ADMM Cybersecurity and Information Centre of Excellence

Monthly Digest

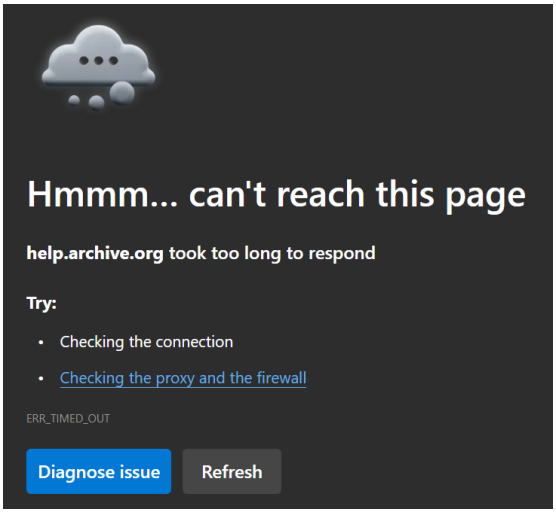
Issue 11/24 (Nov)

A monthly round-up of significant news around the world

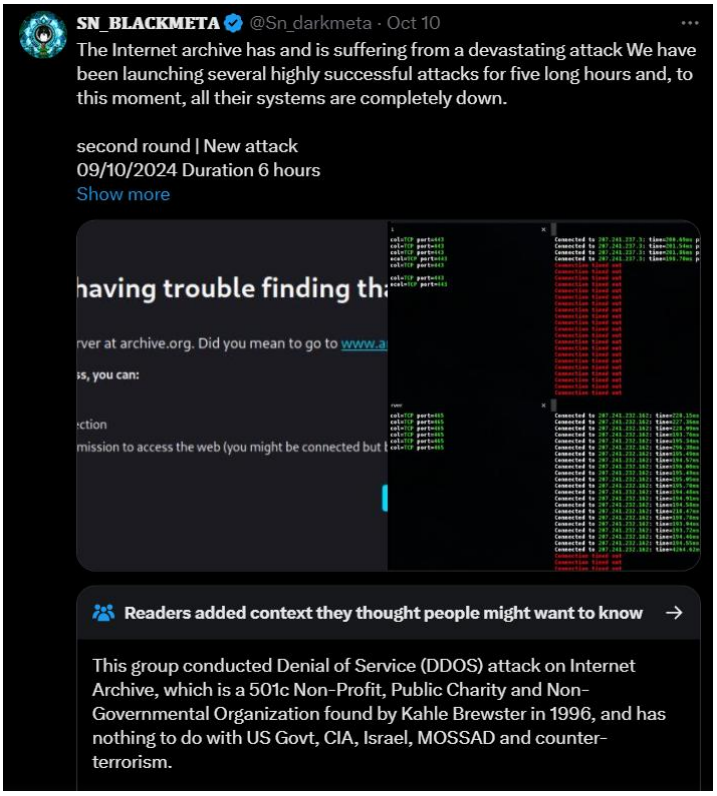
Cybersecurity

Multiple Cyberattacks on Internet Archive

1. Internet Archive (IA) is an American 501c non-profit digital library which offers millions of free books, movies and audio files, with the aim of providing "Universal Access to All Knowledge". Over the week of 9 Oct 2024, IA services were taken offline due to multiple distributed denial-of-service (DDoS) attacks by the pro-Palestine BlackMeta hacktivist group. Subsequent recovery efforts took weeks, and IA announced on X on 29 Oct 2024 that they were still working to secure systems and bring more services online.

