**Malware**

Name:

Institution:

Course:

Professor:

Date:

**Malware**

Malware is both a weapon and a capability. Malware is a malicious software that attackers use to violate and disrupt other people’ computers or devices. Malware gives an attacker an unauthorized access to use system resources, steal passwords, ask for ransom, and even lock one out their computers. Malware is the main weapon for cyber attackers. Through this malicious software, hackers gain control over their target computers or organizations and access unauthorized data for mainly financial gain (Wangen, 2015). For example, hackers leverage their phishing skills to lure employees into opening and clicking malicious links or emails. Once employees open these links, hackers gain access to valuable organization data and cause damage. It only takes one successful hack, and once an employee unleashes the hidden malware, the entire enterprise become infected.

Malware is also varied in type and capabilities. Cyber attackers use these malware capabilities to gain unauthorized access to systems. Malware offers hackers with remote control to use on an infected computer. They can also use these malicious software to send spam from infected computers to unsuspecting targets. Once they gain access to their target company, malware also gives them the capability to investigate the infected network and steal important data. For example, a botnet malware has the capability to infect a network of computer under a single attacker (Wangen, 2015). These type of malwares are versatile and adaptable able to remain resilient even if servers are redundant.

**Reference**

Wangen, G. (2015). The role of malware in reported Cyber Espionage: A review of the impact and mechanism. *Information*, *6*(2), 183–211. https://doi.org/10.3390/info6020183