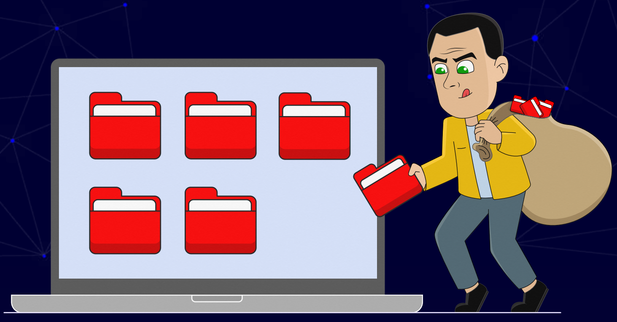
EXFILTRATION



Stealing valuable data

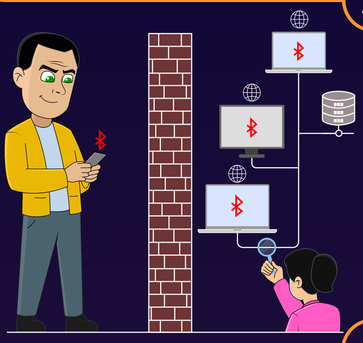
Once adversaries like Mr. Gene gain control over a victim's network, their goal is to exfiltrate critical data. Before exfiltration, adversaries can choose to package data through encryption or compression to evade detection. Here are just five ways adversaries can exfiltrate data.

1

Transferring data to a compromised cloud account

Mr. Gene can gain access to an organization's cloud environment and transfer critical data to a different cloud account to avoid network based exfiltration detection.

2



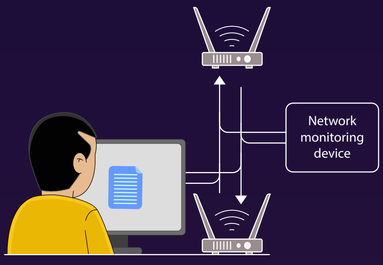
Exfiltrating over other network mediums

Mr. Gene can exfiltrate data through mediums like Bluetooth instead of the organization's command and control channel. This can be a grave challenge if Mr. Gene gets sufficiently physically close to the data.

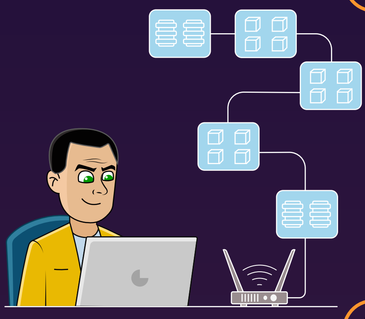
3

Duplicating traffic

After compromising the network, Mr. Gene can use certain network devices' inherent traffic mirroring feature to duplicate and redirect data to a system under his control.



4



Limiting data transfer size

System admins may set alerts to notify them in case of large data transfers. Mr. Gene can exfiltrate data in fixed size chunks instead of whole files, thereby limiting packet sizes to below preset thresholds.

5

Scheduling data transfer

Mr. Gene can schedule data exfiltration to occur at a specific time of the day or at certain time intervals. This can help blend exfiltration traffic patterns with normal data transfer activity.