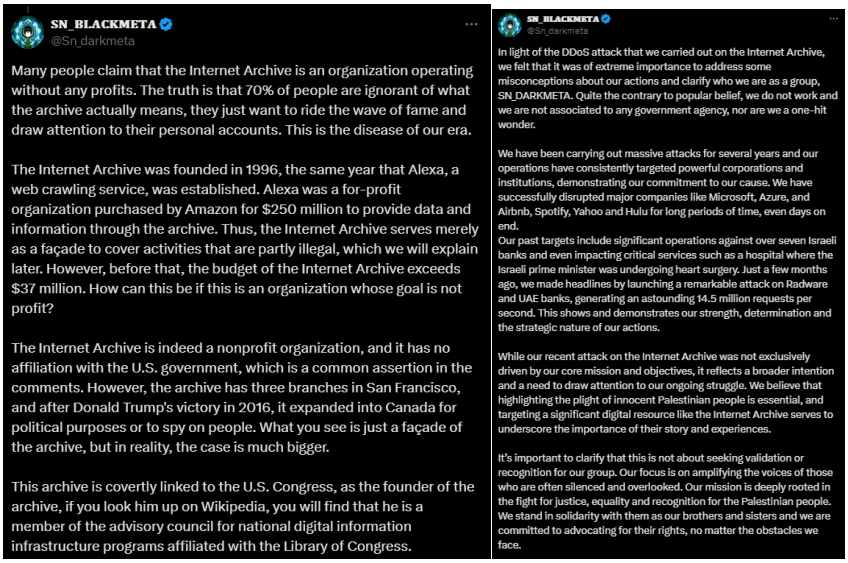


ADMM Cybersecurity and Information Centre of Excellence (ACICE)'s attempts to visit IA's Help Centre webpage were unsuccessful
(Source: ACICE and IA Help Centre)



BlackMeta claiming responsibility for the DDoS attacks on IA
(Source: X/[@]Sn_darkmeta)

2. On X, BlackMeta claimed that IA was "covertly linked to the United States (US) Congress", to which numerous users responded that IA is a 501c non-government organisation with no ties to the US government. BlackMeta also stated that its goal for these attacks were to highlight "the plight of innocent Palestinian people" and "fight for justice, equality and recognition for the Palestinian people".



BlackMeta explaining their reasons for targeting IA
(Source: X/[@]Sn_darkmeta)

3. During the same period, IA also suffered a data breach by a different unknown threat actor that resulted in the theft of 31 million users' email addresses, screen names and Bcrypt-hashed passwords. The threat actor also stole application programming interface (API) access tokens for IA's Zendesk support system, and subsequently used these tokens to gain unauthorised access to IA's Zendesk system on 20 Oct 2024. According to BleepingComputer, data in IA's Zendesk system might include users' personal identifiable information. BleepingComputer further stated that this threat actor hacked IA with the goal of increasing their reputation within the threat actor community.

Second threat actor, unknown and unaffiliated with BlackMeta, defaced the IA website and stole 31 million users' data
(Source: BleepingComputer)

4. This incident showed the devastating impact of multiple simultaneous cyberattacks on a single entity. While targeting the same entity, the two threat actors had seemingly different goals, showing the increasingly complex cyber threat landscape that cyber defenders have to defend against. Finally, while IA would not be considered critical infrastructure, the cyberattacks on it affected millions of users for a prolonged period of time, and underscored the importance of cybersecurity even for non-critical infrastructure.

Ransomware Group Interlock Targeting FreeBSD Systems

5. Since end-Sep 2024, the ransomware group Interlock had claimed attacks on six organisations, including Wayne County, a county in the US state of Michigan. Other victims were from the investment, healthcare and manufacturing sectors.

6. Notably, Interlock malware was designed to target FreeBSD systems, in addition to Microsoft systems. According to BleepingComputer, Interlock is only the second ransomware group to specifically target FreeBSD systems, which are widely used in servers and critical infrastructure. Trend Micro's Cybersecurity Research Team suggested that future Interlock attacks could aim to disrupt vital services. Therefore, there is a need to be aware of Interlock's tactics, techniques and procedures (TTPs) to better safeguard against the actor's potential attacks.

Malicious Remote Desktop Protocol (RDP) Files Utilised in Cyberattacks by Midnight Blizzard

7. Since 22 Oct 2024, Microsoft Threat Intelligence, the US Cybersecurity and Infrastructure Security Agency (CISA) and Ukraine's Computer Emergency Response Team (CERT-UA) observed threat actor Midnight Blizzard, also known as APT29, sending highly targeted spear-phishing emails to individuals in more than 100 organisations, including government, defence and non-governmental entities.

