Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

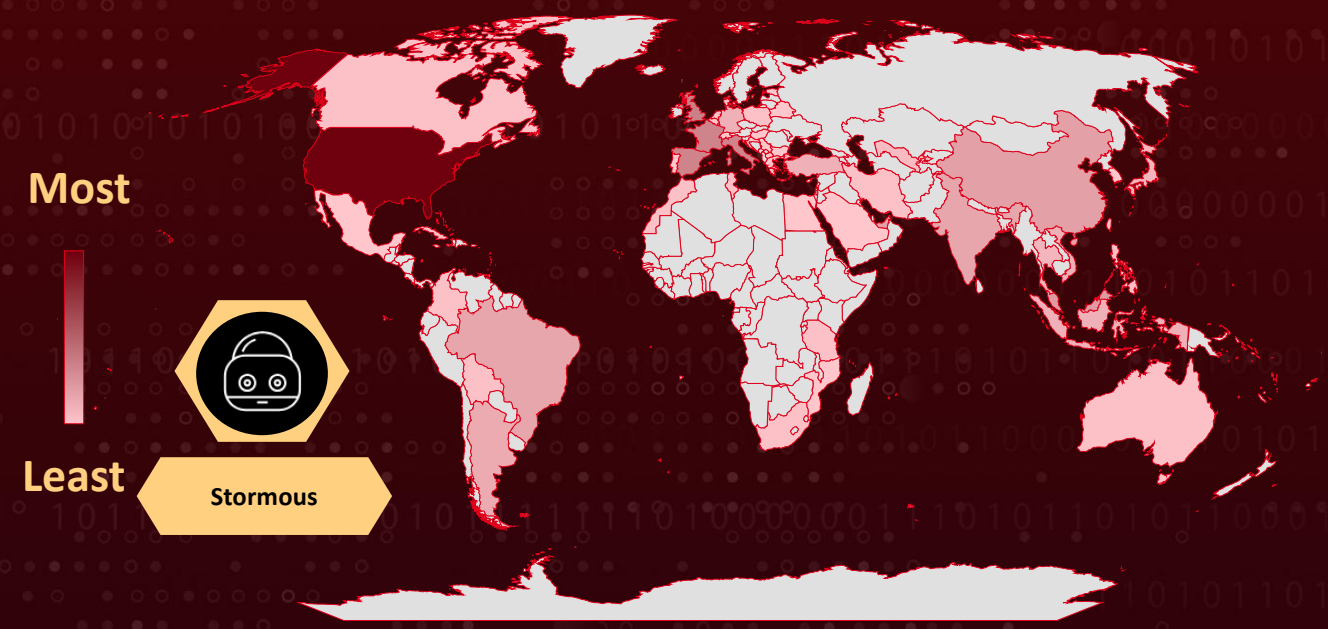
Stormous Extortion Group Announces Shutdown After Four Years of Leak-Site Activity

Date of Publication	Admiralty Code	TA Number
September 17, 2026	A2	TA2026272

Summary

First Seen: 2021
Targeted Regions: United States, United Kingdom, Spain, France, Italy, Malaysia, United Arab Emirates, China, Brazil, India, Argentina, Turkey, Indonesia, Germany, Vietnam, Japan, Thailand, Uzbekistan, Iran, Lebanon, Colombia, Poland, South Africa, Taiwan, Tanzania, Tunisia, Bolivia, Canada, Cuba, Australia, Philippines, Denmark, Netherlands, Morocco, Portugal, Egypt, Croatia, Serbia, Belarus, Singapore, Mexico, Hungary, Bulgaria, South Korea, North Macedonia, Belgium, Greece, Switzerland, Saudi Arabia, Estonia, Mozambique
Targeted Industries: Technology, Business Services & Consulting, Manufacturing, Retail, Hospitality, Education, Healthcare, Telecommunications, Media, Government, Financial Services, Pharmaceutical, Energy, Transportation, Casino & Gambling, Aerospace and Defense, Food Service, Religion, Agriculture, Real Estate, Aviation, Insurance
Malware: StormousX
Threat Actor: Stormous
Attack: Stormous is an Arabic-speaking double-extortion group active since 2021 that gains access through unpatched internet-facing systems, phishing, and weak MFA, then leaks stolen data via a Tor site and Telegram, often without deploying encryption. Trackers record between 179 and 240 claimed victims across manufacturing, education, technology, finance, and healthcare, with the UAE, Brazil, Italy, the US, and the UK most affected, though only a few incidents are independently corroborated and past proofs have included recycled public data. In early July 2026 the group announced it would terminate operations, and all tracked leak-site mirrors are currently offline. Stormous is best assessed as an opportunistic, reputation-driven data-extortion actor whose claims warrant low confidence until victim-confirmed.

