DEFENSE EVASION

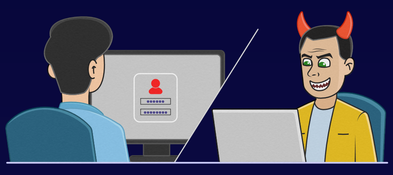
Dodging security controls

After adversaries like Mr. Gene gain entry into an organization's network, they want to remain inconspicuous throughout the course of the attack. Mr. Gene can use various techniques such as exploiting elevation control mechanisms and access tokens, hiding artifacts, and weakening encryption to evade defensive measures.

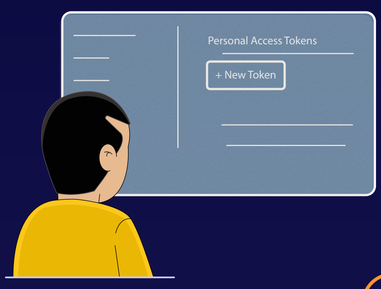
1

Misusing elevation control mechanism

APIs such as "Authorization ExecuteWithPrivileges" can be used to perform operations with root privileges. Mr. Gene can misuse these to prompt users into giving away their credentials.



2



Modifying access tokens

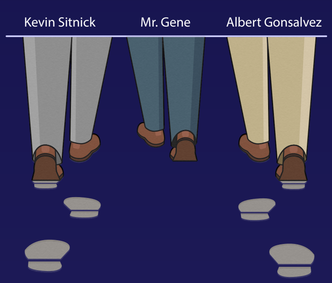
Mr. Gene can duplicate access tokens to bypass access controls and make a malicious process appear as though it's the child process of another legitimate process. This makes it difficult to track any illicit processes in the network.

3

Hiding artifacts

By default, operating systems enable important files to be hidden from users to prevent accidental alteration. Mr. Gene can abuse this feature to hide artifacts associated with malicious behavior and avoid detection.

4



Defusing defense mechanisms

Mr.Gene can disable IT security measures such as firewalls, antivirus solutions, and threat intelligence. He can also tamper with logging policies, disable tracking, and reduce his digital footprint in the network.

5

Weakening encryption

Many network devices use encryption hardware to perform encryption on network traffic. Mr. Gene could disable this hardware to bypass encryption and evade defenses.