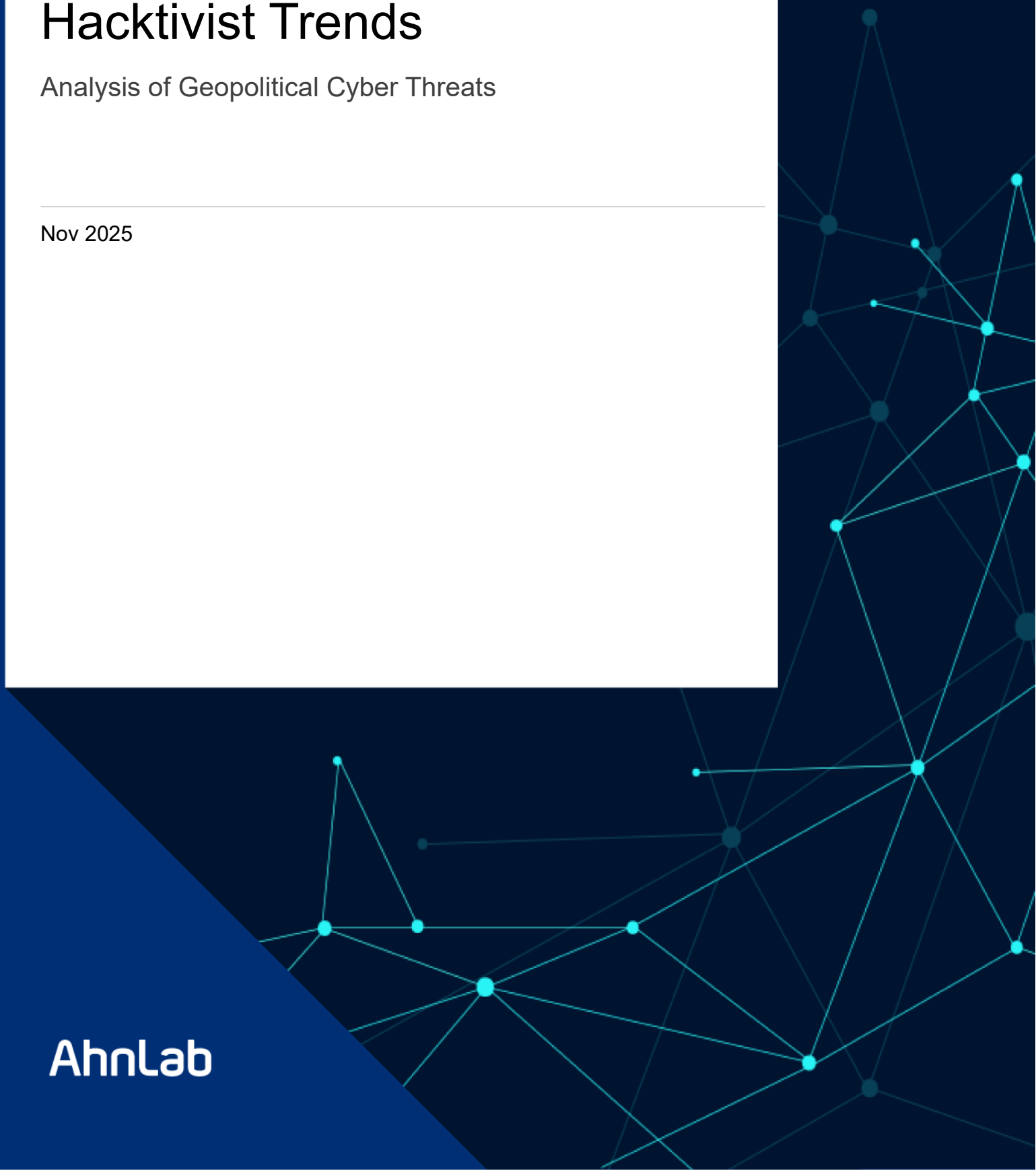
Indian APT Group and Hacktivist Trends

Analysis of Geopolitical Cyber Threats

Nov 2025



AhnLab

Table of Contents

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Purpose and Scope of the Report

This report aims to analyze the activities of advanced persistent threat (APT) groups and hacktivists among cyberattack organizations based in certain countries.

State-sponsored threat groups, suspected of engaging in cyber espionage or sabotage activities with the support of specific national organizations, are referred to as 'APT groups' for convenience. Groups that carry out various attack activities in cyberspace, such as information leakage, service disruption, and website defacement, for specific social or political purposes are classified as 'hacktivists'.

APT groups have been organized based on activity details, attack techniques, and technical characteristics disclosed by major security companies and organizations. Hacktivists have been organized based on their politically and ideologically motivated cyberattack cases and activities, using online promotion and propaganda activities.

By understanding their attack motivations, strategies, and technical characteristics, we aim to improve an organization's security response capabilities and use this report as a reference to prepare for future threats. Additionally, we aim to analyze how the geopolitical and social background of the country affects the activities of cyberattackers and, based on this, propose directions for security response and policy implications.

21st-century cyberspace has become a new battleground for conflicts between nations. Especially, India is emerging as a hub for cybersecurity amid rapid digitalization and geopolitical tensions. India strengthens its cyber defense to protect its technological capabilities and information infrastructure, while sometimes expressing conflicts with neighboring countries through offensive cyber strategies. This article examines major cyberattack cases in India, activities of APT groups linked to India, and the movements of hacktivists surrounding India.

This report assumes that the names and classification criteria of APT and hacktivist groups may vary depending on the security company or researcher, and classified them into the most relevant groups based on the well-known names of threat actors organized in the AhnLab Threat Intelligence Platform (ATIP).

Cases of Cyberattacks Against India

Due to India's geopolitical conflicts with neighboring countries, Pakistan and China, cyberattacks against India are often associated with these nations.

The major cyberattack cases that occurred in India are as follows.

