Their first leak was some private keys from Israeli government bodies.

Cyber Toufan's initial activities have been marked by a deliberate and focused approach, targeting high-profile Israeli entities and causing significant data breaches. Their attacks have not only led to substantial data leaks but have also served as a form of digital retaliation, aligning with broader strategic objectives in the region.

This background sets the stage for understanding Cyber Toufan's operational tactics and the wider implications of their cyber campaigns.

Modus Operandi of Cyber Toufan

Cyber Toufan has exhibited a distinct and effective modus operandi in their cyberattacks. Their primary strategy involves extensive data breaches and **the extraction of sensitive information**, impacting both organizations and individuals. Notable tactics include:

Data Extraction and Release: They have been adept at extracting large volumes of data, including personal details like emails, phone numbers, and business interactions. This not only disrupts the operations of targeted entities but also poses significant privacy and security risks to individuals whose data is compromised.

Targeted Organizations: Their choice of targets has been strategic, focusing on Israeli companies and organizations that hold significant value or sensitive information. This includes security firms, government agencies, and commercial entities, indicating a well-thought-out approach to maximize impact.

Propaganda and Psychological Warfare: Beyond technical breaches, Cyber Toufan also engages in psychological warfare, using their cyberattacks to make political statements and spread propaganda. This dual use of technical skill and psychological manipulation underscores their broader strategic objectives.

Alleged Collaboration and Coordination: Reports suggest that Cyber Toufan possibly coordinating with other hacker groups and participating in larger collective operations, indicating a level of organization and collaboration unusual for independent hacking groups. Since in many hashtags and other hacker group's posts they are also tagged and other hacker groups seem to follow their lead in some sense.

Notable Attacks and Breaches by Cyber Toufan

Cyber Toufan's cyberattacks have been widespread and significant, impacting a variety of Israeli and its allied countries' organizations. In just one month, their total leaks reached more than 100. Ransomware.live also tagged them as a ransomware group and listed the group's victims in its list, with 106 victims listed. Of course, although a ransomware attack is not yet known, they seem to have TTPs similar to ransomware groups and the capacity to deploy a ransomware variant if they have it.

Some of the notable breaches include:

> *Many companies were listed before the leaks, for example, Strauss' name was listed in one of their first posts but the leak was published on December 19.*

MAX Security: A Tel Aviv-based security and risk management company, confirmed a breach that led to the exposure of user email addresses.

Bermad: A prominent Israeli water system provider, was purportedly targeted, aligning with heightened regional tensions and resource access issues.

Other Israeli Entities: The group claimed successful breaches of several other organizations, including OSEM (a food company), H&O (a fashion brand), Hagarin (an e-commerce brand), and various government entities.

> *In their first press release, they mentioned many governmental organizations.*

The attacks spanned various industries, from food and fashion to critical infrastructure, demonstrating Cyber Toufan's wide-reaching capabilities. The scale and variety of these attacks underscore Cyber Toufan's significant capabilities and their potential impact on national security and personal privacy.

Alleged State Sponsorship

The operations of Cyber Toufan, particularly their sophisticated cyberattacks, have raised suspicions of **state sponsorship**, with many signs pointing towards Iran. This speculation is bolstered by analyses from cybersecurity experts, such as those at Check Point Software, who have noted similarities in tactics between Cyber Toufan and other Iran-linked groups.

The International Institute for Counter-Terrorism (ICT) also provides insights into this alleged connection, underscoring the potential involvement of a nation-state in Cyber Toufan's activities. The link to state sponsorship, if substantiated, reveals a deeper layer of geopolitical maneuvering, positioning Cyber Toufan within a broader context of regional power dynamics and state-level cyber warfare strategies.

> *Left: Cyber Toufan post on Radware leaks; Right: List of hacking groups operating together against Israel as part of Anonymous Op-Israel (ICT).*

ICT also mentioned the joint work of hacktivist/hacker groups and drew attention to this point. The various groups in the figure targeting Israel have diverse motives and behaviors. Some groups display immature, "troll-like" actions. When state-sponsored actors collaborate with these groups, it could be a strategy to disguise their involvement and make their actions seem less serious or organized. This approach can help obscure the true nature of state sponsorship in cyber activities, or they are simply not sponsored/fully sponsored.

Impact and Consequences

The cyberattacks executed by Cyber Toufan have far-reaching consequences, both in terms of cybersecurity and geopolitical ramifications.

Data Privacy and Security: The breaches have led to significant exposure of personal and sensitive data, affecting countless individuals and organizations. This raises serious concerns about data privacy and the security of personal information.

Economic and Operational Impact: Targeted attacks on key industries and infrastructure have potential economic repercussions and can disrupt critical operations, affecting national security and the economy.

Geopolitical Implications: The alleged state sponsorship of Cyber Toufan adds a layer of complexity to international relations, especially in the Middle East. It signifies the growing use of cyber warfare as a tool in broader geopolitical strategies.

Psychological Impact and Propaganda: The use of cyberattacks for propaganda purposes by Cyber Toufan has a psychological impact, spreading fear and uncertainty, which is an integral part of modern warfare tactics.

The cumulative impact of these activities underscores the evolving nature of cyber threats and the need for robust cybersecurity measures globally.

Conclusion

The emergence and activities of Cyber Toufan in the cyber warfare landscape underscore the critical need for advanced cybersecurity measures. Their sophisticated attacks on Israeli organizations highlight a new frontier in digital conflict, intertwining state-sponsored operations with geopolitical agendas. To combat such threats effectively, SOCRadar's Dark Web Monitoring is essential.

SOCRadar Dark Web Monitoring

This solution comprehensively monitors dark and deep web activities, providing **early warnings** and **actionable intelligence** to prevent or mitigate cyber threats from groups like Cyber Toufan. Organizations can better protect themselves in this evolving cyber battleground by staying vigilant and employing advanced security solutions.

MITRE ATT&CK TTPs of Cyber Toufan

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Description
TA0040: Impact	T1485: Data Destruction	Cyber Toufan's attacks often involve data extraction and leaks, possibly leading to data destruction or manipulation.
TA0043: Reconnaissance	T1595: Active Scanning	Cyber Toufan likely conducts active scanning to identify vulnerabilities in targeted organizations.
TA0042: Resource Development	T1583: Acquire Infrastructure	Given their operational scale, they may acquire infrastructure such as servers to support their activities.
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	Cyber Toufan might use obfuscation techniques to evade detection.
