Reactive Measures: Blocking File-Based Artifacts

Malicious attachments have the potential to be extremely damaging to an organization and its systems. From viruses to ransomware, backdoors to keyloggers, it is important to take strong defensive measures when these artifacts are present in a phishing attack. There are two standard types of blocks we can take when defending against malicious files;

- MD5, SHA1, or SHA256 hash blocking
- File name blocking

FILE HASHES

We can block the MD5, SHA1, or SHA256 hash within the organization's endpoint detection and response (EDR) tool. This means whenever the hash becomes present on a protected endpoint, the software will recognize and delete it immediately before it is able to run. Unless the phishing attack is using different files (and therefore different hashes, although this is unlikely) then simply blocking the file hash will defend against that specific email attachment. If the organization's anti-virus (AV) solution isn't flagging the malicious file, the hash can usually be submitted to the vendor, who will add the hash to their AV's detection list if they deem it appropriate, helping to protect all other customers of that product. Commodity malware (frequently sold online) and more advanced polymorphic malware can edit itself, or simply write trash data to its code, altering the file hash and rendering hash blocks ineffective. Due to hash collisions, MD5 and SHA1 have been widely deprecated, and SHA256 is the current standard for file hashing.

FILE NAMES

This is typically not a good idea, unless the file has an extremely unique file name. For example, if the file was named "Budget FINAL March 2019.xls" we could have an issue with blocking it based on its name, as this ***could*** be used legitimately within the business, and we don't want to delete legitimate files. If the file was named "INVOICE #8491 READ NOW URGENT" then this would be less likely to be used legitimate, due to the specific numbering (#8491) and the text trying to create a sense of urgency. File name blocks are rarely used, and can instead be used to generate watchlists, a set of IOCs/artifacts that are monitored, and when detected are alerted to analysts to investigate further. In almost every circumstance of a malicious file, file hashes will be used to block them.

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

investigate further. In almost every circumstance of a malicious file, file hashes will be used to block them.

‹ Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic ›