OLD DOMINION UNIVERSITY

CYSE 300: INTRODUCTION TO CYBERSECURITY

U.S Communications Breach by Salt Typhoon

George “Trey” Smith

01249099

Last year, a major breach of United States security was uncovered. It is said that they could tap into and monitor incoming and outgoing calls within the state. Official reports say that Chinese hackers named the Salt Typhoon compromised many United States-based telephone providers. Providers such as AT&T, T-Mobile, and Verizon were caught up in this attack and were subject to outsider spying for over a year.

Within this breach, there are multiple different vulnerabilities that the hackers were able to exploit. The Wikipedia page says that the two major vulnerabilities that were exploited were "multiple unpatched network devices" and "weak authentication practices." These are major vulnerabilities that all IT and cybersecurity professionals need to be aware of. Having unpatched systems means that previous malware that is probably widely known can compromise and mess with your systems. Weak authentication practices make it so that people can easily either brute force or gain access to an account without going through multiple steps to get in. Having just a username and password can make a system very vulnerable to the outside due to the weak personal security people have online.

The scale and impact of this attack are major. Sources say that the hackers were able to access something called "CDRs or call record details." (Perper, 2024) CDRs can have information like metadata, date and time, IP addresses from both source and destination, and phone numbers. This information was collected mainly within their target area, which was Washington, D.C., and can presumably be trying to target high-level government officials. Anne Neuberger a national security advisor, said that "the goal of identifying who those phones belong to and if they were government targets of interest... probably less than 100 individuals were targeted for collection." (Perper, 2024)

Lastly, some things that could have been done to prevent this attack are more active security updates and monitoring. Anytime a system doesn't have an up-to-date patch on it, it's like having your door unlocked. Another way they could have prevented this from happening is by enforcing multi-factor authentication. This is, in my opinion, the most effective way to stop a good amount of hackers and bad actors. Something as simple as having a security key plugged in when you log on can stop malicious users from accessing your systems.

Perper, R. (2024, December 27). *Chinese hackers used broad telco access to geolocate millions of Americans and record phone calls - POLITICO*. POLITICO; Politico. https://www.politico.com/news/2024/12/27/chinese-hackers-telco-access-00196082

to, C. (2024, August 27). *2024 cyberattack by China*. Wikipedia.org; Wikimedia Foundation, Inc. https://en.wikipedia.org/wiki/2024_United_States_telecommunications_hack