LATERAL MOVEMENT

Traversing the network

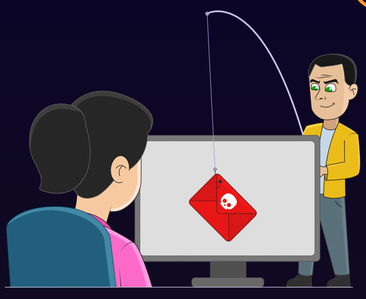
Remaining inconspicuous isn't always enough. Hackers like Mr. Gene have to weasel their way to the critical resource. Lateral movement is the combination of techniques that they use to hop from one entity to the next, moving deeper into the network. Here are five ways adversaries can move laterally through the network.

1

Exploiting vulnerabilities in remote services

Mr. Gene can take advantage of the vulnerabilities spotted in remote services, such as Server Message Block (SMB) and Remote Desktop Protocol (RDP), and move laterally through the network.

2



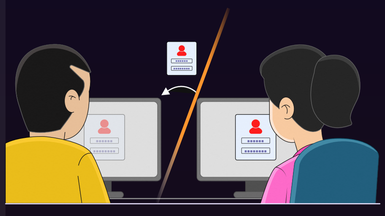
Carrying out internal spear phishing

From a compromised account, he can send emails with malicious attachments to several employees whose email addresses were possibly collected during the reconnaissance phase.

3

Hijacking remote service sessions

When a user logs on to a service with valid credentials, a session is established. Mr. Gene could hijack this session by compromising the agent or the agent's socket to move laterally.



4

Corrupting shared content

Mr. Gene can add a malicious payload to a legitimate shared file in the network. When a user clicks on it, the malicious code executes and infects the system, enabling Mr. Gene to gain remote access.

5

Circumventing conventional authentication

Once an application or user validates their identity using a username and password, alternate authentication materials are generated and stored in the cache. Mr. Gene can steal these materials to bypass normal access controls and gain remote access.