December 16, 2024

Holy League: A Unified Threat Against Western Nations, NATO, India and Israel

Amid intensifying hacktivist activity, the Holy League hacktivist collective emerged in July 2024, formed through the union of the High Society and 7 October Union alliances. The group declared the unification of pro-Russian and pro-Palestinian hacktivists, collaborating to launch coordinated attacks against shared adversaries—primarily Western nations and India as well as countries backing Ukraine and Israel.

Figure 1: Announcement of Holy League, a unification of High Society & 7 October Union (source: Telegram)

Pro-Palestinian and anti-Western ideologies drive this union, which allegedly comprises more than 80 hacktivist groups (see Appendix A: Alleged Members of). It quickly rose to prominence with its high-profile cyber campaigns and provocative messaging.

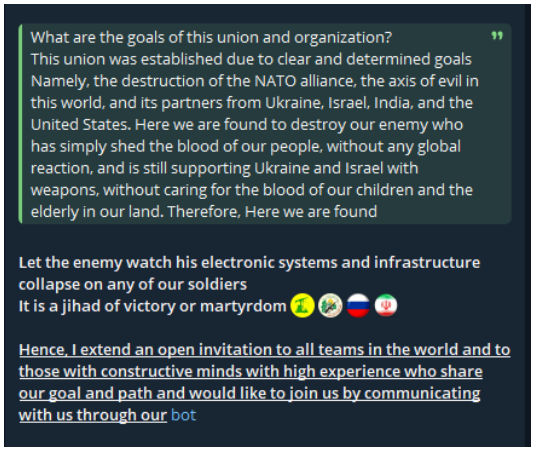

Figure 2: Motivation, threats and invitation to like-minded hacktivists by Holy League (source: Telegram)

Following a ban on their original Telegram channel, Holy League launched a new channel on December 3, 2024. Their new presence reinforced their resolve to act as a digital force against their perceived adversaries. Operating under a religiously charged manifesto, the group's rhetoric combines political resistance with calls for solidarity.

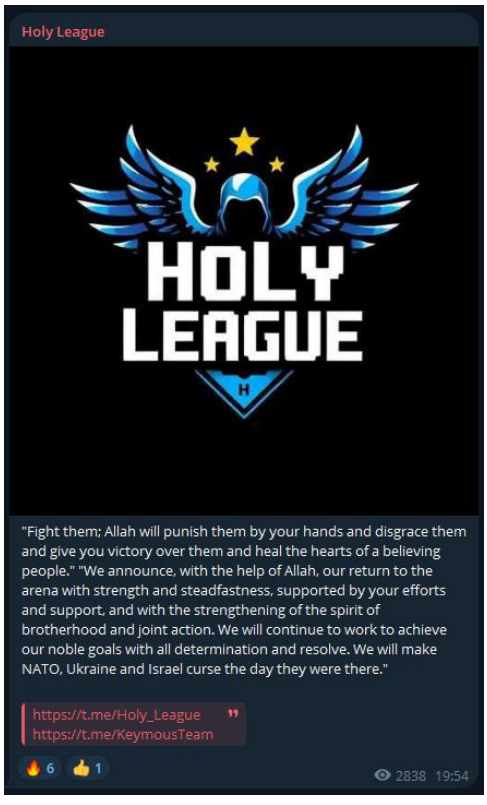

Figure 3: Post announcing the rebirth of Holy League on their new Telegram channel (source: Telegram)

On December 9, 2024, Holy League announced a pivotal leadership development: Brother Abu Omar was appointed as the leader of both Holy League and 7 October Union alliances.

Figure 4: Brother Abu Omar appointed leader of Holy League and 7 October Union alliances (source: Telegram)

Attack Campaigns in December 2024

Holy League has launched numerous coordinated cyberattacks since its relaunch, targeting mainly European nations as symbols of Western influence and political opposition.

France: December 6, 2024

In a direct digital strike against France, Holy League publicly announced an impending cyber offensive. Their message, laced with ominous warnings, declared:

> "France! For a long time, we have awaited this moment to let you pay.
> Tomorrow, you will witness the digital inferno of our power."

The group claimed responsibility for distributed denial of service (DDoS) attacks, data breaches, and system disruptions targeting French governmental and critical infrastructure. These attacks were accompanied by visual propaganda symbolizing Holy League's intent to bring chaos to their adversaries.

Figure 5: Holy League announcing imminent attack campaign targeting France (source: Telegram)

Germany: December 14, 2024

Holy League extended to Germany, vowing to cause "digital descent into chaos." Their propaganda, marked by futuristic and apocalyptic imagery, highlighted their objective to destabilize German systems. While the exact targets were unspecified, their rhetoric underscored a larger mission to disrupt Western infrastructure.

The group's official statement for the German campaign read:

"The skies of Germany will darken. Chaos will reign for those who stand against us."

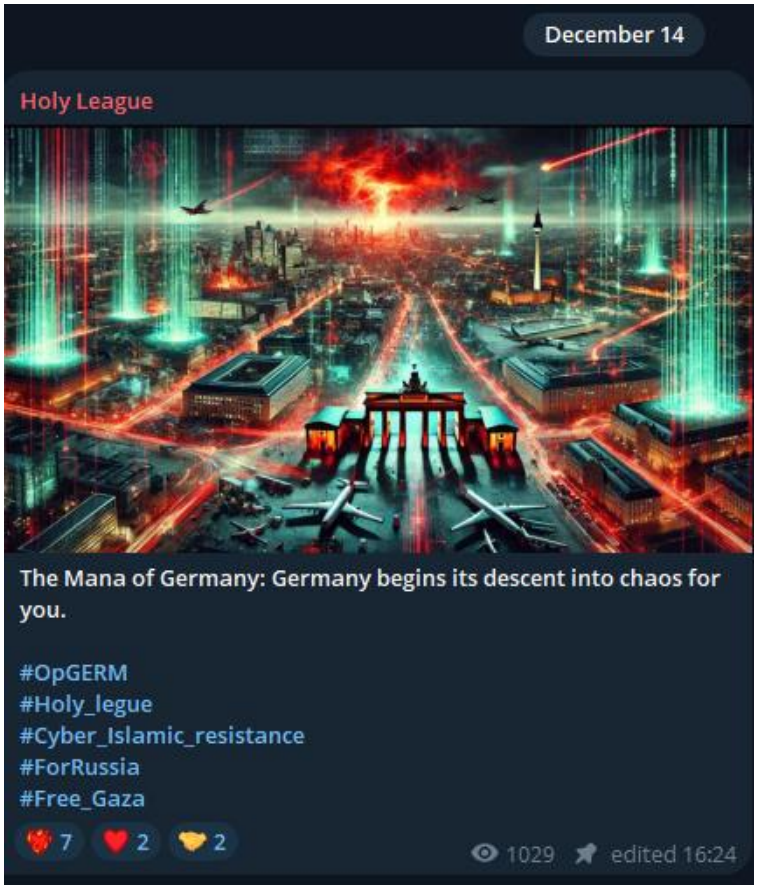

Figure 6: Holy League announcing attack campaign targeting Germany (source: Telegram)

Tactics and Motivation

Holy League members operate with a combination of DDoS attacks, website defacements and leaking sensitive information to incite fear through data breaches. Their motivations are deeply intertwined with geopolitical conflicts, particularly advocating for Palestine and condemning Western alliances like NATO. Their messaging invokes religious and moral justifications, positioning themselves as defenders of oppressed communities.

Holy League has expertly utilized visual propaganda to amplify its message. Its images often depict dystopian cityscapes, religious symbols, and fiery apocalyptic themes, creating a powerful visual identity. These efforts are intended to attract sympathizers and recruit new members from like-minded hacktivist circles.

Their Telegram channel is a hub for communication, announcements, and demonstrations of their campaigns' successes.

A Growing Cyber Threat

Holy League represents a new force in the evolving landscape of hacktivism. Their ability to coordinate attacks, spread propaganda, and orchestrate attacks between allied groups highlights the growing influence of hacktivist alliances.

With recent attacks on France and Germany and a clear anti-Western stance, Holy League poses a persistent digital threat.