8. According to Microsoft, the US and UK governments had linked APT29 to the Russian Foreign Intelligence Service. Since 2018, APT29 was reported to have targeted governments, diplomatic entities, non-governmental organisations and information technology service providers across US, Europe, Australia and Japan to collect intelligence and conduct espionage.

9. Notably, the spear-phishing emails contained malicious RDP files, which would provide the threat actor with access to the target via a remote server once executed. APT29 could then extract sensitive information, including smart card and clipboard contents, from the compromised target. The threat actor could also install malware on the compromised target's computer. This was APT29's first use of RDP files in its cyberattacks.

10. To prevent successful attacks, Microsoft and CISA advised users to implement phishing-resistant multi-factor authentication (MFA), such as Microsoft Authenticator or Fast IDentity Online (FIDO) tokens, and to avoid Short Messaging Service (SMS) MFA. Users should also install endpoint detection and response systems on their computers. Finally, Microsoft and CISA recommended organisations to conduct user education on how to spot and report suspicious emails to reduce the impact of spear phishing emails.

Artificial Intelligence (AI)

Military Use of Meta's AI Models

1. *Reuters* reported on 1 Nov 2024 that, since Jun 2024, China had developed a military-focused AI tool, ChatBIT, using Meta's open-source large language model, Llama. ChatBIT could gather and process intelligence, and offer accurate and reliable information for operational decision-making.

2. In response, a Meta spokesperson stated that "any use of our models by the People's Liberation Army is unauthorised and contrary to our acceptable use policy". According to Meta's acceptable use policy, users were prohibited from using its AI models, including Llama, for defence and national security applications such as "military, warfare, nuclear industries or applications, espionage". This policy applied to users from all countries, including the US.

3. However, in an apparent policy shift, Meta subsequently announced on 4 Nov 2024 that it was "making Llama available to US government agencies, including those that are working on defence and national security applications". In explaining this shift, Meta highlighted that the responsible use of Llama in US national security applications would "help the US lead in AI and strengthen global security". Meta did not mention whether this policy shift applied to other countries, such as China.

US' National Security Memorandum on AI

4. On 24 Oct 2024, the US issued its National Security Memorandum on AI as part of its comprehensive strategy for responsible innovation. This development stemmed from the recognition that advances at the frontier of AI could have significant implications for national security and foreign policy in the near future.

5. According to the White House, the Memorandum would direct critical actions to (a) ensure that the US leads the world's development of safe, secure and trustworthy AI; (b) enable the US government to harness cutting-edge AI, while protecting human rights and democratic values, to achieve national security objectives; and (c) advance international consensus and governance around AI.

6. The US also released a Framework to Advance AI Governance and Risk Management in National Security on the same day. This Framework aimed to guide the implementation of the Memorandum, including mandating mechanisms for risk management, evaluations, accountability and transparency. Through such

mechanisms, US agencies were required to monitor, assess and mitigate AI risks related to (a) invasions of privacy, bias and discrimination; (b) the safety of individuals and groups; and (c) other human rights abuses.

Information

10 Inauthentic Websites Blocked by Singapore Authorities

1. On 22 Oct 2024, Singapore's Infocomm Media Development Authority (IMDA) instructed local Internet Access Service Providers to disable access to 10 inauthentic websites for users in Singapore.

2. According to IMDA, the 10 websites had been observed to be masquerading as Singapore websites by "using terms associated with Singapore in their domain name and incorporating familiar local features and visuals". In an S. Rajaratnam School of International Studies (RSIS) commentary published on 23 Oct 2024, Benjamin **Ang**, Head of Centre of Excellence for National Security (CENS) at RSIS and member of the ACICE Experts Panel, pointed out that such websites might carry non-controversial lifestyle or entertainment news to avoid scrutiny and appear authentic. In addition, Ang stated that there could be a coordinated network of websites promulgating the same fake news stories to create an "illusory truth effect" through users' repeated exposure to the stories.

