MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

January 2022

- **Serious log4j vulnerability leads to rise in cyberattacks**
- **Amendments introduced to Australian Critical infrastructure Act**
- **Government to set up national cyber security task force for critical infrastructure**
- **IGF and OEWG sessions held in December**
- **India File**

Serious log4j vulnerability leads to rise in cyberattacks

A vulnerability in a ubiquitous piece of Java software, log4j, has resulted in attacks worldwide on internet connected enterprise software. The vulnerability, first disclosed on December 9, allows attackers to execute malicious code on systems where the software has been downloaded. According to a Microsoft report, so far, "attackers have exploited the flaw to install cryptominers on vulnerable systems, steal system credentials, burrow deeper within compromised networks, and steal data."[1]

The Apache Foundation which developed the software, released patches within a week but the vulnerability still presents a severity rating of 10 as most enterprises and organisations are still unaware that the software is present in their systems since it is usually downloaded as a bundle or is part of other enterprise software. CERT-In advisories were issued on December 10th and 16. In a press release issued on December 22, The US Cybersecurity and Infrastructure Security Agency (CISA) along with other international cybersecurity agencies noted that "Numerous groups from North Korea, Iran, Turkey and China have been seen exploiting the vulnerability alongside a slate of ransomware groups and cybercriminal organizations." [2]

Later reports indicated that the vulnerability was first discovered by an engineer at Alibaba Cloud in late November of 2020 who then reported it to Apache, the developers of the software. Subsequently, the Cyber Security Administration of the Ministry of Industry and Information Technology (MIIT) suspended Alibaba Cloud, a part of the China based Alibaba group from its ongoing information-sharing partnership for six months since it did not follow the requirement of China's Cybersecurity Law to report all such vulnerabilities to the ministry rather than to the affected software developer, as part of its efforts to develop a library of zero-day exploits to be used in cyberattacks as well as to prepare a defence from such attacks.[3]

Amendments introduced to Australian Critical infrastructure Act

Australia passed amendments to the Security of Critical Infrastructure Act 2018 on December 2, 2021, to deliver an enhanced framework for the security of critical infrastructure. The amendments expanded the list of critical sectors from four to eleven. Critical infrastructure is now deemed to consist of entities in communications, financial services and markets, data storage or processing, defence industry, higher education and research, energy, food and grocery, health care and medical, space technology, transport, and water and sewerage. [4]

The government also arrogated to itself the power to intervene and "take over" entities in the event of cyber incidents as a "last resort." This power has been criticised by cybersecurity companies for setting a "troublesome global precedent" since they were not "subject to reasonable due process, which would normally allow affected entities to appeal or have these decisions independently reviewed." The requirement of reporting cyber incidents within a 12 hour framework would also result in companies having to set aside manpower to fulfil such duties at a time when they would be better engaged in responding to such incidents.[5] For its part, the government has maintained that these powers would be used only in the rarest of circumstances and invoking them required

a process in which the Minister for Home Affairs has to get agreement from the Prime Minister and the Minister of Defence.[6]

The Australian government has put further amendments out for public discussion which are designed to clarify many of the doubts raised by the previous amendments as well as further expand the provisions of the ACT to bring more entities within the ambit of critical infrastructure.[7]

Government to set up national cyber security task force for critical infrastructure

According to newspaper reports, the Indian government is in the process of setting up a unified national-level cyber security task force with specialised sub-level task forces within it to focus on priority sectors.[8] The need for such a task force was felt with increasing attacks on critical infrastructure and a more centralised response than the existing system which largely depends on the Computer Emergency Response Team-India (Cert-IN) as the first responder. With enhanced collaboration with international partners on the anvil, there would have to be real-time co-ordinated responses to inputs on cyber-attacks from across the world. The task force is expected to act in conjunction with CERT-In.

The first sub-level taskforce is expected to be set up in the telecom sector which is already in the throes of change with the impending shift to 5G. This unit would be populated by officers with the "relevant skill sets and capabilities required specifically for the telecom sector."

IGF and OEWG sessions held in December

*The 2021 edition of the Internet Governance forum (IGF) was hosted by the Government of Poland from 6 to 10 December with the theme, *Internet United.* Over 70 sessions were held on various topics from development to socio-cultural issues to cybersecurity. The cybersecurity sessions focussed on the implementation of agreed-upon norms and the necessity of involving all stakeholders in the process. It was felt that cyber-norms should continue to be developed through the existing UN mechanisms but with increased involvement of other stakeholders, be it civil society or private enterprises.[9]

*The first Substantive Session of the UN Open Ended Working Group (OEWG) on s*ecurity of and in the use of information and communications technologies 2021-2025* was held at New York from 13-17 December 2021. The OEWG was established with an unprecedented five-year mandate and is chaired by Singapore.

The two member Indian delegation, led by Shri Atul Malhari Gotsurve, Joint Secretary (eG & IT and CD), delivered substantive statements covering the gamut of existing and emerging cyber threats and cooperative measures to prevent and counter such threats, application of international law to the use of ICTs by States, confidence-building measures, cyber capacity building and the possibility of establishing a regular institutional dialogue under the auspices of the UN for all matters related to the use and security of ICTs.[10]

The second substantive session will be held from 28 March to 1 April 2022.

India File

*Indian views on the Scope, Objectives and Structure on the Ad Hoc Committee (AHC) to elaborate a comprehensive International Convention on countering the use of Information and Communications

Technologies for criminal purposes were presented to the United Nations on 6 December 2021. India welcomed the participation of multi-stakeholders in giving their suggestions, feedback etc. to the UN Ad Hoc Committee on Cybercrime that can be considered by Member States in the regular session of AHC. The detailed statement presented by India can be viewed at https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/India_-_Views_on_scope_objective_and_structure_7.12.2021_1.pdf

The Open-Ended Ad Hoc Intergovernmental Committee of Experts (AHC) has been set up to initiate a formal negotiation process with the outcome of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, in other words, to outline a global legal instrument to deal with cybercrime. The first meeting is to be held in New York from Monday, January 17, 2022, to Friday, January 28, 2022.

[1] The Log4J Vulnerability Will Haunt the Internet for Years at https://www.wired.com/story/log4j-log4shell/?utm_source=pocket_mylist

[2] Log4j flaw: Attackers are 'actively scanning networks' warns new CISA guidance at https://www.zdnet.com/article/cisa-cybersecurity-centers-from-australia-nz-uk-and-canada-release-log4j-advisory/

[3] China regulator suspends cyber security deal with Alibaba Cloud at https://www.reuters.com/world/china/china-regulator-suspends-cyber-security-deal-with-alibaba-cloud-2021-12-22/

[4] Amendments to the Security of Critical Infrastructure Act 2018 at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018-amendments

[5] Tech giants say gov cyber incident intervention powers 'unworkable' at https://www.itnews.com.au/news/tech-giants-say-gov-cyber-incident-intervention-powers-unworkable-571327

[6] Gov says 'community' expected it to have cyber incident intervention powers at https://www.itnews.com.au/news/gov-says-community-expected-it-to-have-cyber-incident-intervention-powers-573053

[7] Gov puts forward second critical infrastructure security bill at https://www.itnews.com.au/news/gov-puts-forward-second-critical-infrastructure-security-bill-574071

[8] Unified cyber security task force by March: Source at https://timesofindia.indiatimes.com/india/unified-cyber-security-task-force-by-march-source/articleshow/88379846.cms

[9] IGF 2021 at *https://www.intgovforum.org/en/dashboard/igf-2021*

[10] UN Web TV, *Open-ended working group on security of and in the use of information and communications technologies 2021–2025* – First substantive session, 01:44:03 onwards at https://media.un.org/en/asset/k1l/k1lppp00z1