MIDN 2/C Coffey, Lewis

Capt Rashley, USMC

Si430

20 February 2025

Crooks

In an ever more technologically integrated society, cybercrime will always be a facet of our digital world. Machines and programs will be vulnerable, and bad actors will look to exploit those vulnerabilities. Modern cybercrime as we know it did not become mainstream until the early 2000s. But even then, those cyber-attacks were far from anything as sophisticated as one would find today. Nowadays, cyber crime comes in a few main forms; Botnets, Malware, and Spam. Botnets are groups of machines that have been hijacked by a bad actor in order to leverage the machine resources for malicious purposes. For instance, if a hacker has access to a botnet consisting of a few thousand machines, they can employ all of those machines to send get requests to a particular website, overwhelming it and putting it offline is a DDoS attack. A famous example of this occurred in 2009, when the Internet Service Provider (ISP) Panix fell victim to a syn flood attack from a botnet consisting of ten million infected machines. Examples like this show how quantity is a quality in it of itself. However, when we think of malware, we tend to think of viruses infecting a computer and potentially locking files in order to ransom them back for money. Modern malware tends to use vulnerabilities in order to execute buffer overflow attacks, bypassing PIE, ALSR, and stack canary security implementations in order to get a program to do something it wasn’t intended to. In the case of malware, that ‘something’ is opening a backdoor or a reverse TCP shell. Spam is also a facet of cyber crime as well. Most of the time, a vulnerability in a digital system arises from the fact that a human is in charge of running and maintaining that system. A simple phishing email can extract a password or other confidential information that would allow a bad actor to gain access. On average, companies spend a total of one billion dollars in a year in spam counter. However, regardless of how hard cyber security professionals try, it is ultimately a game of cat and mouse. Cyber security gets better, vulnerability exploits become more sophisticated, and so on and so forth. All we can do is get as far ahead as we can ahead of the Crooks.