3. Malicious actors could deploy these disinformation tactics to influence the local population through hostile information campaigns intended to sway public sentiments. Ang gave an example of a finding via a reverse internet protocol search that one of the inauthentic websites, Alamak.io, had links to an ".ru" domain, which is used for Russian entities. Alamak.io carried AI-generated Singaporean content, and also published factually inaccurate commentaries on socio-political issues in Singapore. Hence, Alamak.io was one of the 10 websites blocked by IMDA as a pre-emptive measure.

4. Besides the pre-emptive blocking of inauthentic websites using legislation, Ang highlighted that countermeasures could include public education programmes on how to recognise inauthentic websites and their potential adverse impacts, so as to safeguard information integrity.

Terrorism

Arrests and Foiled Plot in Central Java, Indonesia

1. On 4 Nov 2024, Indonesia's Counterterrorism Special Detachment 88 (Densus 88) arrested three suspected terrorists across Central Java. The suspects were associated with Jamaah Ansharut Daulah (JAD), an umbrella organisation established in 2015 comprising 24 Indonesian extremist groups.

2. One of the suspects, Bahrul Irfan, had planned to conduct acts of terror. Details of the plot and targets were not specified. Meanwhile, Sutaryono alias Abu Zaid and SQ had incited others to conduct terror acts through religious study groups and social media. This development indicated the continued presence of threats from JAD elements in Indonesia.

Regional Extremists Utilised Artificial Intelligence in Propaganda Material

3. Regional extremists had utilised AI to create deepfake videos of deceased terrorist leaders in two propaganda videos.

4. These videos featured prolific Malaysian Jemaah Islamiyah (JI) bombmakers Azahari Husin, who masterminded several attacks on Indonesia including the 2002 Bali bombings, and Noordin Mohammad Top, who was behind the suicide bombings in Jakarta in 2009.

5. These videos had garnered over 120,000 and 90,000 likes respectively. The reach of these videos suggested that they could be effectively used by regional extremists to conduct recruitment activities.

Screenshots of videos featuring deceased Malaysian JI bombmakers Azahari Husin and Noordin Mohammad Top

REFERENCES

Cybersecurity

Multiple Cyberattacks on Internet Archive

1. Internet Archive's Wayback Machine is Back Up After Data Breach - With a Catch
   https://www.zdnet.com/article/internet-archives-wayback-machine-is-back-up-after-data-breach-with-a-catch/

2. Internet Archive Hacked, Data Breach Impacts 31 Million Users
   https://www.bleepingcomputer.com/news/security/internet-archive-hacked-data-breach-impacts-31-million-users/

3. Internet Archive Breached Again Through Stolen Access Tokens
   https://www.bleepingcomputer.com/news/security/internet-archive-breached-again-through-stolen-access-tokens/

4. Sn_darkmeta on X
   https://x.com/Sn_darkmeta/

5. brewster_kahle on X
   https://x.com/brewster_kahle

6. internetarchive on X
   https://x.com/internetarchive

7. Internet Archive Services Update | Internet Archive Blogs
   https://blog.archive.org/2024/10/28/internet-archive-services-update/

8. Internet Archive: About IA
   https://archive.org/about/

Ransomware Group Interlock Targeting FreeBSD Systems

9. Meet Interlock — The New Ransomware Targeting FreeBSD Servers
   https://www.bleepingcomputer.com/news/security/meet-interlock-the-new-ransomware-targeting-freebsd-servers/

10. Ransomware.live - Group: Interlock
    https://www.ransomware.live/group/interlock

11. Cyberattack Hits Wayne County; Services Affected As Hacker Demands Ransom
https://www.wxyz.com/news/local-news/investigations/cyberattack-hits-wayne-county-government-services-affected-as-hacker-demands-ransom

12. FreeBSD Servers Subjected to Novel Interlock Ransomware Attacks
https://www.scworld.com/brief/freebsd-servers-subjected-to-novel-interlock-ransomware-attacks

13. TrendMicroRSRCH on X
https://x.com/TrendMicroRSRCH/status/1851172123399606517

Malicious Remote Desktop Protocol (RDP) Files Utilised in Cyberattacks by Midnight Blizzard

14. Russia Midnight Blizzard Hackers Target Government Sector
https://therecord.media/russia-midnight-blizzard-hackers-target-government-sector

15. CERT-UA Identifies Malicious RDP Files in Latest Attack on Ukrainian Entities
https://thehackernews.com/2024/10/cert-ua-identifies-malicious-rdp-files.html

16. Midnight Blizzard | Microsoft
https://www.microsoft.com/en-us/security/security-insider/midnight-blizzard

17. Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments
https://www.cisa.gov/news-events/alerts/2024/10/31/foreign-threat-actor-conducting-large-scale-spear-phishing-campaign-rdp-attachments

18. RDP Configuration Files as a Means of Obtaining Remote Access to a Computer or “Rogue RDP” (translated from Ukrainian)
https://cert.gov.ua/article/6281076

19. Midnight Blizzard Conducts Large-Scale Spear-Phishing Campaign Using RDP Files
https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

20.'Midnight Blizzard' Targets Networks with Signed RDP Files
https://www.darkreading.com/cyberattacks-data-breaches/midnight-blizzard-targets-networks-signed-rdp-files

21.Microsoft Warns of Russian Spear-Phishing Attacks Targeting Over 100 Organizations
https://www.securityweek.com/microsoft-warns-of-russian-spear-phishing-attacks-targeting-over-100-organizations/

22.Midnight Blizzard Escalates Spear-Phishing Attacks
https://www.techrepublic.com/article/midnight-blizzard-spearphishing-us-officials/

Artificial Intelligence

Military Use of Meta's AI Models

1. Exclusive: Chinese Researchers Develop AI Model for Military Use on Back of Meta's Llama
https://www.reuters.com/technology/artificial-intelligence/chinese-researchers-develop-ai-model-military-use-back-metas-llama-2024-11-01/

2. Chinese Military Adapts Meta's Llama for AI Tool
https://dig.watch/updates/chinese-military-adapts-metas-llama-for-ai-tool

3. Meta Permits Its A.I. Models to Be Used for U.S. Military Purposes
https://www.nytimes.com/2024/11/04/technology/meta-ai-military.html

4. Open-Source AI Can Help America Lead in AI and Strengthen Global Security
https://about.fb.com/news/2024/11/open-source-ai-america-global-security/

US' National Security Memorandum on AI

5. FACT SHEET: Biden-Harris Administration Outlines Coordinated Approach to Harness Power of AI for U.S. National Security
https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/24/fact-sheet-biden-harris-administration-outlines-coordinated-approach-to-harness-power-of-ai-for-u-s-national-security/

6. NSM Framework to Advance AI Governance and Risk Management in National Security (PDF)
   https://ai.gov/wp-content/uploads/2024/10/NSM-Framework-to-Advance-AI-Governance-and-Risk-Management-in-National-Security.pdf

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. Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence
   https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/

Information

10 Inauthentic Websites Blocked by Singapore Authorities

1. How a Network of Inauthentic Websites Could Be a Threat to Singapore
   https://www.rsis.edu.sg/rsis-publication/rsis/how-a-network-of-inauthentic-websites-could-be-a-threat-to-singapore/

2. Ten Inauthentic Websites Blocked for Potential Threat
   https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/ten-inauthentic-websites-blocked

3. Study Finds Russian Link to Website Blocked by Singapore Government
   https://www.channelnewsasia.com/singapore/alamak-io-russia-links-foreign-interference-4710121

4. Singapore Blocks 10 Websites Set Up by Foreign Actors Over Potential Hostile Information Threat
   https://www.channelnewsasia.com/singapore/singapore-blocks-websites-foreign-interference-hostile-information-mha-imda-fica-4692746

5. Malicious Foreign Actors Playing 'Long Game' Using Credible-Looking Websites and Gen AI: Analysts
   https://www.channelnewsasia.com/singapore/malicious-foreign-actors-long-game-credible-looking-websites-gen-ai-hostile-information-4694276

Terrorism

1. Densus 88 Nabs Three Suspected Terrorists in Central Java
   https://en.tempo.co/read/1937352/densus-88-nabs-three-suspected-terrorists-in-central-java

2. Three Terror Suspects Arrested in Central Java - Indonesian Police
   https://thesun.my/world-news/three-terror-suspects-arrested-in-central-java-indonesian-police-HE13243501

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