ACICE
ADMM Cybersecurity and
Information Centre of Excellence

Monthly Digest

Issue 09/24 (Sep)

A monthly round-up of significant news around the world

Cybersecurity

New Multi-Stage Backdoor Used by Peach Sandstorm to Gain Access to Targets in Critical Sectors

1. From Apr to Jul 2024, Microsoft observed threat actor Peach Sandstorm's use of a new multi-stage backdoor, Tickler, to target companies in the satellite, communications, oil and gas sectors, as well as defence and government sectors in Australia, Europe, the United Arab Emirates and the United States.

2. Prior to Tickler, Peach Sandstorm had used password spraying[1] and social engineering via LinkedIn to form connections with targets and illegally access sensitive information held by satellite and defence organisations.

3. With Tickler, existing compromised user accounts were used to procure operational Microsoft Azure infrastructure, which then served as command and control (C2) tools for Peach Sandstorm operations targeting government, defence and space infrastructure. Trojan malware disguised as a PDF as well as software to collect network information from targets were also part of Tickler's attack arsenal. Finally, upon gaining access to a single device, Tickler utilised various exploits to infect other devices on the same network. For example, during Peach Sandstorm's recent cyberattack on a European defence organisation, a network sharing protocol was exploited to infect other computers on the same network and establish a foothold for long-term intelligence gathering.

[1] In a password spray attack, a threat actor attempts to use a single password or a list of commonly used passwords to enter many different accounts.

4. Overall, the usage of Tickler showed a notable increase in Peach Sandstorm’s ability to infiltrate various sectors, including the defence sector, using multiple cyberattack tools.

5. To reduce the chance of an attack, Microsoft advised device users to use strong passwords, change passwords regularly, ensure multi-factor authentication was turned on, and frequently review sign-in activity for suspicious sign-in attempts.

Use of ToneShell Backdoor to Target Attendees of the IISS Defence Summit

6. On 3 Sep 2024, cybersecurity researchers reported the discovery of a malicious executable .exe file disguised as the official agenda for the IISS Prague Defence Summit in Nov 2024. The Defence Summit is a key forum for the discussion of defence strategies and security concerns in the Euro-Atlantic region, and key attendees include officials from Europe, the US and other allied nations.

7. The malware had C2 signatures like those used in ToneShell malware; ToneShell had previously been linked to Mustang Panda cyber espionage campaigns targeting governments and non-governmental organisations. The malware also evaded detection using techniques like those previously used by Mustang Panda.

8. Notably, the malware was designed to establish persistence in compromised devices for long-term stealing of data. Combined with the specific targeting of defence officials, there is possibility of a cyber espionage campaign that could lead to the potential compromise of sensitive defence information over time.

Critical Microsoft Zero-Day Vulnerability in Servicing Stack

9. On 10 Sep 2024, Microsoft announced a previously undisclosed critical vulnerability (CVE-2024-43491) in the Servicing Stack for some versions of Windows 10. For these versions, security updates installed from Mar 2024 to Aug 2024 resulted in the rolling back of fixes for previously mitigated vulnerabilities. This vulnerability was detected internally by Microsoft’s Windows product team.

10. While Microsoft had not detected any exploitation of CVE-2024-43491 itself, exploitation of other vulnerabilities due to the rolling back of fixes had been reported. Hence, Microsoft had given this vulnerability a CVSS severity score of 9.8/10. Affected users were instructed to install Sep 2024’s Servicing Stack update (SSU KB043936), followed by the Sep 2024 Windows security update (KB5043083).

Artificial Intelligence (AI)

Unveiling of the World's First International Standard Covering the Life Cycle of Large Language Models (LLMs)

1. On 6 Sep 2024, the World Digital Technology Academy (WDTA) and various China and US technology companies came together to unveil their *Large Language Model Security Requirements for Supply Chain* security standard during a side event at the Inclusion Conference on the Bund[2] in Shanghai, China. WDTA is a non-governmental organisation, registered in Geneva following the United Nations' guidance framework. Established in Apr 2023, it has five major action objectives[3], and included prominent technology companies such as Google, Microsoft, OpenAI, Meta, Huawei and iFLYTEK.

2. LLMs are large-scale models trained on large amounts of data that can understand instructions and generate outputs in various forms, including human languages, program codes and images. They form the backbone of many generative AI models, including OpenAI's ChatGPT and Google's Bard. Specific to the military, LLMs can be used to automate scenario planning, synthesise large amounts of intelligence and generate targeting recommendations.