Period	Target	Details
2010	Indian military and defense	Operation Shady RAT. Attempt to steal confidential information from the Indian government and military institutions
2010	CBI (Central Bureau of Investigation)	The Pakistani Cyber Army hacked the Central Bureau of Investigation (CBI) website
2013	Education, defense, government agencies, aerospace	Start of attack by the Transparent Tribe group, suspected to be linked to Pakistan
2013	20,000 Indian websites	Massive volume attack by Dr@cul@ and Muhammad Bilal
2013	Reserve Bank of India (RBI), Lucknow Customs	Defacement of financial and customs institutions by PCA on the anniversary of the November 26 Mumbai attacks
2014	2,000 Indian websites	A large-scale defacement led by Team Madleets to mark India's Republic Day
2014	Reserve Bank of India (RBI)	The second defacement targeting the central bank by PCA, following the one in 2013
2016	Over 7,000 Indian websites	A large-scale defacement by the Pakistan Haxors Crew immediately after the Uri incident*
2017	Indian media, defense, finance	Lazarus group's Ratankba malware attack on India
2019	Indian nuclear power	Suspicion of an attack on the Kudankulam Nuclear Power Plant (KKNPP) by a suspected North Korea-linked group
2020	Indian energy	RedEcho group's attack on the Indian power grid
2024	India virtual assets (cryptocurrency) exchange	Due to an attack by a suspected North Korean hacker,[1] Company W (an Indian cryptocurrency exchange) was hacked, resulting in an approximate loss of $234.9 million[2]
2025	Indian power grid, airport servers, railway systems, communication networks, etc.	Due to an attack led by the Pakistani military, there was a temporary disruption, delays, and paralysis of the affected services

Table 1. Major cyberattacks against India

[1] https://www.cnbctv18.com/technology/wazirx-crypto-breach-cyfirma-north-korean-lazarus-group-19450904.htm

[2] https://en.wikipedia.org/wiki/2024_WazirX_hack

In 2010, Operation Shady RAT, which attempted to steal confidential information from the Indian government and military institutions, was discovered.[3] It was not an attack targeting India alone but part of attacks on multiple regions.

In 2010, the website of the Indian Central Bureau of Investigation was hacked, and the Pakistani Cyber Army (PCA) claimed it was their actions.[4]

Since 2013, attacks by Pakistani APT groups like Transparent Tribe[5] have begun.

In late September 2013, Dr@cul@ and Muhammad Bilal launched defacement attacks on around 20,000 Indian websites.[6]

On November 26, 2013, the anniversary of the Mumbai attacks, the Pakistani Cyber Army (PCA) launched website defacement attacks targeting the Reserve Bank of India (RBI) and Lucknow Customs. They launched another website defacement attack targeting the same bank on March 20, 2014. [6]

On January 26, 2014, on the occasion of India's Republic Day, 2,000 Indian websites were defaced by groups including StrikerRude, KashmirCyberArmy, PakCyber Expert, and Hunter Gujar, led by Team MadLeets.[6] [7]

In early October 2016, about a month after the Uri incident, around 7,000 Indian websites were defaced by the Pakistan Haxors Crew.[6]

On September 18, 2016, in the Uri area of Indian-administered Jammu and Kashmir, an attack on the Indian Army brigade headquarters by armed militants reportedly resulted in the deaths of 19 Indian soldiers.

In 2017, an attack by the Lazarus Group on India was discovered,[8] and in 2019, an attack suspected to target the Kudankulam Nuclear Power Plant (KKNPP) was discovered.[9]

---

[3] https://en.wikipedia.org/wiki/Operation_Shady_RAT

[4] https://www.ndtv.com/india-news/cbi-website-hacked-by-pak-cyber-army-441049

[5] https://atip.ahnlab.com/threat-actor/view?seq=1070

[6] https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/314582/Cyber-Reports-2018-04.pdf

[7] https://www.indiatoday.in/world/neighbours/story/pakistani-hackers-claim-defacing-2000-indian-websites-on-26th-jan-179552-2014-02-03

[8] https://www.trendmicro.com/en_us/research/18/a/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba.html

[9] https://arstechnica.com/information-technology/2019/10/indian-nuclear-power-company-confirms-north-korean-malware-attack/

In 2020, a cyberattack targeting the power grid in northern India caused a temporary blackout. This attack is suspected to be the work of the Chinese APT Group, RedEcho, and was interpreted as part of the cyber warfare related to the India-China border conflict. The threat actor distributed malware targeting the SCADA system, paralyzing the power infrastructure.[10]

In 2024, Company W, a leading cryptocurrency exchange in India, had over $230 million in virtual assets stolen.[11] The threat actor, suspected to be linked to a North Korean hacker group, is believed to have exploited a security vulnerability in multi-signature wallets.

After May 2025, 4,600 power feeders in India were hacked by Pakistan, and 80% of the power was temporarily disrupted. Due to another attack, airport communications were temporarily disrupted, and there were also cases of train operations being delayed. There was an incident where the OTP authentication system was disrupted, leading to an interruption of government email services. This is known as Operation Bunyanum Marsoos and was reported to be directly involved with the cyber wing of Pakistan's armed forces.[12]

[10] https://go.recordedfuture.com/redecho-insikt-group-report

[11] https://www.cnbctv18.com/technology/wazirx-crypto-breach-cyfirma-north-korean-lazarus-group-19450904.htm

[12] https://tribune.com.pk/story/2546050/security-sources-reveal-details-of-pakistans-massive-cyberattack-against-india

Indian Threat Actors

India's APT groups and hacktivists primarily target Pakistan, but some also carry out attacks on various countries.

1) APT Groups

India's APT groups have been targeting Pakistan and China since 2010, and recently, it has expanded its targets to neighboring countries. They primarily use spear phishing to deliver malware and are attacking using malicious Android apps disguised as chat apps, among others.

APT Group	Emergence	Target	Details
Bitter	2013	Government agencies, energy, high-tech industries, universities, and defense industries in China, Pakistan, Saudi Arabia, and other countries	Spear phishing and exploitation of document vulnerabilities Malicious files in various formats, such as PUB, PDF, CHM, LNK, and searchConnector-ms, are sent via email
Patchwork	2015	Industries related to Pakistan's diplomatic and national institutions, U.S. think tanks	Attempt at long-term infiltration through social engineering-based phishing and backdoor installation Most malware is used as is from what is distributed on online forums
SideWinder	2012	Government agencies and the energy, defense, mineral, and logistics sectors in several countries, including China, Bangladesh, Pakistan, India, Afghanistan, Nepal, Sri Lanka, and Egypt	Spear phishing and document-based malware are the main attack vectors Attacks using vulnerabilities in malicious LNK files and Office document files (CVE-2017-0199, CVE-2017-11882)
Viceroy Tiger	2015	Pakistan's manufacturing and defense industries	Phishing attacks characterized by the use of malicious documents and Android malware. The attack involves LNK files disguised as RTF files to target Windows, and also uses

			malware designed for Android devices

Table 2. Major Indian APT groups

Bitter

The BITTER group[13] is also known as APT-C-08, Hazy Tiger, Orange Yali, T-APT-17, and 蔓灵花, and is believed to be based in India. Since 2013, attacks have been conducted against government agencies, energy, high-tech industries, universities, and defense industries in China, Pakistan, Saudi Arabia, and other countries. Malicious files in various formats, such as PUB, PDF, CHM, LNK, and searchConnector-ms, are sent via email to infect the systems.

A phishing attack using searchconnector-ms files was discovered in 2024. When the malicious searchconnector-ms file included in the phishing email's attachment is opened, a malicious LNK file or CHM file is remotely downloaded via WebDAV. Malware strains such as ArtraDownloader, BITTER RAT, Dracarys, ORPCBackdoor, MiyaRat, and wmRAT are used.

Patchwork

The Patchwork group,[14] first discovered in December 2015, is a threat group also known by names such as APT-C-09, APT-Q-36, ATK11, Chinastrats, Dropping Elephant, Hangover, Orange Athos, Quilted Tiger, Sarit, White Elephant, and ZINC EMERSON. There is no conclusive evidence, but based on circumstantial evidence, it is presumed to be India or an Indian group.

The main targets are industries related to Pakistan's diplomatic and national institutions, and in March and April 2018, there were instances of spear-phishing attacks targeting a U.S. think tank group. Most malware is known to be used as is from what is distributed on online forums.

In 2024, a spy operation targeting primarily Pakistani users was conducted through romance scams. This operation includes 12 Android apps sharing a common malware called VajraSpy. Among these, 6 apps were available on Google Play and installed more than 1,400 times. The remaining 6 were found on VirusTotal.

In the 2024 Bhutan attack, the PGoShell backdoor and Brute Ratel C4 were used. Using the

[13] https://atip.ahnlab.com/threat-actor/view?seq=6176

[14] https://atip.ahnlab.com/threat-actor/view?seq=69

BadNews malware to remotely control targets, it uses Remcos and the open-source penetration framework Havoc.

SideWinder

The SideWinder group,[15] also known as APT-C-17, Razor Tiger, Rattlesnake, SloppyLemming, and T-APT-04, is a threat group suspected to be linked to India. This group was first reported in 2012 and has been conducting attacks targeting government agencies and the energy, defense, mineral, and logistics sectors in several countries, including China, Bangladesh, Pakistan, India, Afghanistan, Nepal, Sri Lanka, and Egypt.

They carried out attacks using vulnerabilities in malicious LNK files and Office document files (CVE-2017-0199, CVE-2017-11882).

In late 2019, a malicious mobile app suspected to be associated with the SideWinder group was discovered. This app was disguised as a photo and file manager tool and attempted to root the device using the Android kernel vulnerability (CVE-2019-2215).

In early 2025, attacks were carried out targeting high-level government agencies in Sri Lanka, Bangladesh, and Pakistan. They sent spear phishing emails exploiting vulnerabilities in Office document files (CVE-2017-0199, CVE-2017-11882). The threat actor's server examined the requester's IP address or User-Agent information to apply geofencing, ensuring that the malicious payload was delivered only to the target country, making analysis difficult.

The SideWinder group is known to use malware, including IntelX, DSC, and StealerBot.

Viceroy Tiger

The Viceroy Tiger group,[16] also known as APT-C-35, APT-Q-38, Donot, Donot Team, Mint Tempest, OPERATION HANGOVER, Orange Kala, Origami Elephant, and SectorE02, is a threat group. They are working to represent the interests of the Indian government.

This group has been active since 2015, primarily targeting government agencies, diplomacy, and defense sectors in Bangladesh, Sri Lanka, and Pakistan.

Their attack method involves using spear phishing emails to deliver documents disguised as executable files or Microsoft Office documents containing macros. They also uses malicious apps disguised as chat applications targeting Android devices.

---

[15] https://atip.ahnlab.com/threat-actor/view?seq=31647

[16] https://atip.ahnlab.com/threat-actor/view?seq=28593

They are known to have carried out attacks using malware such as LoptikMod and Tanzeem.

2) Hacktivist

Hacktivist groups from India and Pakistan primarily conduct DDoS attacks and web defacement attacks targeting the opposing side's websites, and some also infiltrate systems. The conflict between India and Pakistan has a long history, with groups active for a long time, including some that were first identified 10 years ago.

The known pro-India hacktivist group is presumed to be mostly composed of their own nationals. Most well-known hacktivist groups have a pro-Pakistan stance and side with Pakistan. Therefore, the groups supporting Pakistan are numerically superior in general, but the groups supporting India are considered to have a relatively superior impact through their infiltration of websites of Pakistan's paramilitary and drug enforcement agencies and the internal systems of the railway authority.

Below is a table categorizing hacktivist groups presumed to be based in India and those with a pro-India stance, considering their activity levels and influence comprehensively. If major channels (X, Instagram, YouTube, Telegram, etc.) were not found, or if the channel was found but ceased activity long ago, they were all classified as 'Low Risk'. For reference, the table below is based on information confirmed at the time of investigation, and it should be noted that it may change as additional information is found or changes in activity patterns are detected.

Name	High Risk	Medium Risk	Low Risk
India	Crack Codes Dex404 Team UCC Night Hunters Red Eagle India 7 Proxies	Team White Lotus Hexaforce Alliance Indian Cyber Force Indian Cyber Mafia Black Dragon Hell Shield Hackers Indishell Mallu Cyber Soldiers Ne0-H4ck3r Kerala Cyber Xtractors	Kingsman (India) J43v3r Code Man Godzilla (also known as G.O.D) HMG India Cyber Pirates Indian BlackHats Indian Hackers Indian Hackers Online Squad Kerala Cyber Warriors Lulzsec India Mr Z Nomcat Team Indi-Heax Telangana Cyber Warriors Vicky Singh Virkid (part of MaDLeeTs)

			Virushacker Z Company Hacking Crew Zindabad (part of PCA) Bhagat Cyber Soldiers Krutik
Pro-India		Cyber volk	One Sec SilentOne

Table 3. Indian and pro-India hacktivists

The hacktivists selected as the subject of analysis was comprehensively evaluated by considering the volume of activity, influence, and diversity of activities to illuminate the current situation from multiple angles. Information on the selected hacktivists is as follows.

Name	Target	Attack Type	Details
Dex404	Pakistani government websites, military enrollment portals, energy and power maintenance systems, public services	DDoS attacks, hacking of industrial control systems (SCADA), and infiltration of power systems	Created malware based on Coil Command Flooding that exploits a Modbus vulnerability, and announced its evolution into RaaS and MaaS forms, along with a move to the dark web
Hexaforce Alliance	Pakistan's government, military, and public institutions	Website defacement, data breach, DDoS attack	Claimed to have secured all confidential documents and information from the Pakistani police and also carried out a DDoS attack on the search engine Shodan.io
Indian Cyber Force	Pakistan's financial system, bank websites, and surveillance cameras	Website defacement, data breach, DDoS attack	150 GB of data leaked from the online tax management system IRIS operated by Pakistan's Federal Board of Revenue
Night Hunters	Pakistan's railways, military, and government institutions	Website defacement, SCADA and database breaches	Significant data breaches such as hacking Pakistan's railway system to leak data and leaking military accounting information
Team UCC	Pakistan's government and military institutions, educational	Website defacement, admin panel infiltration, website data deletion	Exfiltrated the entire database of a private company, deleted all data on the server, and stole the entire database of Pakistan's logistics management system

	institutions, and public infrastructure systems (logistics, administrative management, etc.)		
Team White Lotus	Websites of major national institutions in Pakistan, state-owned enterprises, telecommunication companies, universities	Website defacement, admin panel infiltration, website data deletion	Only carries out attacks to cause damage without any inciting messages, and the use of a web shell was detected

Table 4. Major India-related hacktivists

Dex404

Dex404 is a hacktivist group believed to be based in India, with a pro-India and anti-Pakistan stance.[17]

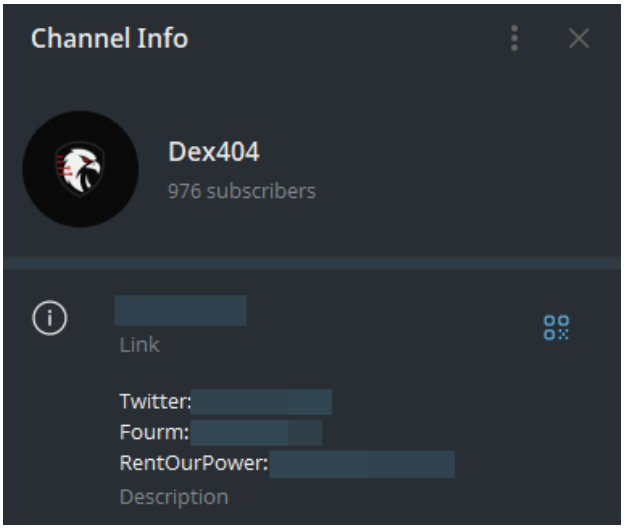


Figure 1. Dex404's Telegram channel

Their main attack methods are DDoS and breaches of government websites, attacks on industrial infrastructure (Islamabad server IP, SCADA/OT systems, etc.), data leaks and

[17] https://atip.ahnlab.com/threat-actor/view?seq=105327

broadcast disruption, and paralysis of transportation infrastructure. In particular, they caused public transportation disruption through an attack on the Natco Bus reservation system, and after that, they showed signs of expanding their scope of activities by stating that they will be providing Ransomware-as-a-Service and Malware-as-a-Service.

The tools used include malware employing the Modbus Coil Flooding technique, Check-host for verifying targeted attacks, and Telegram and X (formerly Twitter) for spreading ideology and activities. Additionally, they revealed plans to transition their activity environment to one based on the darknet, also showing attempts to enhance the concealment and persistence of their activities.

The main targets of Dex404 are Pakistani government departments (Tourism, Defense, Energy, Commerce, Engineering Council), national agencies (NDMA, Punjab Government), broadcasting stations (Radio Pakistan), and civil service infrastructure (Natco Bus reservation system).

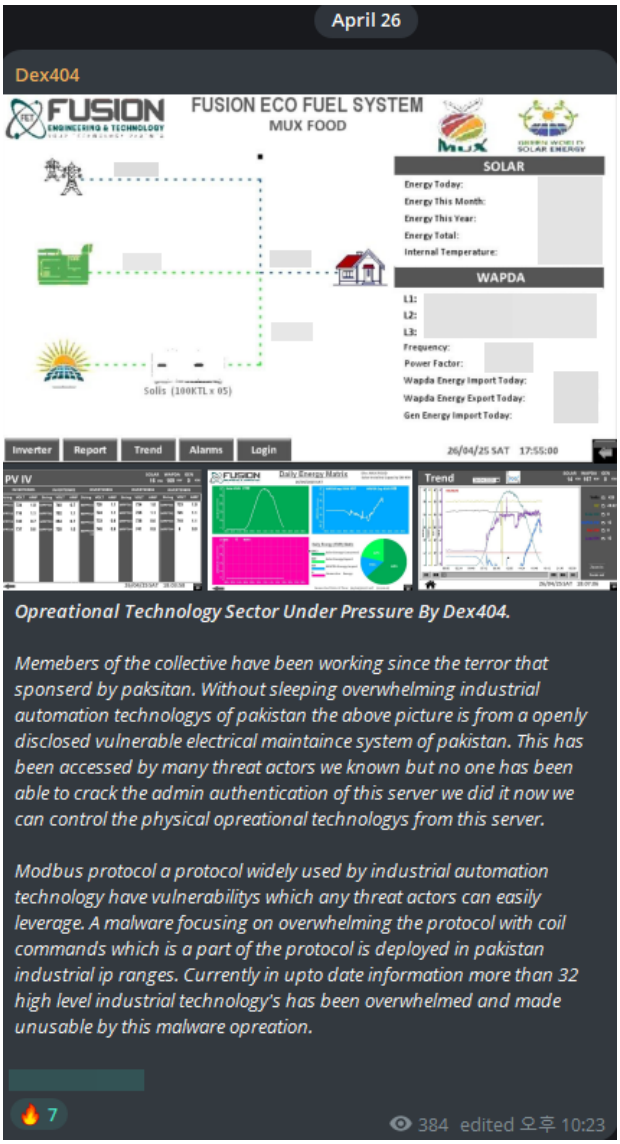


Figure 2. Penetration into Pakistan's industrial automotive systems released by

Dex404

Targeting actual physical operation disruption beyond simple defacement and DDoS levels is a characteristic of this group. Exploiting a vulnerability in the Modbus protocol to disrupt OT (industrial control) systems suggests a relatively high level of technical understanding. Last July, they officially announced the RaaS/MaaS framework, blatantly revealing its cybercriminal nature.

After April 2025, attacks on multiple Pakistani government department websites, claims of SCADA system paralysis, an attack on the official Pakistan Airforce website, disruption of Radio Pakistan broadcasts, and a breach of the Natco Bus reservation system have been reported. This group is expected to continue advancing their strategies and techniques and carry out continuous attacks.

Hexa Force Alliance

Hexa Force Alliance is a hacktivist group believed to be based in India, with a pro-India and anti-Pakistan stance. They targeted Pakistan's railway, government, security infrastructure, and private companies as their main targets.

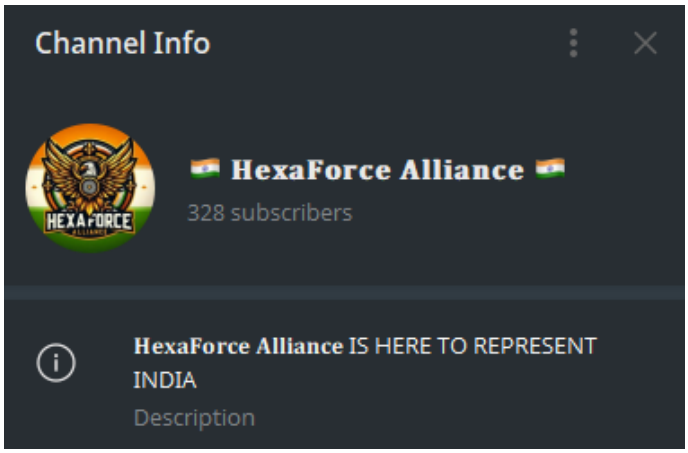


Figure 3. Hexa Force Alliance's Telegram channel

The main attack methods include website defacement, service disruption, unauthorized system penetration, and database leakage. Threat actors demonstrate their success by sharing evidence of service disruption through Check-host links or by publishing proof of concept (PoC).

This group, in relation to the Ahmedabad plane crash on June 12, 2025, posted a blood donation campaign message, also revealing its social activism aspect. This reveals that the group has not only nationalist and patriotic tendencies but also a tendency towards social participation.

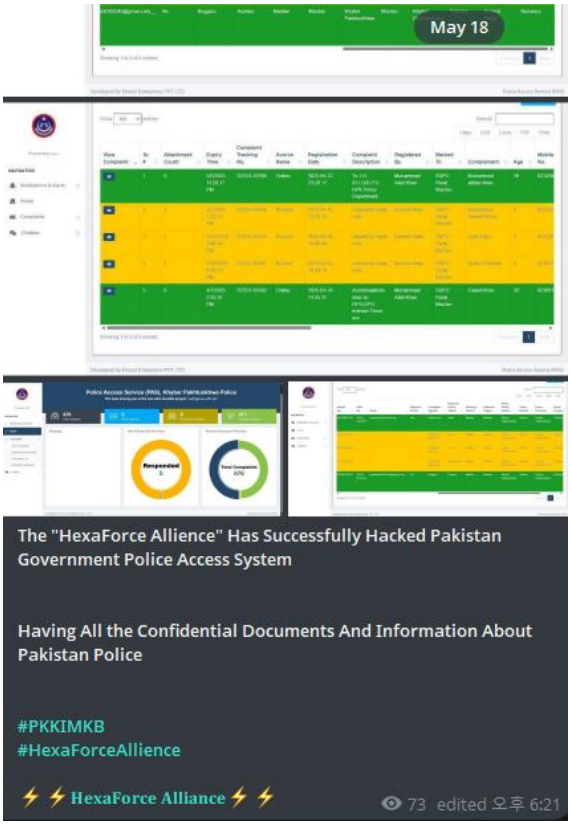


Figure 4. Penetration into Pakistan's Police Access System released by Hexa Force Alliance

Major attack cases include the disruption of the Pakistan Railways official website and the breach of the Police Access System on May 18, 2025, claims of an attack on Shodan.io and hacking of Speed PLC servers, an attack on the Pakistan government website on June 5, and the leak of Company S (a media production studio) DB on June 10.

Hexa Force Alliance is targeting Pakistan's critical infrastructure and government systems, while emphasizing both nationalist ideology and social engagement by overlaying social messages.

Indian Cyber Force

Indian Cyber Force is a hacktivist group believed to be based in India, with a pro-India and anti-Pakistan stance.

Figure 5. Indian Cyber Force's X (formerly Twitter) channel

The attack methods are varied, including system intrusion, data theft, service disruption, website defacement, and surveillance camera breaches, among others. They use their X (Twitter) account to post propaganda messages, redistribute attack achievements, and promote their activities.

The main targets are the Pakistan Federal Board of Revenue (FBR) IRIS portal, financial institutions like the Bank of Pakistan, CCTV/surveillance camera systems, and numerous educational institution sites.

This group is characterized by borrowing the image of NGOs and non-profit organizations to emphasize legitimacy. They are adopting a strategy of framing the attack as an extension of political and social struggle, rather than just a simple criminal act.

Figure 6. Deletion of Company D (an engineering firm) DB and hacking of over 1,000 surveillance cameras in Pakistan, released by Indian Cyber Force

On the anniversary of the Pulwama attack in 2024, defacement attacks were conducted on numerous websites, followed by a denial-of-service attack on the Bank of Pakistan website, and over 1,000 surveillance cameras in Pakistan were also compromised. In May 2025, the group claimed to have stolen over 150 GB of data through a breach into the Pakistan FBR IRIS portal, pressuring financial and administrative institutions. The claim of breaches of over 1,000 surveillance cameras has been reported to be used by the pro-India online propaganda network 'Hidden Charkha', which has been confirmed to be active since 2021, to beautify India's image and criticize Pakistan's side in shaping public opinion.[18]

Night Hunters

The Night Hunters is a hacktivist group believed to be based in India, with a pro-India and anti-Pakistan stance. They also show a pro-Israel tendency, and attacks targeting other countries like Indonesia and Malaysia have also been identified. Attacks were carried out targeting Pakistan's railways, government institutions, military finance departments, as well as the energy infrastructure of Indonesia and Malaysia.

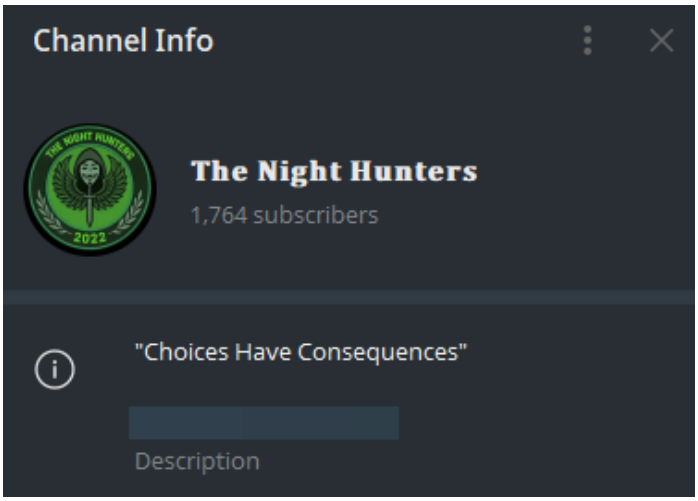


Figure 7. The Night Hunters's Telegram channel

This group uses SQL server breaches, data leaks, website defacement, and industrial control system (SCADA) breaches as their main attack methods, and they also release videos on YouTube as evidence of their successful attacks. They are known to have used open-source scanners such as SQLmap, Nikto, Wpseku, and Sublist3r, as well as tools like the Weevely web shell, GoldenEye, Hulk, and Xerxes.[19] Additionally, political slogans like 'Jai Hind' and 'India stands with Israel' are used to express national and ideological messages.

[18] https://www.recordedfuture.com/research/influence-operations-and-conflict-escalation-in-south-asia

[19] https://www.scribd.com/document/764226244/The-Night-Hunters-IOCs-240812-193803

Notable attack cases between May and June 2025 include the leakage of internal assets and workflow of Pakistan Railways, breach of the Pakistan Government SQL Server and document theft, hacking of the Indonesian Solar Energy Monitoring System and release of PoC video, and breach of the Pakistan Military Accounts Department server and release of 88-page PDF data.

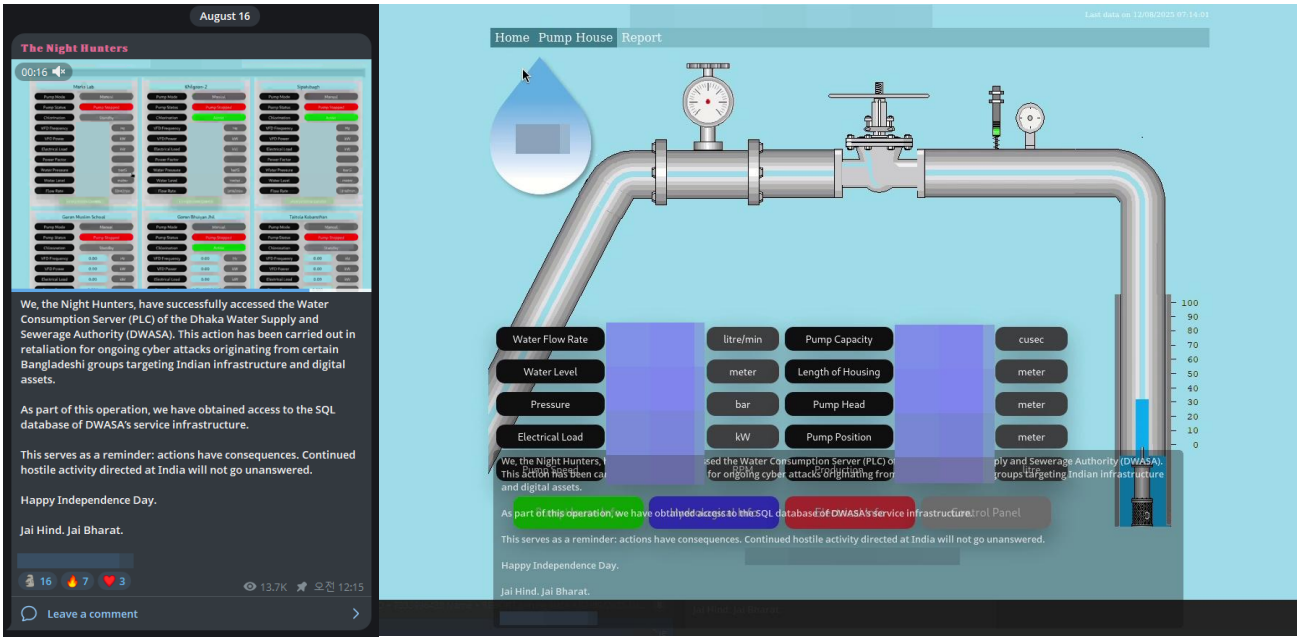


Figure 8. Penetration into Malaysia's DWASA PLC released by The Night Hunters

Especially recently, on the occasion of India's Independence Day on August 15, a retaliatory attack was launched on the infrastructure of Malaysia, which had attacked their country, revealing an intention to highlight a political message and strengthen its symbolic meaning. This group is expected to continue their activities, using specific anniversaries or political events as opportunities.

Team UCC (Unknown Cyber Cult)

Team UCC is a hacktivist group believed to be based in India, with a pro-India and anti-Pakistan stance. They were found to be active since May 2025, primarily targeting private companies and government agencies in Pakistan.

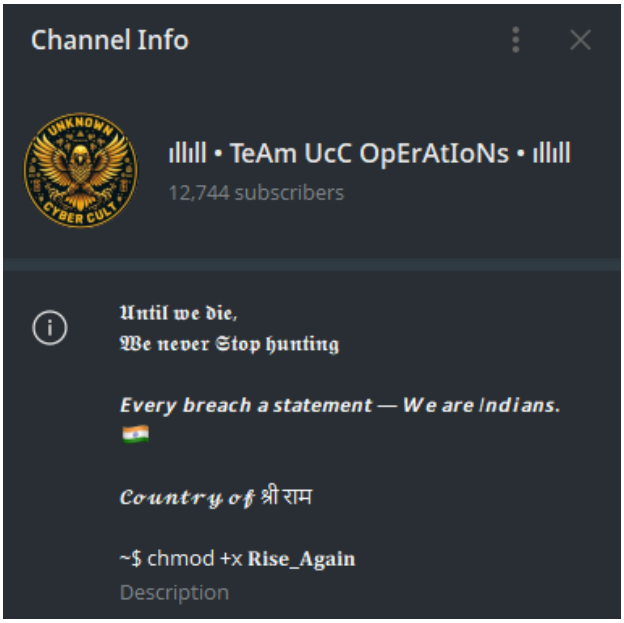


Figure 9. Team UCC's Telegram channel

The attack methods include system intrusion and data theft, leakage of internal documents and databases, website defacement, and data deletion and destruction, among others. They also use data leaks as political and ideological tools by combining a large-scale global data leak (16 billion password leak) with propaganda messages.

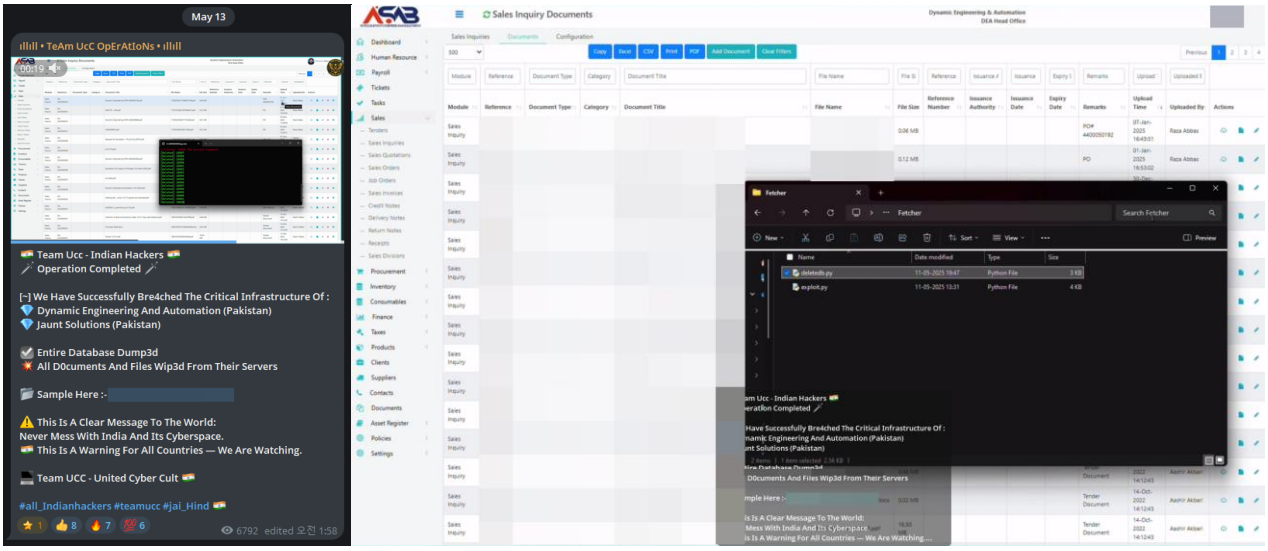


Figure 10. Deletion of Pakistan's Company D DB released by Team UCC

Major attack cases include the breach of Company D and Company J and the leak of the Logistics Management System DB in May 2025, and defacement of the Govt. Girls Degree College website on May 14. Additionally, the group displayed unusual behavior by performing a redefacement on Indian websites that had been defaced by Pakistan around July.

Team UCC did not just stop at attack activities; they also attempted to expand their influence by

releasing a Telegram bot for searching Pakistan SIM/CNIC. They are also focusing on spreading political and social messages by strengthening their identity through declarations like 'Revival of the Cyber Cult' and using social issues, such as airplane crash incidents, as propaganda tools. This group is expected to continue as a major India-based hacktivist group in the cyber conflicts between India and Pakistan.

Team White Lotus

Team White Lotus is a hacktivist group believed to be based in India, with a pro-India and anti-Pakistan stance.[20] They were active around May 2025, primarily targeting government agencies, state-owned enterprises, and telecommunications companies in Pakistan.

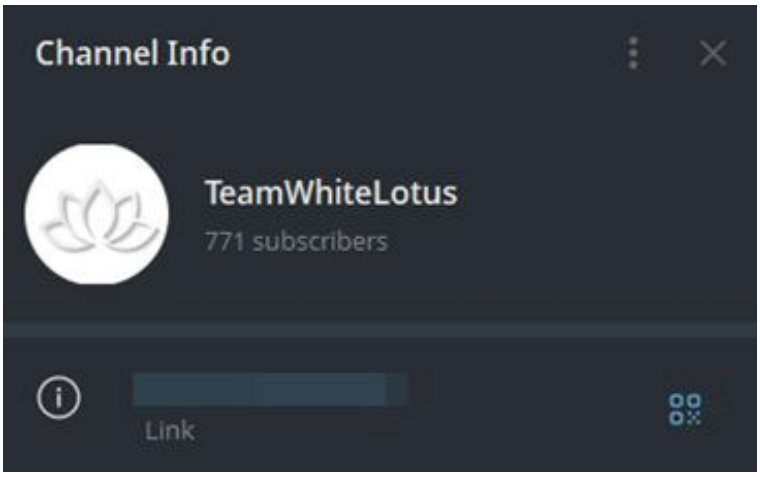


Figure 11. Team White Lotus's Telegram channel

This group uses attack methods such as web page defacement, admin panel infiltration, and website data deletion, and was observed uploading web shells in the process. Interestingly, instead of leaving a separate long message for propaganda, they only upload photos or videos proving the success of the attack.

The main targets are identified as Pakistani military and government agency websites, state-owned enterprises, telecommunications companies, and university websites.

[20] https://atip.ahnlab.com/threat-actor/view?seq=105333

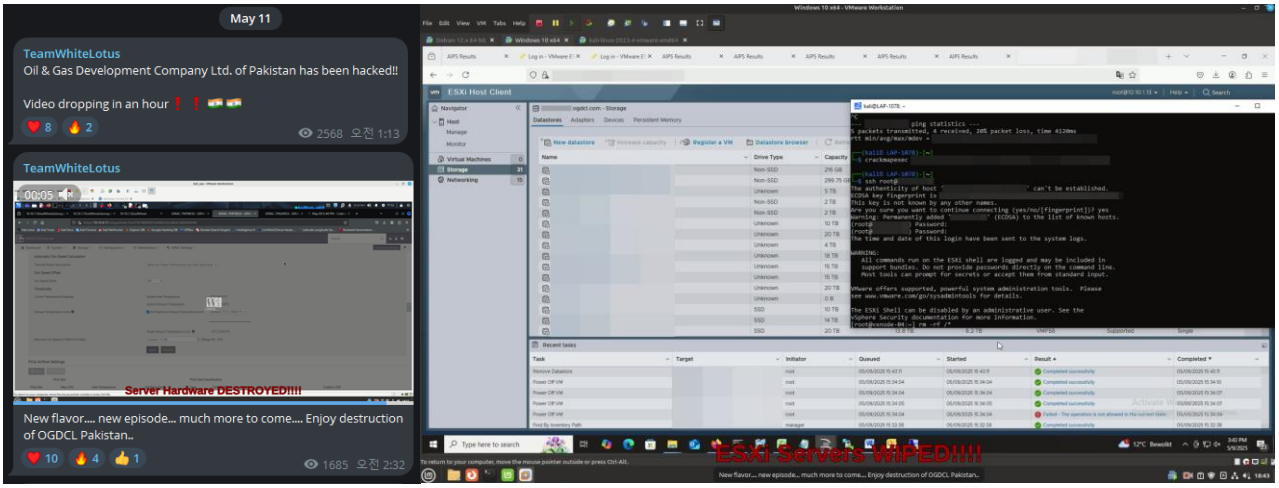


Figure 12. Wiping of Pakistan's OGDCL ESXi server released by Team White Lotus

Major attack cases reported in May 2025 include website attacks on Pakistan Rangers Sindh, National Defence University CMS, Pakistan Anti-Narcotics Force, Pak-Sat CMS, Military Lands & Cantonments Department, Pakistan Air Force, Oil & Gas Development Company Limited (OGDC), and Wateen Telecom. The attack was carried out in ways such as defacement, data deletion, and service disruption.

Team White Lotus has shown a high level of technical skill among hacktivist groups, as evidenced by wiping of ESXi servers, among other things. They appeared to be operating actively during the heightened tensions between India and Pakistan around last May, but recently, they seem to be inactive. However, if conflicts intensify again, they may resume their activities. Therefore, considering the behavior this group has shown so far, we must continue to exercise caution.

Conclusion

India-based APT groups and hacktivists are engaging in increasingly sophisticated and organized cyber activities. APT groups conduct information gathering and cyber espionage activities reflecting the strategic interests of the Indian government, while hacktivists engage in digital activism in response to political and social issues.

APT groups use various infiltration techniques such as spear phishing, malicious documents, and disguising mobile apps, and there have been increasing cases of exploitation of cloud infrastructure and mobile platforms. Their main targets are countries surrounding China and Pakistan, and in the future, there is a high possibility that they will expand their scope of activities to include supply chain attacks and attacks on industrial infrastructure.

Meanwhile, hacktivists are going beyond simple defacement or DDoS attacks and are now carrying out attacks that affect physical infrastructure, such as compromising industrial control

systems, hacking surveillance cameras, and causing data breaches. Some groups promote their attack achievements through Telegram or X (Twitter) and also conduct propaganda by combining social messages.

Their activities go beyond simple cyberattacks, having a tangible impact on international relations and information security. They also have a clear tendency to launch attacks timed with specific anniversaries or political events. In the future, India-based threat actors are expected to enhance both technical sophistication and political messaging, becoming key players in cyber conflicts.

Therefore, closely analyzing their trends and preparing proactive response strategies will be an important task not only for cybersecurity but also from diplomatic and policy perspectives.

References

[1] Vijay Anand. (July 29, 2024). North Korean Lazarus Group linked to $235 million WazirX crypto breach. CNBC TV18.

[2] The Express Tribune. (May 15, 2025). Security sources reveal details of Pakistan's massive cyberattack against India. The Express Tribune.

[3] Baezner, Marie. (August, 2018). Regional rivalry between India-Pakistan: tit-for-tat in cyberspace. ETH Zürich.

[4] Insikt Group. (September 2, 2025). Influence Operations and Conflict Escalation in South Asia. Recorded Future.

[5] CH Lei, Fyodor Yarochkin, Lenart Bermejo, Philippe Lin, Razor Huang. (January 24, 2018). Lazarus Campaign Uses Remote Tools, RATANKBA, and More. Trend Micro.

[6] ThreatsEye Lab. (August 12, 2024) Indian Hackers Threaten Moroccan Organizations. Scribd.

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
https://www.ahnlab.com | https://asec.ahnlab.com/en

About ASEC

AhnLab SEcurity intelligence Center (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab