Blogs

CloudSEK

Southeast Asia Region-specific Iran-israel War Threat Intelligence

info@cloudsek.com
www.cloudsek.com

Executive Briefing

Situation at Glance

On February 28, 2026, the United States and Israel jointly launched Operation Epic Fury, a coordinated pre-emptive military strike against Iranian nuclear and military infrastructure across Tehran, Isfahan, and Qom. Iran responded within hours with ballistic missile strikes against US military bases in Bahrain, Qatar, Kuwait, and the UAE. This marks the first full-scale direct kinetic war between Iran and Israel, ending years of shadow conflict and entering an open, multi-domain confrontation.

For Southeast Asia, this is not a distant conflict. It is an active threat event with immediate, measurable consequences across cybersecurity, financial systems, energy supply and political stability.

Why Southeast Asia is in the crosshairs

Southeast Asia sits at the intersection of four simultaneous risk vectors triggered by this war:

1. **Iran's Asymmetric Cyber Doctrine** - With its conventional military degraded by US-Israeli strikes, Iran's primary retaliation tool is offensive cyber operations. Iranian state-sponsored groups (APT33, APT34, APT35, APT42, MuddyWater) have pre-positioned infrastructure across global networks and will now activate it against US-aligned targets, energy sector organizations, financial institutions, and telecom providers, all heavily present in SEA.
2. **US Military Presence in the Region** - The Philippines hosts four active US EDCA military bases. Iran has already demonstrated willingness to strike US military infrastructure globally. These bases and the Philippine government systems and defense contractors around them, are plausible cyber and physical retaliation targets.
3. **Muslim-Majority Population Dynamics** - Malaysia and Indonesia, the world's third and first largest Muslim-majority nations respectively, face elevated risk of domestic radicalization, social unrest, and hacktivist mobilization should Iranian religious sites or civilian populations be struck. Pro-Palestinian hacktivist group INDOHAXSEC is already operationally active in both countries.
4. **Energy & Financial System Exposure** - 13 million barrels of oil per day transit the Strait of Hormuz, representing 31% of global seaborne crude. Iran has threatened and partially demonstrated Hormuz closure capability. Singapore operates as SEA's primary energy trading and refining hub. A blockade scenario would push oil to USD 130–300/barrel, a direct economic shock to every SEA economy. Singapore is also identified by FinCEN as one of three global hubs for Iranian shadow banking, with $9 billion in suspicious transactions in 2024 alone, placing it directly in the path of intensified US secondary sanctions enforcement.

THREAT INTELLIGENCE MATRIX

Country	Direct Iranian/Proxy Threats	Israeli/US Retaliation Risk	Documented Threat Actors	Critical Infrastructure at Risk	US/Israeli Assets Targeted	Evidence/Sources
🇵🇭 **Philippines**	**CRITICAL**: US military EDCA bases (Cagayan, Isabela, Palawan, Cebu) likely targets for Iranian proxy cyber/physical retaliation. Iran's doctrine explicitly targets US military installations globally.	**MODERATE**: If Philippine-based threat actors target Israeli interests, Israeli Unit 8200 has demonstrated willingness to conduct offensive cyber operations globally.	**APT41, Mustang Panda, Dark Pink, ToddyCat** (85% APT group coverage — highest in SEA alongside Vietnam). Iranian APT34/APT35 may pivot toward EDCA sites.	**Energy, telecom, government networks, US military logistics/C2 systems**	**US EDCA bases, Clark/Subic-adjacent facilities, US-linked defense contractors**	Philippines ranks #1 in SEA for APT targeting density; US-Philippines integrating "cutting-edge" cyber defense tech for Balikatan 2026, Iran fired ballistic missiles at US bases in Bahrain/Qatar today

🇲🇾 **Malaysia**	**HIGH**: Pro-Iranian hacktivist groups (CyberAv3ngers, Mr. Hamza, Team 313, Cyber Jihad) likely to target government/military sites via DDoS and defacement. Malaysia's vocal pro-Palestinian stance increases targeting likelihood. Iranian shadow banking networks ($9B via Singapore/HK) may route funds through Malaysian institutions.	**DOCUMENTED**: Israeli Mossad operationally active in Malaysia — kidnapped Hamas-linked Palestinian Omar al-Balbaisi (Oct 2022), who hacked Iron Dome in 2015-16. Israeli cyber attacks confirmed targeting Malaysian companies: Maxis (telecom), Aminia (palm oil), Yoututor (edtech), Dell regional HQ. Prime Minister Anwar Ibrahim confirmed June 2025 Mossad operates weapons/drug smuggling network recruiting Malaysian citizens.	**INDOHAXSEC** (pro-Palestinian Indonesian hacktivist group targeting Malaysia), **Israeli Unit 8200/Mossad** (confirmed active), **APT41, Mustang Panda** (Chinese espionage groups also active). Malaysian Army Salary System already breached by INDOHAXSEC	**Petronas (oil/gas), telecom (Maxis), government portals, palm oil sector, tech sector (Dell)**	**None confirmed** — Malaysia has no diplomatic relations with Israel, no Israeli embassy. However, Malaysian companies perceived as pro-West may be targeted by pro-Iranian groups.	Malaysian NC4 issued advisories on hacktivist threat; Israeli cyber attacks on Maxis, Aminia, Yoututor, Dell confirmed 2024-2026; Mossad kidnapping confirmed by Malaysian Home Affairs Ministry; PM Anwar confirmed Mossad recruitment networks June 2025

🇸🇬 **Singapore**	**HIGH**: Singapore is one of three global hubs for Iranian shadow banking ($9B in suspicious transactions 2024 via front companies/shell entities). Post-strikes, expect secondary sanctions pressure from OFAC. Iranian APT groups may target financial sector for sanctions evasion intelligence.	**MODERATE**: Singapore hosts US-linked financial institutions and Israeli-connected companies. As a US treaty ally and financial hub, hacktivist targeting likely.	**APT34 (OilRig), APT35 (Charming Kitten)** (Iranian state groups targeting telecom/finance sectors regionally), **UNC3886** (Chinese espionage group already active in Singapore)	**Financial services sector (banks, forex, fintech), energy trading/refining hubs, telecom infrastructure**	**US-linked financial institutions, Israeli company regional offices, Changi Naval Base (US visits), potential secondary sanctions targets**	FinCEN report (Oct 2025) identified Singapore as Iranian shadow banking hub with $9B in 2024 transactions; CSA Singapore already tracking nation-state threats including UNC3886; Singapore is US treaty ally and regional financial center

🇮🇩 **Indonesia**	**HIGH**: World's largest Muslim-majority nation — social unrest risk if Iranian religious sites struck. INDOHAXSEC pro-Palestinian hacktivist group already deploying ransomware/DDoS against perceived pro-Israeli entities. Terrorist groups increasingly exploiting digital tools for recruitment/financing (UNODC Jan 2026).	**LOW-MODERATE**: Indonesia has no formal Israeli diplomatic presence. Israeli targeting unlikely unless Indonesian threat actors significantly escalate.	**INDOHAXSEC** (pro-Palestinian ransomware/DDoS group allied with Russian NoName057(16), **APT41, Mustang Panda** (Chinese espionage groups), potential for Iranian APT pivot. Indonesian Government Land Authority credentials sold on dark web Feb 13, 2026.	**Government systems (Land Authority already compromised), energy infrastructure (oil import dependency), telecom, social media platforms**	**Western-linked companies, perceived pro-Israel entities, US company regional offices**	INDOHAXSEC confirmed active with ransomware capabilities [9][4]; Indonesian Gov Land Authority breach advertised Feb 13, 2026; UNODC regional meeting in Indonesia Dec 2025 addressed terrorist tech exploitation

🇹🇭 **Thailand**	**MEDIUM-HIGH**: 70% APT group coverage (third-highest in SEA). Hosts US military assets (Utapao, Cobra Gold exercises). Tourism sector faces soft-target risk if lone-wolf attacks materialize. Iranian APT groups may exploit distracted defensive posture during war escalation.	**LOW-MODERATE**: Thailand maintains balanced foreign policy. Israeli retaliation unlikely unless direct Thai-based attacks occur.	**APT41, Mustang Panda, Dark Pink, ToddyCat** (70% APT group coverage). Iranian APT34/APT35 may pivot to telecom/energy espionage.	**Government networks, defense systems, telecom infrastructure, tourism sector (hotels, airports), energy imports (oil price shock impact)**	**US military assets (Utapao Naval Air Base, Cobra Gold training sites), Western hotel chains, Israeli-branded tourism businesses**	Thailand has 70% APT group targeting coverage; hosts US military exercises annually; tourism sector comprises ~18% GDP (vulnerable to regional instability)
🇻🇳 **Vietnam**	**MEDIUM**: Shares 85% APT group coverage with Philippines (highest in SEA) but dominated by China-linked threats. Iran's telecom espionage campaigns targeting Asia supply chains may include Vietnam's expanding 5G infrastructure. War creates "distraction window" for opportunistic intrusions.	**LOW**: Vietnam maintains independent foreign policy. Israeli targeting unlikely.	**APT41, Mustang Panda, ToddyCat** (Chinese state groups), **Earth Kurma** (active since June 2024 targeting Vietnamese government for data exfiltration using rootkits) [12]. Potential for Iranian APT telecom targeting.	**Government sectors (Earth Kurma confirmed active), telecom/5G infrastructure, oil refining (Nghi Son, Binh Son vulnerable to Hormuz supply disruption)**	**None identified** — Vietnam has no US military bases; limited Israeli commercial presence	Vietnam has 85% APT group coverage; Earth Kurma confirmed targeting Vietnamese government since June 2024 [12]; Iranian APT groups historically target Asian telecom supply chains [13]

🇰🇭 **Cambodia**	**MEDIUM**: Weak regulatory environment makes Cambodia attractive for Iranian sanctions evasion via cryptocurrency/online gambling platforms. Risk profile is **abuse as conduit** rather than direct targeting.	**LOW**: Minimal Israeli/US strategic interest. Retaliation unlikely.	**General cybercriminal ecosystem** (crypto laundering, gambling sector exploitation). No confirmed nation-state APT focus.	**Cryptocurrency exchanges, online gambling platforms (used for sanctions evasion), weak government cybersecurity infrastructure**	**None identified**	Cambodia's crypto/gambling sector known as financial crime conduit; weak AML enforcement creates sanctions evasion risk

KEY THREAT ACTORS TARGETING SOUTHEAST ASIA

Iranian State Groups

- **APT34 (OilRig)** — Targets energy, telecom, government. Confirmed active with SideTwist Trojan and Menorah RAT. 9 active C2 IPs, 4 confirmed malware hashes.
- **APT35 (Charming Kitten**) — Spear-phishing via 36 confirmed fake domains impersonating Microsoft, LinkedIn, energy companies, and Israeli academic institutions. 18 active C2 IPs.
- **APT33 (Elfin/Peach Sandstorm)** — Aviation and energy sector targeting.
- **MuddyWater (Seedworm**) — Telecom supply chain espionage. High relevance for SEA's expanding 5G infrastructure.
- **APT42** — Now using Gemini AI agents for automated attack planning and reconnaissance. Represents a fundamental capability uplift.

Pro-Iranian Hacktivist Groups

- **Handala** — Exploiting CrowdStrike brand trust to distribute data-destructive payloads. SEA enterprises running CrowdStrike EDR are plausible targets for a war-themed lure campaign.
- **CyberAv3ngers** — IRGC-linked, targets OT/SCADA systems. Water, power, and industrial control systems are at risk.
- **INDOHAXSEC** — Indonesia-based pro-Palestinian group already conducting ransomware and DDoS operations in Malaysia. Allied with Russian NoName057.

Opportunistic Actors (Exploiting Distraction Window) - APT41, Mustang Panda, Dark Pink, ToddyCat, Earth Kurma — Chinese state-linked groups will intensify espionage operations against SEA governments during the geopolitical distraction period. Earth Kurma already confirmed active in Vietnamese and Philippine government networks using kernel rootkits.

Key Tactics, Techniques, and Procedures (TTPs) Mapped to MITRE ATT&CK

To effectively defend against Iranian state-sponsored operations escalating during this conflict, organizations must pivot from merely blocking Indicators of Compromise (IOCs) to detecting the underlying behaviors. Below are the confirmed TTPs utilized by the primary threat actors targeting the SEA region:

Threat Actor	Nexus / Focus	Primary MITRE ATT&CK TTPs	Key Malware & Tools	Defensive Priorities for SEA
APT34 (OilRig)	MOIS-linked *Focus:* Energy, Telecom, Government	**T1566.001**: Spearphishing Attachment **T1068**: Exploitation for Privilege Escalation (e.g., CVE-2024-30088) **T1059.001**: PowerShell Execution **T1071.004**: DNS Tunneling for C2	SideTwist Trojan, Menorah RAT, STEALHOOK, QUADAGENT, Helminth, Mimikatz, LaZagne	Monitor for typosquatted domains (e.g., google.com). Baseline and alert on unusual PowerShell execution and excessive DNS text record lookups picussecurity+1.

APT35 (Charming Kitten)	IRGC-linked *Focus:* Diplomatic, Academic, NGOs	**T1592 / T1595**: Active Scanning / Victim Profiling **T1190**: Exploit Public-Facing Apps (SharePoint, WordPress) **T1539**: Steal Web Session Cookie **T1213.003**: Data from Information Repositories	POWERSTAR, CharmPower, BellaCiao, NokNok (macOS), sqlmap	Implement strict conditional access policies. Alert on impossible travel logins and monitor for MFA-bypass via session cookie theft/replay
APT33 (Elfin)	IRGC-linked *Focus:* Aerospace, Defense, Energy	**T1566.002**: Spearphishing Link (Defense impersonation) **T1053.005**: Scheduled Tasks (Persistence) **T1561.002**: Disk Structure Wipe (Shamoon/StoneDrill)	Shamoon, StoneDrill, TURNEDUP, NANOCORE	Isolate OT/SCADA environments from IT networks. Hunt for unauthorized scheduled tasks and prepare for destructive (wiper) malware incident response threatpost+1.

MuddyWater	MOIS-linked *Focus:* Telecom Supply Chain, Govt	**T1584**: Compromise 3rd-Party Infrastructure (Legit sites as C2) **T1574.002**: DLL Side-Loading (PowGoop via GoogleUpdate.exe) **T1132**: Non-Standard Data Encoding (Modified Base64) **T1572**: Protocol Tunneling — DNS (Mori Backdoor) **T1059**: Scripting — LotL Abuse **T1027**: Obfuscated PowerShell Scripts	PowGoop (DLL loader), Mori (DNS tunnel backdoor), CHAR (Telegram Bot C2 — Jan 2026), POWERSTATS, Covicli, Sharpstats, Koadic RAT, Chisel, ngrok, Plink, Mimikatz, LaZagne	Block outbound Telegram Bot API calls from non-user processes (disrupts CHAR C2). Monitor GoogleUpdate.exe loading non-standard DLLs. Alert on high-volume outbound DNS TXT record queries (Mori tunneling). Enforce strict egress filtering.

Handala Hack	Pro-Iran Hacktivist *Focus:* Wipers, Tech Supply Chain	**T1036.005**: Match Legitimate Name or Location **T1485**: Data Destruction **T1567**: Exfiltration Over Web Service	Handala Wiper (Crowdstrike.exe NSIS installer), custom data destruction scripts	Monitor for fake software update lures (e.g., CrowdStrike/EDR fixes). Block unauthorized outbound API connections to Telegram (used for exfiltration) and monitor abuse of IP lookup services (e.g., icanhazip.com).
CyberAv3ngers	IRGC-linked Hacktivist *Focus:* OT / SCADA Systems	**T1190**: Exploit Public-Facing Apps **T1078.001**: Default Accounts / Credentials **T1565.002**: Manipulation of Control Processes	Custom PLC exploitation scripts targeting Unitronics Vision Series	Audit internet-facing PLCs (especially Unitronics). Disable default credentials, restrict OT management interfaces to internal VPNs, and disable exposed administrative ports (TCP 20256).

INDOHAXSEC	Indonesian Pro-Palestine Hacktivist *Focus:* DDoS, Defacement	**T1498.001**: Direct Network Flood (DDoS) **T1491.001**: Internal Defacement **T1486**: Data Encrypted for Impact	Custom DDoS tools, ransomware variants, credential harvesting kits	Implement aggressive web application firewalls (WAF) and DDoS mitigation. Monitor Telegram channels for operation announcements targeting specific organizations/countries (#OpMalaysia, #OpSingapore).

Universal Baseline Defensive Controls

These behavioral detections are not vendor-specific or tool-dependent. They address the overlapping attack behaviors shared across all seven threat actors documented in this report and should be treated as non-negotiable minimum controls during the current conflict escalation period.

1. Block Outbound Telegram Bot API Calls from Non-User Processes

Cuts Across: MuddyWater (CHAR C2), Handala (data exfiltration), INDOHAXSEC (attack coordination)

Telegram's Bot API (api.telegram.org) is being weaponized as a live command-and-control and exfiltration channel. Legitimate enterprise users access Telegram via browser or app — no business process should require a server or background process to call the Telegram API.

Implementation: Firewall egress rule blocking api.telegram.org from all non-approved endpoints. Alert on any DNS resolution of api.telegram.org from server infrastructure.

2. Alert on Abnormal PowerShell Execution Chains

Cuts Across: APT33, APT34, MuddyWater, INDOHAXSEC

PowerShell remains the single most abused execution environment across all Iranian state groups. Specifically hunt for:

- PowerShell spawned by Office applications (Word, Excel) — phishing document execution
- PowerShell with encoded command parameters (-EncodedCommand, -enc)
- PowerShell making outbound HTTP/HTTPS connections directly
- PowerShell executing from temp directories or user profile paths

Implementation: EDR rule alerting on powershell.exe with parent process = winword.exe, excel.exe, outlook.exe or child process = cmd.exe → powershell.exe chain.

3. Monitor High-Volume Outbound DNS TXT Record Queries

Cuts Across: APT34 (DNS tunneling C2), MuddyWater Mori Backdoor (DNS tunneling)

DNS tunneling is specifically chosen because most organizations do not monitor DNS traffic at the query-type level. Both APT34 and MuddyWater's Mori Backdoor use DNS TXT record queries to encode C2 commands and exfiltrate data — a technique invisible to HTTP/HTTPS-focused proxy monitoring.

Implementation: DNS firewall or SIEM rule alerting when a single endpoint generates >50 DNS TXT record queries within a 10-minute window to the same or rotating domains.

4. Detect DLL Side-Loading via Legitimate Application Paths

Cuts Across: MuddyWater (PowGoop via GoogleUpdate.exe), APT34, Mustang Panda

Threat actors plant malicious DLLs in directories alongside trusted executables, causing the legitimate binary to load the malicious library. This bypasses application whitelisting entirely.

Implementation: Alert when GoogleUpdate.exe, svchost.exe, or any signed Microsoft/Google binary loads a DLL from a non-standard or user-writable path (e.g., %AppData%, %Temp%, %Downloads%).

5. Alert on Bulk File Modification or Deletion Events

Cuts Across: Handala (wiper), APT33 (Shamoon/StoneDrill), INDOHAXSEC (ransomware)

Both wipers and ransomware share the same behavioral signature — mass file modification in rapid succession. This is detectable before encryption or deletion completes if monitoring is in place.

Implementation: EDR/SIEM alert when a single process modifies or deletes >100 files within 60 seconds. Automatically suspend the process and isolate the endpoint pending analyst review.

6. Monitor Non-Browser Outbound Connections to IP-Lookup Services

Cuts Across: Handala (pre-wipe victim reconnaissance via icanhazip.com)

Handala's wiper queries icanhazip.com to collect victim IP, hostname, and system information before initiating destruction — sending this data to a Telegram channel. icanhazip.com itself is legitimate, so it will not be blocked by reputation-based filters.

Implementation: Alert when any non-browser process (i.e., process is not chrome.exe, firefox.exe, msedge.exe) makes an outbound connection to icanhazip.com or similar IP-lookup services (ifconfig.me, ipinfo.io, checkip.amazonaws.com).

7. Detect Default Credential Usage on Internet-Facing OT/ICS Devices

Cuts Across: CyberAv3ngers (Unitronics PLCs), APT34 (OT targeting)

CyberAv3ngers explicitly targets PLCs and SCADA systems using factory-default credentials — a control failure that requires zero exploitation skill. Any internet-facing industrial device retaining default credentials is an immediate critical risk.

Implementation: Quarterly automated scan of all internet-facing OT/ICS management interfaces. Alert on any successful authentication using known default credential pairs for Unitronics, Siemens, Schneider Electric, and Honeywell platforms.

8. Monitor for War-Themed Spear-Phishing Lure Keywords

Cuts Across: APT33, APT34, APT35, Handala, INDOHAXSEC

All seven threat actors are currently generating phishing content leveraging the Iran-Israel war narrative. Email security gateways should flag and quarantine messages containing these subject line or body keywords:

Flag keywords: "Iran strikes", "Operation Epic Fury", "Hormuz closure", "CrowdStrike emergency patch", "oil supply disruption", "nuclear attack alert", "Gaza ceasefire update", "EDCA base advisory", "Israeli cyber retaliation"

Why Organizations Must Monitor These Threat Actors

These adversary groups have confirmed attack histories against sectors identical to those operating across Southeast Asia, and the Iran-Israel war has removed all prior restraints on their operations.

1. They Have Already Proven Reach Into Your Region

Every threat actor in this report has struck organizations structurally identical to those operating in SEA. APT34 has compromised telecom and energy supply chains; MuddyWater has breached government ministries via managed service providers; and critically, INDOHAXSEC has already breached the Malaysian Army System, this is not a future risk, it is a present one.

2. Wartime Mandate Removes Restraint

Prior to February 28, 2026, Iranian APT groups operated under implicit rules of engagement, prioritizing intelligence collection over destruction. With Iranian nuclear facilities struck and senior IRGC commanders killed, the political authorization for destructive cyber operations has been granted at the highest level. Adversary Groups previously restrained from deploying wiper malware against civilian infrastructure are now operating under a wartime mandate.

3. Your Organization May Be Infrastructure, Not the Target

MuddyWater and APT34 routinely compromise organizations not because they are the target, but because they are the path via managed service provider access, cloud hosting, or financial transaction routing to a higher-value target. You can become attack infrastructure without ever being the intended victim.

4. Non-Compliance Is Now a Legal Liability

For Singapore and Malaysia specifically, this is a regulatory emergency, not just a security issue. FinCEN has identified both nations as Iranian shadow banking hubs. Any organization processing Iran-linked transactions after documented public warnings faces direct OFAC secondary sanctions exposure making an unmonitored breach a legal failure, not merely a technical one.

5. The Cost Asymmetry Is Stark

Deploying 174 verified IOCs to a SIEM takes hours. Recovering from a confirmed APT34 energy sector breach or Handala wiper event takes weeks to months, costs millions in incident response, and risks permanent loss of government and enterprise contracts.

These adversary groups are not scanning the internet looking for weak targets at random. They have a pre-built list of organizations in SEA that sit adjacent to US military assets, energy infrastructure, financial systems, and government networks. Your organization is very likely already on that list. Monitoring for them is not best practice in the current geopolitical environment, it is the minimum viable security posture.

Next Steps for Organizations

Phase – 1 (Immediate)

Action	Responsible Team	Target Countries
Ingest all verified IOCs (domains, IPs, hashes) into SIEM, firewall, EDR	SOC / Threat Intel	All countries
Deploy war-themed phishing detection rules ("Iran strikes", "Hormuz closure", "CrowdStrike emergency update")	SOC / Email Security	All countries
Audit all internet-facing PLCs — change default credentials and restrict to internal VPN	OT Security	Philippines, Singapore, Thailand
Raise physical security posture at US-adjacent facilities, Western hotels, and embassy zones	Physical Security	Philippines, Malaysia, Thailand
Subscribe security teams to INDOHAXSEC, CyberAv3ngers, Handala Telegram channels for early warning	Threat Intel	Malaysia, Indonesia, Singapore
Report any known Iranian financial transaction exposure to compliance officers	Compliance / Legal	Singapore, Malaysia

Phase – 2 (Short Term)

Action	Responsible Team	Target Countries
Implement MFA-bypass detection rules — alert on session cookie theft and impossible travel logins	Identity Security	All countries
Conduct emergency audit of DNS traffic for tunneling patterns (APT34 IOC-aligned)	Network Security	All countries
Coordinate formally with national CERTs — CSA Singapore, NC4/NACSA Malaysia, BSSN Indonesia, DICT Philippines	CISO	All countries
Isolate OT/SCADA environments from enterprise IT networks if not already done	OT / ICS Security	Philippines, Malaysia, Singapore
Block all outbound Telegram API calls from non-approved enterprise devices	Network Security	All countries

Phase – 3 (Long Term)

Action	Responsible Team	Target Countries
Commission full MITRE ATT&CK-aligned threat hunt across critical infrastructure environments	Red Team / Threat Hunters	All countries
Implement AI-assisted phishing detection to counter APT42's Gemini AI-generated lures	Email Security / AI Tools	All countries
Establish a 14-day IOC refresh cadence — Iranian APT infrastructure rotates rapidly	Threat Intel	All countries
Conduct staff awareness training focused on war-themed social engineering lures	HR / Security Awareness	All countries
Review third-party vendor access — MuddyWater specifically targets supply chain and managed service providers	Vendor Risk	All countries
Submit IOC packages to regional MISP communities for cross-organization sharing	Threat Intel	All countries

Strengthening Your Defenses with the Right Intelligence

The threat landscape documented in this report is complex, fast-moving, and deeply contextual. Keeping pace with it manually — tracking 7 threat actor groups, rotating IOC infrastructure, dark web credential leaks, hacktivist Telegram channels, and real-time CVE exploitation timelines, is beyond the capacity of most security teams operating in isolation.

CloudSEK, ranked #1 in APAC for external threat intelligence, offers Southeast Asian organizations a practical way to operationalize everything documented in this report:

- When INDOHAXSEC announces #OpMalaysia on Telegram, you should know before your website goes down, not after. **CloudSEK's hacktivism monitoring provides that early warning window**.
- When APT34 registers a new typosquatted domain mimicking your brand or infrastructure, you should be alerted within hours, not discover it during an incident response. **CloudSEK's brand and phishing monitoring does exactly that.**
- When your employee's credentials appear on a dark web forum following a supply chain breach, you should find out before the threat actor logs in. **CloudSEK's dark web monitoring surfaces these exposures in real time.**
- When CVE-2024-30088 is being actively exploited by OilRig in the wild, your security team should already know if your systems are exposed. **CloudSEK's BeVigil continuously maps your attack surface against actively exploited vulnerabilities.**

"All IOCs in this report are a strong starting point. But IOCs decay, infrastructure rotates, domains expire, new hashes emerge. What organizations in SEA need right now is not a static list, but a continuously updated intelligence feed that evolves with the threat actors themselves."

IOC Summary

APT33 — Elfin / Peach Sandstorm / HOLMIUM

Domain		SHA256_HASHES	
boeing.servehttp.com	chromup.com	7eb2e9e8cd450fc353323fd2e8b84fbbdfe061a8441fd71750250752c577d198	
alsalam.ddns.net	securityupdated.com	ccb617cc7418a3b22179e00d21db26754666979b4c4f34c7fda8c0082d08cec4	
ngaaksa.ddns.net	googlmail.net	c57c5529d91cffef3ec8dadf61c5ffb2	6f1d5c57b3b415edc3767b079999dd50
ngaaksa.sytes.net	www.googlmail.net	c02689449a4ce73ec79a52595ab590f6	8e67f4c98754a2373a49eaf53425d79a
vinnellarabia.myftp.org	syn.broadcaster.rocks	59d0d27360c9534d55596891049eb3ef	3f5329cf2a829f8840ba6a903f17a1bf
managehelpdesk.com	mywinnetwork.ddns.net	10f58774cd52f71cd4438547c39b1aa7	663c18cfcedd90a3c91a09478f1e91bc
microsoftupdated.com		5df4269998ed79fbc997766303759768ce89ff1412550b35ff32e85db3c1f57b	
microsoftupdated.net	**C2 Server IP**	fb70ff49411ce04951895977acfc06fa468e4aa504676dedeb40ba5cea76f37f	
osupd.com	2.16.155.42	711d3deccc22f5acfd3a41b8c8defb111db0f2b474febdc7f20a468f67db0350	

APT34 - OilRig / Helix Kitten / Hazel Sandstorm / Crambus

Domain		SHA256 HASH
go0gie.com		8a8a7a506fd57bde314ce6154f2484f280049f2bda504d43704b9ad412d5d618
URL		64156f9ca51951a9bf91b5b74073d31c16873ca60492c25895c1f0f074787345
http://tecforsc-001-site1.gtempurl.com/ads.asp		5db93f1e882f4d7d6a9669f8b1ab091c0545e12a317ba94c1535eb86bc17bd5b
IP Address		704360d765f6f1ef735594c7ff5fb6c47467dad8abc3133f8e935a6c0c804c8a
192.99.102.35	83.142.230.138	
136.243.214.247	178.33.94.47	
138.201.7.140	149.202.230.140	
136.243.203.141	85.117.204.18	
158.69.57.61		

APT35 - Charming Kitten / Mint Sandstorm / TA453

Domain		SHA256_HASHES
linkedinz.me	mideasthiring.com	03d0e7ad4c12273a42e4c95d854408b98b0cf5ecf5f8c5ce05b24729b6f4e369
sharepointnotify.com	office-shop.me	35a485972282b7e0e8e3a7a9cbf86ad93856378fd96cc8e230be5099c4b89208
updateddns.ddns.net	onedrivelive.me	5afc59cd2b39f988733eba427c8cf6e48bd2e9dc3d48a4db550655efe0dca798
mastergatevpn.com	onedriveupdate.net	6dc0600de00ba6574488472d5c48aa2a7b23a74ff1378d8aee6a93ea0ee7364f
microsoftcdn.co	service.chrome-up.date	767bd025c8e7d36f64dbd636ce0f29e873d1e3ca415d5ad49053a68918fe89f4
microsoftdefender.info	online-chess.live	ac8e59e8abeacf0885b451833726be3e8e2d9c88d21f27b16ebe00f00c1409e6
microsoftedgesh.info	updatedefender.net	977f0053690684eb509da27d5eec2a560311c084a4a133191ef387e110e8b85f
outlookdelivery.com	my-mailcoil.ml	cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa
webmaiil-tau-ac-il.ml	mail-macroadvisorypartners.ml	668ec78916bab79e707dc99fdecfa10f3c87ee36d4dee6e3502d1f5663a428a0
savemoneytrick.com	owa-insss-org-ill-owa-authen.ml	724d54971c0bba8ff32aeb6044d3b3fd571b13a4c19cada015ea4bcab30cae26
sparrowsgroup.org	supportskype.com	24a73efb6dcc798f1b8a08ccf3fa2263ff6158710fdec1f2b7641f05550fe3b
talent-recruitment.org	talktalky.azurewebsites.net	28332bdbfaeb8333dad5ada3c10819a1a015db9106d5e8a74beaaf03797511aa
updateservices.co	service.chrome-up.date	e6f4ce982908108759536f5aff21fa6686b8ea8153fdd4cdd087cceff5f1748a

IP ADDRESS		SHA256_HASHES
54.37.164.254	109.202.99.98	927289ddccbb1de98fe3f8af627296d0d7e9833c8f59e5e423fe283b6792da89
134.19.188.242	134.19.188.243	9dce6086c61c23420ac497f306debf32731decc5527231002dbb69523fad3369
134.19.188.244	134.19.188.246	6e842691116c188b823b7692181a428e9255af3516857b9f2eebdeca4638e96e
185.23.214.188	213.152.176.205	bf308e5c91bcd04473126de716e3e668cac6cb1ac9c301132d61845a6d4cb362
213.152.176.206	146.59.185.15	bc8f075c1b3fa54f1d9f4ac622258f3e8a484714521d89aa170246ce0470144
146.59.185.19	185.23.214.187	918e70e3f5fdafad28effd512b2f2d21c86cb3d3f14ec14f7ff9e7f0760fd760
85.114.138.96	168.100.8.190	
168.100.10.216	207.244.79.143	
217.23.5.166	137.74.131.208	

Handala Hack / Handala Hack Team / Handala Group

Domain	SHA256 HASH
icanhazip.com	9e519211947c63d9bf6f4a51bc161f5b9ace596c2935a8eedfce4057f747b961
crowdstrike.com.vc	

Handala operates as a hacktivist collective, not a structured state-sponsored APT with dedicated long-term infrastructure. They do not maintain a persistent network of C2 servers, rotating malware variants, or sustained phishing domains the way APT33/34/35 do. Their operations are campaign-based, they strike, publicize the damage on Telegram, and move on.

Defensive Control	What It Catches
Block outbound connections from non-browser processes to icanhazip.com	**Wiper pre-execution reconnaissance**
Monitor for NSIS installer execution from email/download paths	**Initial wiper deployment**
Alert on bulk file modification events in rapid succession	**Active wiper execution**
Block unauthorized Telegram API calls from endpoints	**Data exfiltration to Telegram**
Phishing awareness for fake vendor update emails	**Initial access vector**

MuddyWater - Seedworm / Mango Sandstorm / TA450

Domain	SHA256_HASHES
arbiogaz.com	12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa
azmwn.suliparwarda.com	dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92
bangortalk.org.uk	9d50fcb2c4df4c502db0cac84bef96c2a36d33ef98c454165808ecace4dd2051
best2.thebestconference.org	2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82
camco.com.pk	7e7545d14df7b618b3b1bc24321780c164a0a14d3600dbac0f91afbce1a2f9f4
cbpexbrasilia.com.br	b5b1e26312e0574464ddef92c51d5f597e07dba90617c0528ec9f494af7e8504
	e7baf353aa12ff2571fc5c45184631dc2692e2f0a61b799e29a1525969bf2d13
	255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a
	5bcdd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f
	9cb79736302999a7ec4151a43e93cd51c97ede879194cece5e46b4ff471a7af7
	9ec8319e278d1b3fa1ccf87b5ce7dd6802dac76881e4e4e16e240c5a98f107e2
	b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a
	ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9

IP ADDRESS		SHA256_HASHES
148.251.204.131	109.201.140.103	e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca
144.76.109.88	137.74.131.16	b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c
138.201.75.227	137.74.131.18	42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986
106.187.38.21	137.74.131.20	3098dd53da40947a82e59265a47059e69b2925bc49c679e6555d102d1c6cbbc8
103.73.65.129	137.74.131.24	63e404011aeabb964ce63f467be29d678d0576bddb72124d491ab5565e1044cf
103.73.65.225	137.74.131.25	94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472
103.73.65.244	137.74.131.30	b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca
103.73.65.246	141.95.177.130	
103.73.65.253	146.70.124.102	
45.150.64.23	146.70.149.61	
162.223.89.11	157.90.152.26	
185.254.37.173	37.120.237.204	
194.61.121.86	37.120.237.248	
195.20.17.44	45.132.75.101	

CloudSEK

Predict ◆ Protect ◆ Quantify

We **Predict** Cyber Threats **Before They Strike**

Registered Office:

CloudSEK Research Pte. Ltd.
160 Robinson Road, #20-03, Singapore Business Federation Center, Singapore - 068914

Regional Office : India

CloudSEK Information Security Pvt Ltd.
16/1, Cambridge Rd, Halasuru, Cambridge Layout, Jogupalya, Bengaluru, Karnataka - 560008

Regional Office : United States

CloudSEK Inc.
8 The Green, Ste A, Dover, DE - 19901, United States

Regional Office : United Kingdom

CloudSEK, 2 Kingdom Street,
6th Floor London, W2 6BD - United Kingdom

CloudSEK

info@cloudsek.com www.cloudsek.com

Scan for a free Demo of CloudSEK platform