Attack Regions



Attack Details

#1

Stormous is an Arabic-speaking extortion group that has claimed to operate as a ransomware gang since 2021, initially publicising attacks through Telegram channels before adding a Tor-based leak site. Its first leak-site listing is recorded on April 12, 2022, and the group has publicly aligned itself with Russia in the Ukraine conflict and leveraged Middle East geopolitical tensions to raise its profile. In July 2023 it announced a partnership with GhostSec targeting Cuban government ministries and relaunched its leak site with a data resale shop and a recruitment page seeking ransomware developers and phishing specialists. The partnership subsequently produced the STMX_GhostLocker ransomware-as-a-service program in 2024, giving Stormous and its affiliates access to the Golang-based GhostLocker 2.0 encryptor alongside its own StormousX.

#2

The group's initial access relies on unpatched internet-facing systems, phishing campaigns, and weak multi-factor authentication. It operates a double-extortion model, threatening both encryption and publication of stolen data, although many incidents involve data theft alone with minimal disruption to production systems, making early detection difficult. Stolen data is distributed through .onion mirrors and legitimate file-hosting services such as mega.nz and gofile.io.

#3

Victimology is broad. Trackers record between 179 and 240 claimed victims, concentrated in manufacturing, education, technology, financial services, hospitality, and healthcare, with the United Arab Emirates, Brazil, Italy, the United States, and the United Kingdom most affected. Credibility remains the central analytical caveat. Only a few incidents between 2022 and 2026 have been corroborated by victim notifications or regulatory filings, and earlier reviews found that some published proof consisted of data already available in dark web forums or open sources. Although working encryptors are documented, recovered samples from Stormous-claimed intrusions remain scarce, and only a handful of corroborated incidents show operational disruption consistent with encryption, leaving it unclear how consistently ransomware is actually deployed.

#4

In early July 2026 the group posted a notice stating it would soon terminate operations, and all six tracked leak-site mirrors are currently offline. Whether this marks a genuine shutdown or a rebrand is unconfirmed, and each new Stormous claim should be treated as attacker-asserted until independently validated.

Recommendations

Harden identity and remote access: Enforce phishing-resistant multi-factor authentication on all remote access, including VPN, RDP and cloud consoles, and eliminate exception accounts. Audit for exposed or reused credentials in infostealer logs and past breach corpora, since a meaningful share of listed victims had employee credentials circulating before being named. Rotate service and administrative passwords on a defined cycle and alert on logins from unfamiliar geographies or hosting providers, where resold VPN access would first appear.

Detect exfiltration, not just encryption: Because encryption is uncommon in Stormous incidents, detection should target data movement rather than ransomware execution. Baseline outbound traffic and alert on large transfers to consumer file-hosting services such as mega.nz and gofile.io, which the actor has used to distribute stolen data. Apply data loss prevention and egress filtering to finance, ERP, email archive and backup systems, which dominate its 2026 claims.

Maintain Offline, Tested Backups: Keep immutable or offline backups and rehearse restoration, since the operation still threatens encryption under its double-extortion model.

Segment Networks to Contain Intrusions: Isolate internet-facing servers from identity infrastructure and business-critical data stores to limit how far an initial compromise can spread before detection.

Preserve Evidence and Engage Incident Response Early: On suspicion of compromise, isolate rather than rebuild affected systems and preserve logs and authentication artefacts, because attackers typically dwell for weeks before discovery and evidence is needed to trace the entry point.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1566: Phishing	
	T1078: Valid Accounts	
	T1133: External Remote Services	
Resource Development	T1585: Establish Accounts	T1585.001: Social Media Accounts
	T1583: Acquire Infrastructure	T1583.001: Domains
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Collection	T1213: Data from Information Repositories	
Impact	T1486: Data Encrypted for Impact	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
TOR Address	3slz4povugieoi3tw7sblxoowxhbzxeju427cffsst5fo2tizepwatid[.]onion, h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd[.]onion, pdcizqzjitsgfcgqeyhuee5u6uki6zy5slzioinlhx6xjnsw25irdgqd[.]onion, 6sf5xa7eso3e3vk46i5tpcqhnlayczztj7zjktzaztlotyy75zs6j7qd[.]onion, zib7duoiglvzvnpjs5faly6bio4xhwiby2lupsnxrkjnx46gmwdfyrid[.]onion, ahb6hjhe4nomgfwxequu52hazigh4ty4gdcnrf3r7z5tiyhour5py2id[.]onion, stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd[.]onion, 5pbckbo5ra36srfwmb2y6mqpqj7akx3e6ewanujszv7nnjndbbgsjsad[.]onion

Recent Breaches

https://www.higuchi-inc.co.jp
https://www.higuchi-usa.com
https://www.eogb.co.uk
https://www.eshacloudqa.com
https://www.monoprix.tn
https://www.palatineschool.org
https://www.maglificiolilliana.com
https://www.lorenzoni-store.com
https://www.montechiaro-store.com
https://www.impulso-store.com
https://www.jaggroup.com
https://www.mlit.com.my
https://www.vspsolutions.com.au
https://www.sa2000.com
https://www.katholiekamersfoort.nl

References

https://www.kelacyber.com/blog/stormous-extortion-group-strikes-back/

https://zensec.ae/stormous-ransomware/

https://blog.talosintelligence.com/ghostsec-ghostlocker2-ransomware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 17, 2026 • 07:09 PM

More at www.hivepro.com