October 6, 2025

Elevated Risk Surrounding October 7

Key Attack Insights:

- Israel's retaliation following the October 7, 2023, Hamas attack sparked an unprecedented wave of DDoS activity led by pro-Palestinian hacktivists, marking a significant escalation in the hacktivist landscape.
- SYLHET GANG recently posted a call to action referencing "7 October" and urged for a coordinated action timed to that date.
- The SYLHET GANG channel functions primarily as a propaganda amplifier and mainly forwards partner claims and alliance announcements rather than publishing independent technical proof of attack activity.

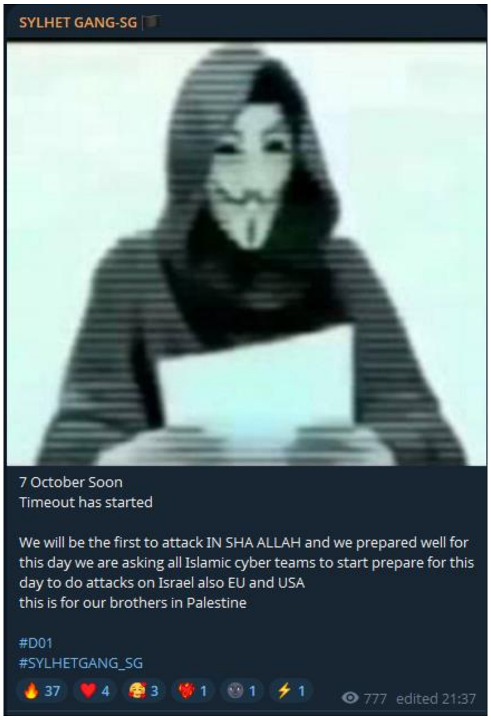
October 7 anniversaries have become focal points for pro-Palestinian hacktivist messaging and calls for coordinated attack campaigns such as DDoS, data leaks and defacements. Ideologically driven actors use the symbolic date to mount publicity-focused campaigns aimed at increasing their visibility in the media and the wider hacktivist community. Given that hacktivist activity often combines low-cost disruptive techniques with high-volume social amplification, defenders should anticipate temporal spikes in website defacement, data leak and DDoS attack claims around the anniversary window.

SYLHET GANG Profile

SYLHET GANG operates primarily via Telegram channels where the group publishes original posts and forwards posts from allied groups to amplify them. The original messages in the Telegram channel are mostly announcements of new alliances, forwarded attack claims from partners and calls to action for coordinated operations. This pattern suggests that the channel plays both a coordination and recruitment role as well as a propaganda and amplification role in the wider hacktivist ecosystem. The channel posts in English, Russian and Arabic languages and repeatedly republishes links to external file hosts and attack proof pages, increasing cross-regional reach and the likelihood that a single claim cascades across many communities.

The Threat

SYLHET GANG explicitly called for coordinated action related to October 7 through a short message in its channel reading "7 October Soon / Timeout has started / We will be the first to attack IN SHA ALLAH…," making a clear intent to time activity to the anniversary.



SYLHET GANG-SG

7 October Soon
Timeout has started

We will be the first to attack IN SHA ALLAH and we prepared well for this day we are asking all Islamic cyber teams to start prepare for this day to do attacks on Israel also EU and USA
this is for our brothers in Palestine

#D01
#SYLHETGANG_SG

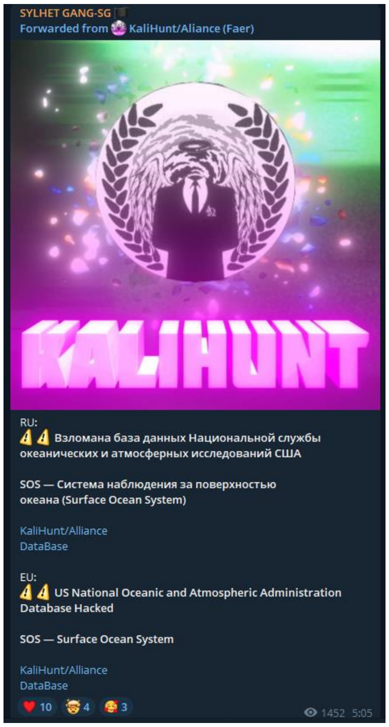
🔥 37 ❤️ 4 🥰 3 ❤️‍🔥 1 🌚 1 ⚡ 1 👁 777 edited 21:37

Figure 1: SYLHET GANG-SG's call to action on October 7, dated Oct 1, 2025 (source: Telegram)

Although the channel contains mainly forwards of other channels, the group’s public call to action and pattern of amplifying alleged proof materially raises the near-term risk of potentially disruptive coordinated DDoS attack waves, opportunistic web defacements and propagation of alleged data leaks by allied groups.

