Post by: Jitesh Balakrishnan

Thanks for sharing the write-up

It is quite interesting to read that the FBI – a principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community has the authority to carry out such a task.

This process, often referred as active defence, seeks to reduce the harm arising from commodity or state-run cyber-attacks by providing services, tools and resources (National Cyber Security Centre, n.d.).

A cyber incident at Lockheed Martin in 2003 exposed evidence of state-sponsored hacking using rootkits to mask their intrusion. As a part of the ‘active defence’ process, the cyber security team laid a trap for the perpetrators by generating honeypots – files with false intelligent information. This investigation albeit unauthorised was able to trace US defence secrets on a server in South Korea (Shackelford et al., 2018).

This was a court-authorised operation to copy and remove malicious web shells from hundreds of vulnerable computers in the United States running on-premises versions of Microsoft Exchange Server software used to provide enterprise-level e-mail service (Department of Justice, 2021). But does this unprecedented intrusion verge on government-sponsored invasion of privacy. Would this set precedence to regulate cybersecurity without the consent of the owners of the targeted computers? Governments across the globe are using the focus on data and national security to push misguided efforts to localize dataand advance cybersecurity or cybercrime laws that are not user-centred, do not keep data secure and effectively open the door to human rights violations (Ben-Hassine, n.d.).

Reference list

Ben-Hassine, W. (n.d.). Government Policy for the Internet Must Be Rights-Based and User-Centred. [online] United Nations. Available at: https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred [Accessed 22 Aug. 2021].

Department of Justice (2021). Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities. [online] www.justice.gov. Available at: https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-exchange [Accessed 22 Aug. 2021].

National Cyber Security Centre (n.d.). Introduction. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/section/active-cyber-defence/introduction#:~:text=Active%20Cyber%20Defence%20(ACD)%20seeks [Accessed 22 Aug. 2021].

Shackelford, S.J., Charoen, D., Waite, T. and Zhang, N. (2018). Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking. SSRN Electronic Journal, 41:2.