Exploitation of security vulnerabilities

*Malicious cyber activity varies; the diagram below is one example of how cyber actors can exploit vulnerabilities and gain access to devices and systems. As patching vulnerable software or devices may not always remove a malicious actor from an already compromised network or system, further investigation may be required to identify malicious activity.*

A security vulnerability within a device or software application is discovered and publicly reported. Note: Exploit code may already be in use by some actors taking advantage of the vulnerability prior to the public announcement.

The vendor usually releases an update or patch to resolve the vulnerability, encouraging users to implement the patch on systems, devices, or software.

Cyber actors create exploits to target security vulnerabilities in unpatched systems, devices, or software.

The cyber actor may directly target vulnerable servers to access systems.

Exploits may drop malware onto vulnerable systems OR allow cyber actors remote access into a network.

Exploits may also be delivered via:
- Attachments to email messages
- Compromised websites
- Social networking sites

Unsuspecting users are lured into executing the exploit through social engineering techniques.