Collaborators

SYLHET’s channel operates inside a network of allied channels whose forwards and alliance messaging broadens their reach and increases their potential of initiating campaigns amongst allies. KaliHunt’s messages, for example, are repeatedly forwarded and SYLHET helped them to become more visible inside the community.



SYLHET GANG-SG

Forwarded from KaliHunt/Aliance (Faer)

RU:
⚠️⚠️ Взломана база данных Национальной службы океанических и атмосферных исследований США

SOS — Система наблюдения за поверхностью океана (Surface Ocean System)

KaliHunt/Alliance
DataBase

EU:
⚠️⚠️ US National Oceanic and Atmospheric Administration Database Hacked

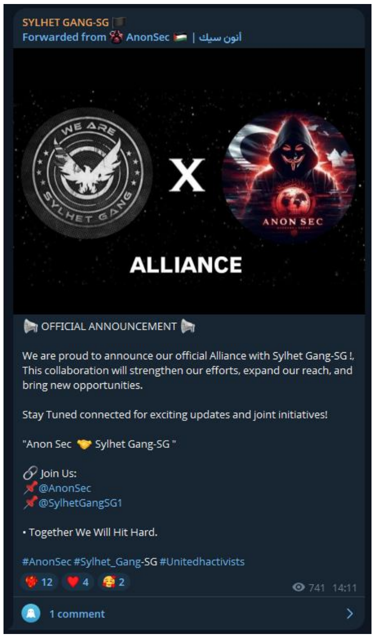
SOS — Surface Ocean System

KaliHunt/Alliance
DataBase

❤️ 10 🤯 4 🥰 3 1452 5:05

Figure 2: Message from KaliHunt forwarded by SYLHET GANG SG, dated Oct 24, 2024 (source: Telegram)

SYLHET also announced AnonSec PS in an official alliance statement, indicating the intentional mutual amplification rather than a few casual mentions.



SYLHET GANG-SG

Forwarded from AnonSec 🇵🇸 | أنون سيك

📢 OFFICIAL ANNOUNCEMENT 📢

We are proud to announce our official Alliance with Sylhet Gang-SG !, This collaboration will strengthen our efforts, expand our reach, and bring new opportunities.

Stay Tuned connected for exciting updates and joint initiatives!

"Anon Sec 🤝 Sylhet Gang-SG "

🔗 Join Us:
📌 @AnonSec
📌 @SylhetGangSG1

• Together We Will Hit Hard.

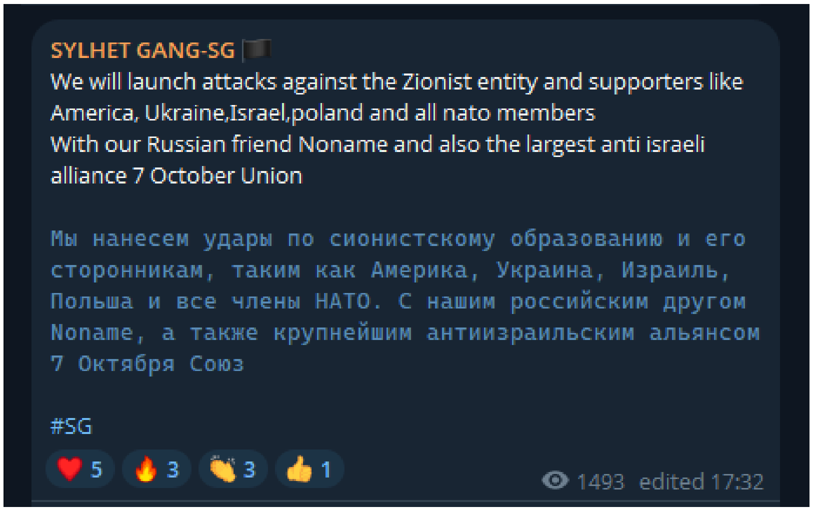
#AnonSec #Sylhet_Gang-SG #Unitedhactivists