Appendix A: Alleged Members of Holy League

High Society, 7 October Union, UserSec, NoName057(16), CyberArmy Of Russia, HorusTeam, CyberHood, Keymous, 313 Team, SilentCyberForce, InsanePakistan, AstroNetworks, GhostXNet, Anonymous Arabs, Team YSG, DXQRTXX, Khilafah Hackers, CyberVolk, CyberStine, Cryptaris, VoltActivist, NetSycho, AlixSec, AzzaSec, Hunt3rKill3rs, HexaLocker, Lapasus, NetForceZ, Al Jihadi, ShadowedWhisper, VendettaNetworks, Anonymous DZ, UCC Team, Nasa1788, KotoBot, YourAnon, B&D Services, Nemesis, CryptoCorp, ZBlackHat, ColtisHere, Al Ahad, SumatraSelatan, LulzSec, WebSec, UnderWorld (Anonymous Revengers), PicoCorp, RedHatElite, UFC Leagues, ShadowSeekers, Spectrum Botnet, TarzanBotnet, Pro-Palestinian Hacker Movement (PPHM), Anon Collective, MarioC2, Fatimion, Ahadun Ahad, CyberDragon, Phantom Group, Islamic Cyber, Team HTR, Morrocan Black Cyber Army, LulzSec Pakistan.

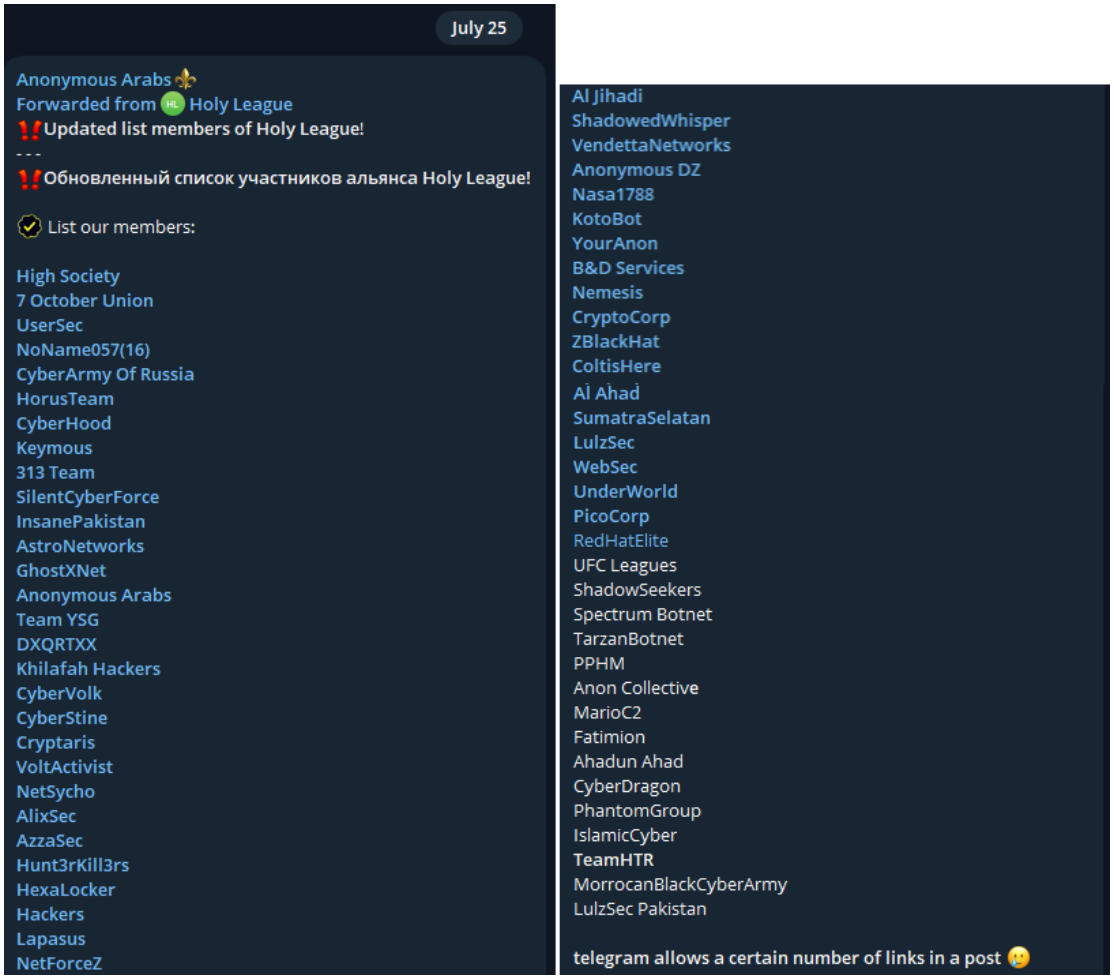

Figure 7: Updated list of members of Holy League dated July 25, 2024 (source: Telegram)

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.