INITIAL ACCESS

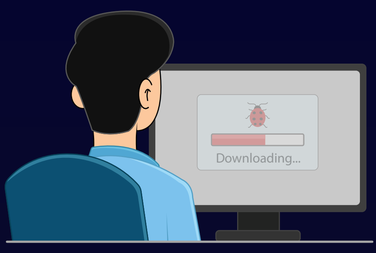
Gaining foothold into the network

Once adversaries like Mr. Gene collect enough information about the target organization, they work on entering the network using techniques such as drive-by downloads, compromise of removable media, phishing, and take advantage of vulnerabilities in public-facing applications and trusted relationships.

1

Entering via drive-by downloads

Mr. Gene can compromise the websites frequented by the target organization's employees to deliver exploit codes to their browser when they surf the sites.



2

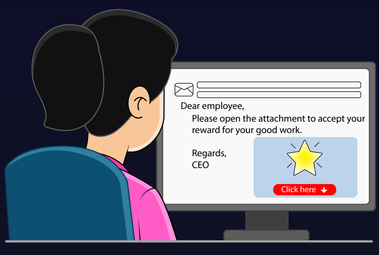
Manipulating public -facing applications

He can make use of vulnerabilities such as bugs and glitches in internet -facing applications and databases to gain access to the organization's network.

3

Phishing

With the email IDs collected in the reconnaissance phase, Mr. Gene can entice employees to open emails containing malicious links and attachments.



4

Infiltrating through removable media

To hack into networks secured by air-gapping measures, Mr. Gene can exploit the autorun features of the target organization's devices, which execute when removable media is inserted.

5

Exploiting trusted relationships

Mr. Gene can bribe third-party providers, such as security-service providers who are trusted users in the target organization, to provide him illicit access to the network.