A recent addition to Apple's malware detection technologies which the company has not publicly documented yet goes by the name of XProtectBehaviorService. Apple refers to this as a "hidden behavioral detection", and the functionality is accessible through the command /usr/libexec/syspolicyd. It pokes and prods at applications on the system for signs of suspicious behavior. It is activated by the eslogger component of XProtect, which logs details of applications that violate certain pre-programmed behavioral rules, currently defined in /var/protected/xprotect/XPdb.

For enterprises, the inability to receive alerts and the difficulty of inspecting logs means there is little chance of catching infections missed by the default remediation options at the user's disposal. The tool will neither warn of nor log suspicious or malicious activity, and relies on a silent remediation to fix threats when they are caught. Remediation involves the removal of problematic files and the automatic reinstallation of the app from the App Store.

This is a high-risk strategy for both enterprises and Apple. A risk of a false positive in this situation could cause users to lose access to legitimate software, even if they have the password to activate the app due to a potential system policy settings which prevents activation using a password. Similarly, the tool will neither warn of nor log suspicious or malicious activity, and relies on a silent remediation to fix threats when they are caught. This can lead to a false sense of security and complacency.

Unfortunately, Apple’s approach to silent remediation does not provide any transparency to the administrators or users. While successful removals are logged, the user or administrator does not have access to these logs, which are stored on the user's local device. This is problematic for enterprises that need to collect evidence in case of a security breach.

Despite the lack of user interfaces for understanding what malware has been remediated, when, or how it was introduced, enterprises still want to gain visibility and control over their devices. Therefore, they need to look for additional endpoint protection on their macOS devices.

Apple's approach to security is, like many other things it does, different to other OS vendors. That's neither a good thing nor a bad thing in itself. While Apple's primary focus is to provide the most seamless and uninterrupted experience for their users, enterprises need to take steps to robustly defend their systems. For enterprises, the inability to receive alerts and the difficulty of inspecting logs means there is little chance of catching infections missed by the default remediation options at the user's disposal. The tool will neither warn of nor log suspicious or malicious activity, and relies on a silent remediation to fix threats when they are caught.

Relying on silent remediation is a high-risk strategy for both enterprises and Apple. A risk of a false positive in this situation could cause users to lose access to legitimate software, even if they have the password to activate the app due to a potential system policy settings which prevents activation using a password. Similarly, the tool will neither warn of nor log suspicious or malicious activity, and relies on a silent remediation to fix threats when they are caught. This can lead to a false sense of security and complacency.

Conclusion

In summary, while Apple's approach to silent remediation provides an easy way to remove malware from their Macs, it does not provide the transparency and visibility that enterprises need. A lack of user interface for understanding what malware has been remediated, when, or how it was introduced into the system. However, as of the last update, Apple had 6 hours to remediate the malware which was neither blocked by XProtect nor removed by XProtectRemediator. Despite the lack of updates to Apple's primary malware blocking tool, the company has been updating its other technologies, such as notarisation and Gatekeeper, which contain these YARA signatures, a tool used to conduct signature-based detection of malware, which Apple updates regularly.