Anti-malware Software in Protecting Endpoints

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**Anti-malware Software in Protecting Endpoints**

Anti-malware software works to detect infections. Anti-malware packages provide several abilities that should be considered when designing a defensive strategy:

* Whistling capabilities (Anomaly-based detection) allow only trusted software to run, and application whitelisting checks to ensure that the software running matches a known good version of the software (a good baseline is needed for this technique).
* Heuristicic or behavior-based anti-malware capabilities look at behavior associated with attackers (unexpected data transfer, scan of other systems, or access to memory or data that is typical).
* Signature-based systems attempt to gather fingerprints of known malware and then compare files and applications with those fingerprints.

Anti-malware technologies can be deployed on networks and on systems and devices. However, modern threats have shown that they can make themselves unable to detect. Using the technology to detect malware, advanced persistent threats (APT) can exploit the detection of anti-malware.

References

Chapple, M., & Seidl, D. (2023). Chapter 11: Protecting Endpoints in *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 9–20). essay, Jones & Bartlett Learning. (1)