International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Cyber Warfare by Chinese Hackers: The AIIMS Story

Dr. Yatu Rani, Sarthak Jain

November 2021, some motivated Chinese hackers targeted Indian seaports. One year later, we see a similar debacle in the shape of the 'AIIMS hacking incident'. Out of the 100 servers at AIIMS - 40 physical and 60 virtual - 5 of the physical servers were allegedly infiltrated by Chinese hackers. On 23rd November, at 7 AM, several servers at AIIMS Delhi were down. Chinese or North Korean hackers were suspected to be behind this attack. All hospital services, including outpatient, in-patient, and laboratories had to be handled manually. 2 of the system analysts at AIIMS were suspended. Indian Computer Emergency Response Team (CERT-In) was invited to take measures to restore the servers back to normal. Data restoration & server cleaning was in progress & was taking time due to the volume of data & the large number of servers for hospital services. National Informatics Centre suspected that this could be a ransom ware attack. Rumour has it that the group of hackers demanded a ransom of 200cr, however, Delhi Police has denied all such claims of ransom. It was suspected that the VIP data stolen from the AIIMS database was being sold on the dark web. Security agencies probing the AIIMS cyber attack approached E&Y executives to examine if they found any vulnerability in the hospital's system when they audited it a few months before the attack. And as if this was not enough, just after 11 days of the initial infiltration at AIIMS servers, another similar cyberattack took place at another very reputable hospital at Safdarjung, Delhi. Although not a ransom ware attack, it was a very serious hacking event due to the presence of crucial VIP data on the Safdarjung database. Although this issue was handled very well by the National agencies, this was still a major failure on the part of the medical institutions and the government authorities as there existed a critical vulnerability in a national-level healthcare organization. The data present in these databases is highly crucial - personal information about the VIPs, and the financial information of the patients; the examples are innumerable. Additionally, the servers once hacked shouldn't have taken so long to get sanitized and restored back to normal. We, a nation in its 76th year of independence, need stronger laws against such cybercrimes and stronger compliance for all healthcare organizations. This also proves to be a crucial learning point for the rest of the national and state-level organizations to have better compliance and a strong cyber defense team.

Keywords: vulnerability, cyber attack, cyber crime, network, ransomeware