❤️‍🔥 12 ❤️ 4 🥰 2 741 14:11

1 comment

Figure 3: Official alliance statement by SYLHET GANG and AnonSec, dated April 5, 2025 (source: Telegram)

DieNet and NoName057(16) are other regularly forwarded groups, increasing the reach of pro-Russian aligned messages across pro-Palestinian channels. NoName057(16) was also mentioned in the “7 October” framing of last year, underscoring the cross-ideological and global nature of the threat.



SYLHET GANG-SG 🏴
We will launch attacks against the Zionist entity and supporters like America, Ukraine,Israel,poland and all nato members
With our Russian friend Noname and also the largest anti israeli alliance 7 October Union

Мы нанесем удары по сионистскому образованию и его сторонникам, таким как Америка, Украина, Израиль, Польша и все члены НАТО. С нашим российским другом Noname, а также крупнейшим антиизраильским альянсом 7 Октября Союз

#SG

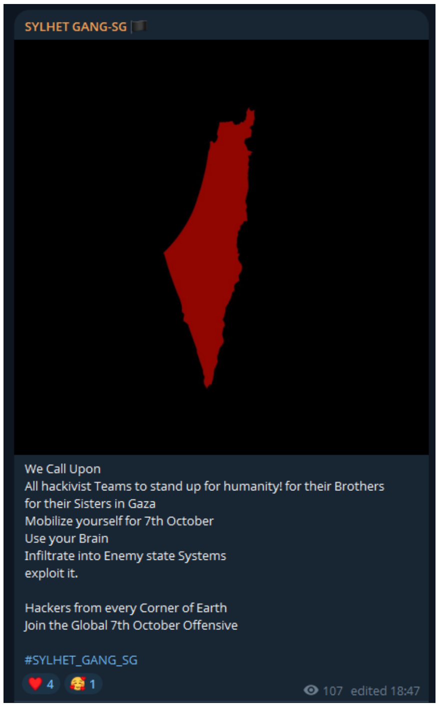
❤️ 5 🔥 3 👏 3 👍 1 👁 1493 edited 17:32

Figure 4: Message from SYLHET GANG referencing NoName, dated July 8, 2024 (source: Telegram)

Taken together, these alliance announcements and forwarding behaviors create a credible amplification pathway. The scale of a potential disruptive event will depend less on SYLHET’s technical capability, but more the speed of cross-channel propagation and how many allied groups pick up the call to leverage their mutual capabilities. This dynamic can result in multiple DDoS attack waves, coordinated defacements and an overwhelming cascade of social claims that could strain organizations’ SOC, IR and communications resources.

Reasons for Concern

- **Anniversary timing:** Explicit calls tied to October 7 raise the likelihood of coordinated time-bound activity.
- **Networked amplification:** Alliance announcements and frequent forwards allow a single claim to be spread quickly across multiple communities and languages, multiplying its reach and potential pressure on targets.



SYLHET GANG-SG

We Call Upon
All hackivist Teams to stand up for humanity! for their Brothers
for their Sisters in Gaza
Mobilize yourself for 7th October
Use your Brain
Infiltrate into Enemy state Systems
exploit it.

Hackers from every Corner of Earth
Join the Global 7th October Offensive

#SYLHET_GANG_SG

Figure 5: A message from the SYLHET GANG Telegram channel, dated October 5, 2025 (source: Telegram)

- **Low barrier attacks:** DDoS and web-layer nuisance attacks are cheap, scalable and hard to fully prevent without proper mitigation solutions in place. These attacks can cause service disruption, customer impact and negative media attention.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and cloud DDoS protection for real-time DDoS attack prevention that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further network and application protection measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's Security Research Center. Additionally, visit Radware's Quarterly DDoS & Application Threat Analysis Center for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED “AS IS” WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILBILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER’S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIREC, INCIDENTAL, CONSEQUENTIAL, OR EXAMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. **CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE**