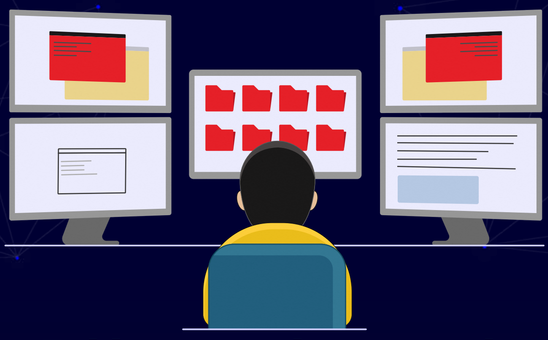
COMMAND AND CONTROL



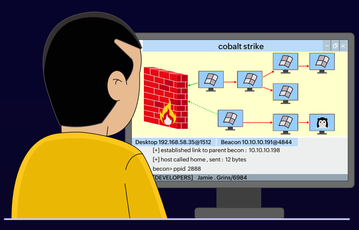
Taking over the network

Adversaries like Mr. Gene try to gain control over compromised systems by communicating with them. Command and control includes the various techniques they use to establish dominance over the target network discretely. Here are five ways in which Command and Control can be established.

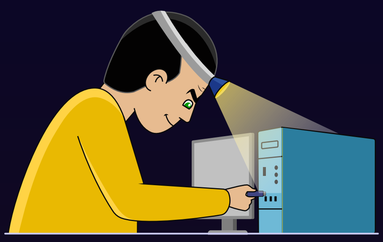
1

Manipulating application layer protocols

Mr. Gene can discretely control a compromised computer remotely by communicating with application layer protocols. He can insert malicious commands within existing protocol traffic to avoid suspicion.



2



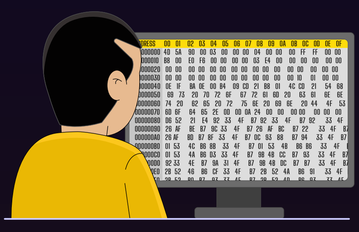
Gaining control through removable media

Mr. Gene can gain control of air-gapped host systems by using removable media (such as USB). Mr. Gene can relay commands from one system to another through the removable media.

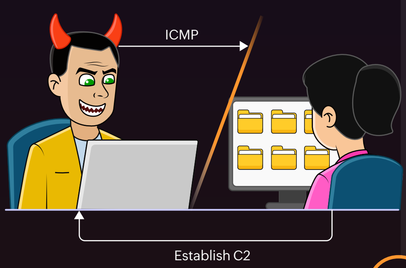
3

Obfuscating data

In order to control compromised devices inconspicuously, Mr. Gene can use tools like FlawedAmmyy, which can obfuscate parts of the initial command and control handshake, to prevent detection.



4



Manipulating non-application layer protocols

Mr. Gene can communicate between the victim device and the Command and Control server using non-application layer protocols such as Internet Control Message Protocol (ICMP), as they are not commonly monitored, and can be used to conceal communication.

5

Misusing remote access software

Mr. Gene can use legitimate remote access and desktop support tools such as AmmyyAdmin and TeamViewer to establish interactive command over devices in the victim network.