3. The security standard published on 6 Sep 2024 was the result of a successful collaboration between China and US companies. This security standard was significant as it provided a comprehensive framework to ensure an LLM's confidentiality, integrity and availability throughout its entire life cycle, from development to deployment. It also represented another milestone in private-sector collaboration among numerous prominent technology companies, and may eventually lay the foundation for future collaborations involving other private- and public-sector stakeholders.

[2] Held from 5 to 7 Sep 2024, this Conference had "Technology for a Sustainable Future" as its theme. The event, which was attended by more than 100 technology companies and research institutions, aimed to explore AI's impact on various sectors in society, including technology accessibility, sustainability, life sciences, and technological ethics.

[3] WDTA's five major action objectives are: promoting the sustainable development of the digital economy, cultivating high-quality technical talents, driving global technological cooperation and sharing, serving society and economic industrial development, and making digital technology accessible to all humanity.

Information

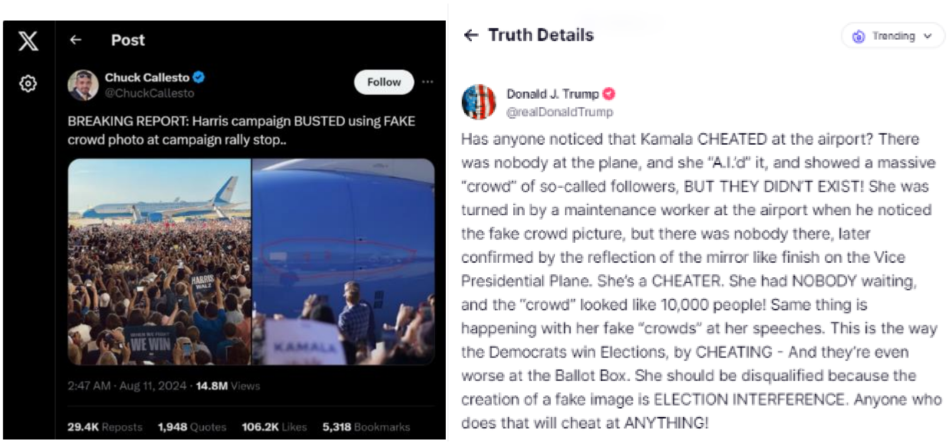
US Presidential Candidate Kamala Harris' Detroit Rally Photos – Real or Fake

1. US presidential candidate Kamala Harris held her Detroit rally on 7 Aug 2024 at an airport hangar. Several days after, various social media posts, including one by fellow candidate Donald Trump, claimed that the crowd shown in her rally photos were fake and were added using artificial intelligence (AI).

2. These social media posts used a zoomed-in photo of an airplane engine showing no crowd reflection to support their assertion. Notably, no other editing software was used to create the zoomed-in photo, unlike other types of fake news such as deepfakes.

3. Hany Farid, a professor at the University of Carolina, Berkeley's School of Information, used two different computer models to analyse the crowd photo in question; patterns associated with generative AI images were not detected. News sites such as *Reuters*, *NPR* and the *BBC* had also published photos of the real crowd taken from different angles by their photographers. Using these sources of information, fact-checking websites such as *Poynter* and *AAP FactCheck* concluded that the crowd at Harris' rally was real, and not added in using AI. Several photographers suggested that the airplane engine showed no crowd reflection because of the large distance between the airplane and the crowd at the rally.

4. The public's increased awareness about deepfakes had been used by opportunistic actors to falsely claim that legitimate content was artificially generated by AI. This could invoke oppositional rallying to advance these actors' agendas.



Chuck Callesto @ChuckCallesto

BREAKING REPORT: Harris campaign BUSTED using FAKE crowd photo at campaign rally stop..

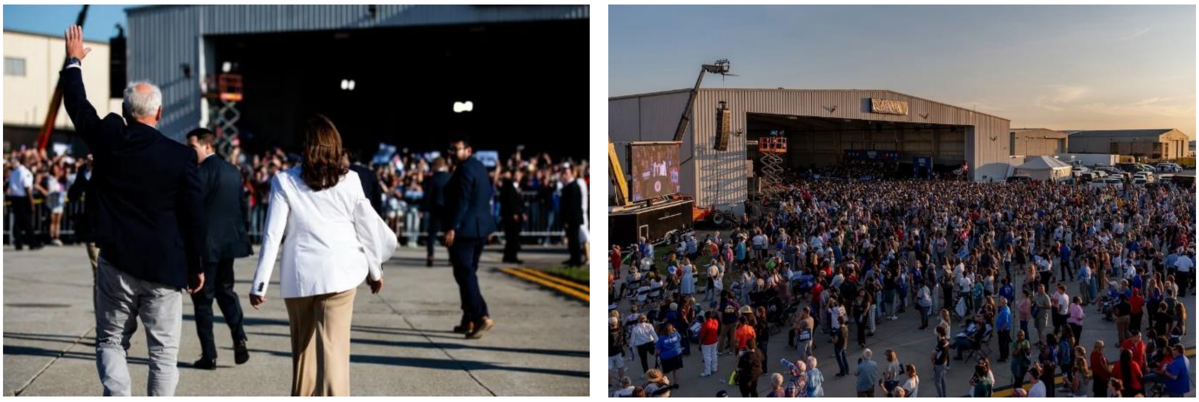
2:47 AM · Aug 11, 2024 · 14.8M Views

29.4K Reposts 1,948 Quotes 106.2K Likes 5,318 Bookmarks

Donald J. Trump @realDonaldTrump

Has anyone noticed that Kamala CHEATED at the airport? There was nobody at the plane, and she "A.I.'d" it, and showed a massive "crowd" of so-called followers, BUT THEY DIDN'T EXIST! She was turned in by a maintenance worker at the airport when he noticed the fake crowd picture, but there was nobody there, later confirmed by the reflection of the mirror like finish on the Vice Presidential Plane. She's a CHEATER. She had NOBODY waiting, and the "crowd" looked like 10,000 people! Same thing is happening with her fake "crowds" at her speeches. This is the way the Democrats win Elections, by CHEATING - And they're even worse at the Ballot Box. She should be disqualified because the creation of a fake image is ELECTION INTERFERENCE. Anyone who does that will cheat at ANYTHING!

Social media posts asserted crowds at Kamala Harris' rally to be fake (Source: X/[@]ChuckCallesto and Truth Social/[@]realdonaldtrump)



Photos of the real crowd from different angles, taken by news sites' photographers
(Source: Getty Images and The Associated Press)

Terrorism

ISIS Attacks Oman for the First Time

1. On 15 Jul 2024, three ISIS attackers opened fire on a Shia Mosque in Muscat, Oman, killing six and wounding at least 30 others. This was the first ISIS attack in Oman.

2. ISIS claimed responsibility for the attack on 16 Jul 2024, and made the attack the editorial subject of its weekly newsletter *Al-Naba 452*, published on 18 Jul 2024. In the editorial, ISIS framed the attack as retaliation for the imprisonment of ISIS members in Iraq, Syria, Lebanon, and Yemen, and incited "young Muslims everywhere" to target Shias in Yemen or Lebanon.

3. Encouraged by the successful attack, pro-ISIS media groups renewed calls for attacks against Shia targets between 10 and 18 Jul 2024.

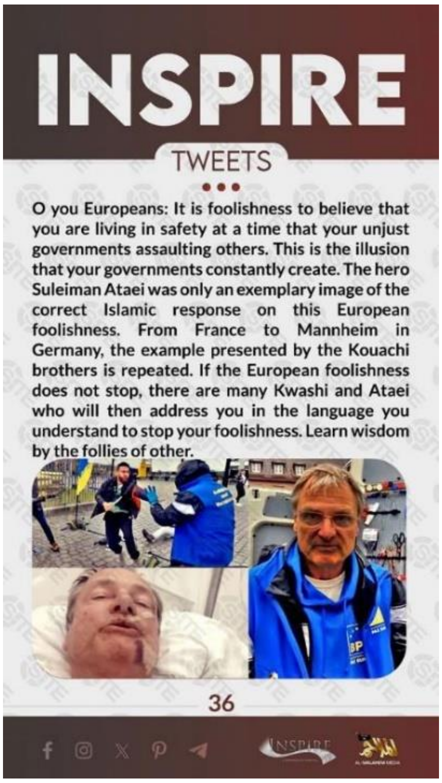
ISIS content on the 15 Jul 2024 Oman attack
(Source: Middle East Monitor and Amaq News Agency)

Significant AQAP Publications

4. Between 24 Jul to 5 Aug 2024, the official AQAP media unit *Al-Malahem Media Foundation* published incitement materials via the Telegram and Rocketchat social media platforms.

5. The group published Arabic and English versions of the 8th edition of the "Inspire Guide", a five-page document which analysed the 31 May 2024 Mannheim stabbing attack in Germany and encouraged lone-wolf jihadists to carry out similar strikes against those who insult Islam. The document also suggested that would-be attackers use firearms to target anti-Islamic government officials.

6. During the same period, it also published #35 to #57 of its "Inspire Tweets" posters. Some of these posters cited Salem/Salim Sharif, the alleged AQ emir Sayf Al-Adl's pen name. The posters mainly denounced Western leaders and threatened attacks on the West. Arabic leaders, armies and security personnel were also listed as possible targets.



INSPIRE

TWEETS

O you Europeans: It is foolishness to believe that you are living in safety at a time that your unjust governments assaulting others. This is the illusion that your governments constantly create. The hero Suleiman Ataei was only an exemplary image of the correct Islamic response on this European foolishness. From France to Mannheim in Germany, the example presented by the Kouachi brothers is repeated. If the European foolishness does not stop, there are many Kwashi and Ataei who will then address you in the language you understand to stop your foolishness. Learn wisdom by the follies of other.

36

Example of an AQAP "Inspire Tweet"
(Source: Terrorism Research & Analysis Consortium)

ISIS-EA Attack Claims

7. On 24 Jul 2024, ISIS-East Asia (ISIS-EA) claimed a 20 Jul 2024 attack in Shariff Saydona Mustapha, Maguindanao del Sur, that targeted Philippines soldiers, allegedly "killing and wounding multiple elements".

8. Mainstream media corroborated ISIS-EA's claims, highlighting an attack which killed one and injured two Philippines soldiers engaged in flood relief work.

9. This is the 11th ISIS-EA attack claim for 2024.

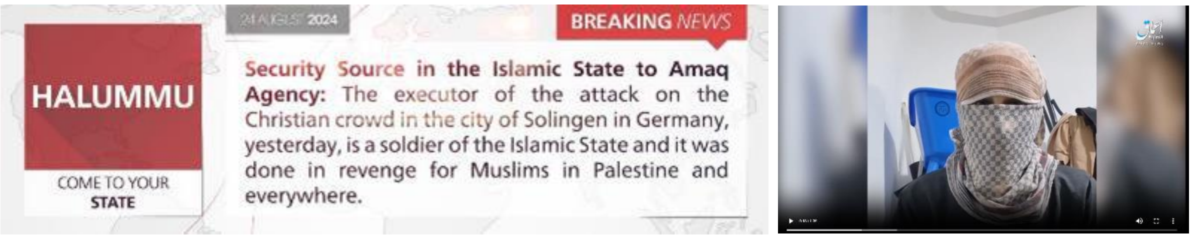
ISIS-Inspired Stabbing Attack in Solingen, Germany

10. On 23 Aug 2024, a 26-year-old Syrian national stabbed several people celebrating a festival at a central market square in Solingen, Germany, killing three and wounding eight others. The attacker surrendered to police a day later.

Authorities reported that the perpetrator was a Syrian war refugee and could be an ISIS member. Three others were also arrested in relation to the attack.

11. ISIS claimed the attack promptly on 24 Aug 2024 and released official content on the attack via its media outlets, *Amaq News Agency* and *Al-Naba*. Pro-ISIS supporters and various pro-ISIS media groups celebrated the attack and called for attacks on other German cities such as Cologne. This attack came amid constant calls to conduct attacks in reprisal for the current atrocities in Palestine.

12. Germany last reported a stabbing attack in May 2024, where a pro-ISIS individual attacked an anti-Islam rally in Mannheim, killing one and wounding five others.



Security Source in the Islamic State to Amaq Agency: The executor of the attack on the Christian crowd in the city of Solingen in Germany, yesterday, is a soldier of the Islamic State and it was done in revenge for Muslims in Palestine and everywhere.

ISIS content on the 23 Aug 2024 Germany stabbing attack
(Source: Watson News)

ISIS Propagates Calls for "Jihad in Europe"

13. On 29 Aug 2024, the official ISIS newsletter *Al-Naba* spotlighted recent attacks in Europe in its editorial piece, including the Aug 2024 Solingen stabbing attack in Germany and the Volgograd hostage-taking in a Russian prison. ISIS claimed that such attacks served to "take revenge on behalf of the Muslims" and "strengthen Islamic unity".

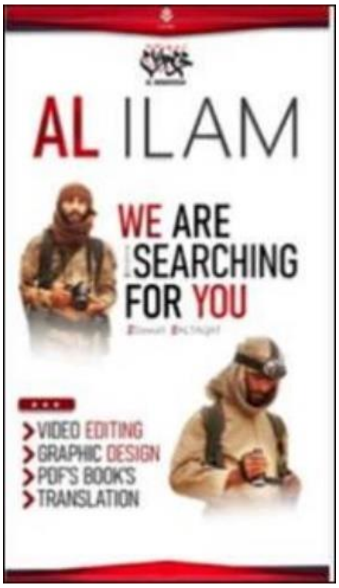
14. ISIS incited Muslim youths to target Christians and Jews, especially in Europe and America, to overwhelm government departments and security apparatuses. Specific targets mentioned included synagogues, neighbourhoods, and bars. ISIS advocated for the use of tactics such as melee weapons (knife, axe, hammer) and vehicle ramming.

Launch of New English-language Magazine Series, *Protect*

15. On 16 Aug 2024, a new English-language extremist magazine, *Protect*, was promoted by Rocketchat user *dawood.123.* The magazine provided guidance to ISIS supporters on how to shield their privacy while on the Internet to avoid detection by authorities. It was produced by the pro-ISIS *Al-Muwaddah Media Foundation.*

16. The Rocketchat user *dawood.123* shared that the *Al-Muwaddah Media Foundation* would be going official and highlighted that those in charge of the foundation were seeking "official recognition" from ISIS.

17. *dawood.123* also posted a recruitment poster for the foundation; the foundation is currently recruiting video editors, graphic designers, and translators.



Recruitment Poster by Al-Muwaddah Media Foundation

The Monthly Digest has been refreshed to cover more recent news related to cyber and information domains of relevance to the defence sectoral.

CONTACT DETAILS

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

REFERENCES

Cybersecurity

New Multi-Stage Backdoor Used by Peach Sandstorm to Gain Access to Targets in Critical Sectors

1. Peach Sandstorm Deploys New Custom Tickler Malware in Long-Running Intelligence Gathering Operations
   https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/

2. Iranian APT Peach Sandstorm teases new Tickler malware
   https://www.computerweekly.com/news/366609332/Iranian-APT-Peach-Sandstorm-teases-new-Tickler-malware

Use of ToneShell Backdoor to Target Attendees of the IISS Defence Summit

3. ToneShell Backdoor Targets IISS Defence Summit Attendees in Latest Espionage Campaign
   https://securityonline.info/toneshell-backdoor-targets-iiss-defence-summit-attendees-in-latest-espionage-campaign/?&web_view=true

4. ToneShell Backdoor Targets IISS Summit
   https://www.broadcom.com/20240909-toneshell-backdoor-targets-iiss-summit

5. ToneShell Backdoor Used to Target Attendees of the IISS Defence Summit
   https://hunt.io/blog/toneshell-backdoor-used-to-target-attendees-of-the-iiss-defence-summit

6. ToneShell Backdoor Used to Target Attendees of the IISS Defence Summit
   https://xfe-integration.xforce.ibm.com/osint/guid:35651b56dd94196cbf73cffabbc98c2f

7. ToneShell (Malware Family)
   https://malpedia.caad.fkie.fraunhofer.de/details/win.toneshell

8. Mustang Panda (Threat Actor)
   https://malpedia.caad.fkie.fraunhofer.de/actor/mustang_panda

9. Stately Taurus Linked to Attacks on Southeast Asian Government
https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/

Critical Microsoft Zero-Day Vulnerability in Servicing Stack

10. Microsoft Windows Update Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491

Artificial Intelligence

Unveiling of the World's First International Standard Covering the Life Cycle of Large Language Models (LLMs)

1. Large Language Model Security Requirements for Supply Chain
https://www.wdtacademy.org/publications/LLM

2. World Digital Technology Academy
https://www.wdtacademy.org/about/overview

3. New AI Supply Chain Standard Brings Together Ant, Tencent, Baidu and Microsoft, Google, Meta
https://www.scmp.com/tech/big-tech/article/3277447/new-ai-supply-chain-standard-brings-together-ant-tencent-baidu-and-microsoft-google-meta

4. Shanghai Conference to Explore Intersection of AI and Society
https://english.shanghai.gov.cn/en-Events/20240904/8b1b796541ed492daf95c356c0e3b2d8.html

5. Inclusion Conference on the Bund
https://www.inclusionconf.com/

6. Why the Military Can't Trust AI
https://www.foreignaffairs.com/united-states/why-military-cant-trust-ai

7. Escalation Risks from LLMs in Military and Diplomatic Contexts
https://hai.stanford.edu/sites/default/files/2024-05/Escalation-Risks-Policy-Brief-LLMs-Military-Diplomatic-Contexts.pdf

8. First International Standard for LLMs To Be Developed by US-China Tech Coalition
   https://www.techradar.com/pro/first-international-standard-for-llms-to-be-developed-by-us-china-tech-coalition

9. New Global Standard Aims to Build Security Around Large Language Models
   https://www.zdnet.com/article/new-global-standard-aims-to-build-security-around-large-language-models/

Information

US Presidential Candidate Kamala Harris' Detroit Rally Photos – Real or Fake

1. ChuckCallesto on X
   https://x.com/ChuckCallesto/status/1822344031537426861

2. realDonaldTrump on Truth Social
   https://truthsocial.com/@realDonaldTrump/posts/112944255426268462

3. Trump Falsely Claims Harris Crowd Was Faked
   https://www.bbc.com/news/articles/cx2lmm2wwlyo

4. Why It Matters That Trump Falsely Said a Harris Rally Was Fake
   https://www.npr.org/2024/08/14/nx-s1-5072687/trump-harris-walz-election-rally-ai-fakes

5. Images From Kamala Harris' Aug. 7 Detroit Rally Are Real, Not Artificial Intelligence
   https://www.poynter.org/fact-checking/2024/kamala-harris-supporters-ai-images-video-detector/

6. US Candidate Kamala Harris's Rally Crowd Photos Not Altered With AI
   https://www.aap.com.au/factcheck/us-candidate-kamala-harriss-rally-crowd-photos-not-altered-with-ai/

7. Fact Check: Plane Reflection Not Proof of Image Manipulation at Michigan Harris Rally
   https://www.reuters.com/fact-check/plane-reflection-not-proof-image-manipulation-michigan-harris-rally-2024-08-22/

8. Photographer Andrew Harnik Shoots Down Trump's Kamala Harris Plane Crowd Conspiracy

https://www.thedailybeast.com/photographer-andrew-harnik-shoots-down-trumps-kamala-harris-plane-crowd-conspiracy

9. Misunderstood Mechanics: How AI, TikTok, and the Liar's Dividend Might Affect the 2024 Elections
https://www.brookings.edu/articles/misunderstood-mechanics-how-ai-tiktok-and-the-liars-dividend-might-affect-the-2024-elections/

10. The Liar’s Dividend: Can Politicians Claim Misinformation to Evade Accountability?
https://isps.yale.edu/research/publications/isps24-07

11. Deepfakes, Elections, and Shrinking the Liar’s Dividend
https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend

12. Deep Fakes
https://www.jstor.org/stable/26891938

Terrorism

1. Oman Shia Mosque Attackers Were Omani Citizens, Police Say
https://www.middleeastmonitor.com/20240718-oman-shia-mosque-attackers-were-omani-citizens-police-say/

2. AQAP “Inspire” Poster
https://trackingterrorism.org/chatter/aqap-inspire-tweets-poster-western-countries-attacks-trac/

3. Terrorism Research & Analysis Consortium on X
https://x.com/TracTerrorism

4. IS Publishes Video Purporting to Show Perpetrators of Solingen
https://www.watson.ch/international/islamischer-staat-is/806559434-is-veroeffentlicht-video-das-taeter-von-solingen-zeigen-soll

5. ISIS Calls for Jihad in Europe to Avenge Muslim Deaths in the Gaza Strip
https://www.terrorism-info.org.il/en/isis-calls-for-jihad-in-europe-to-avenge-muslim-deaths-in-the-gaza-strip/