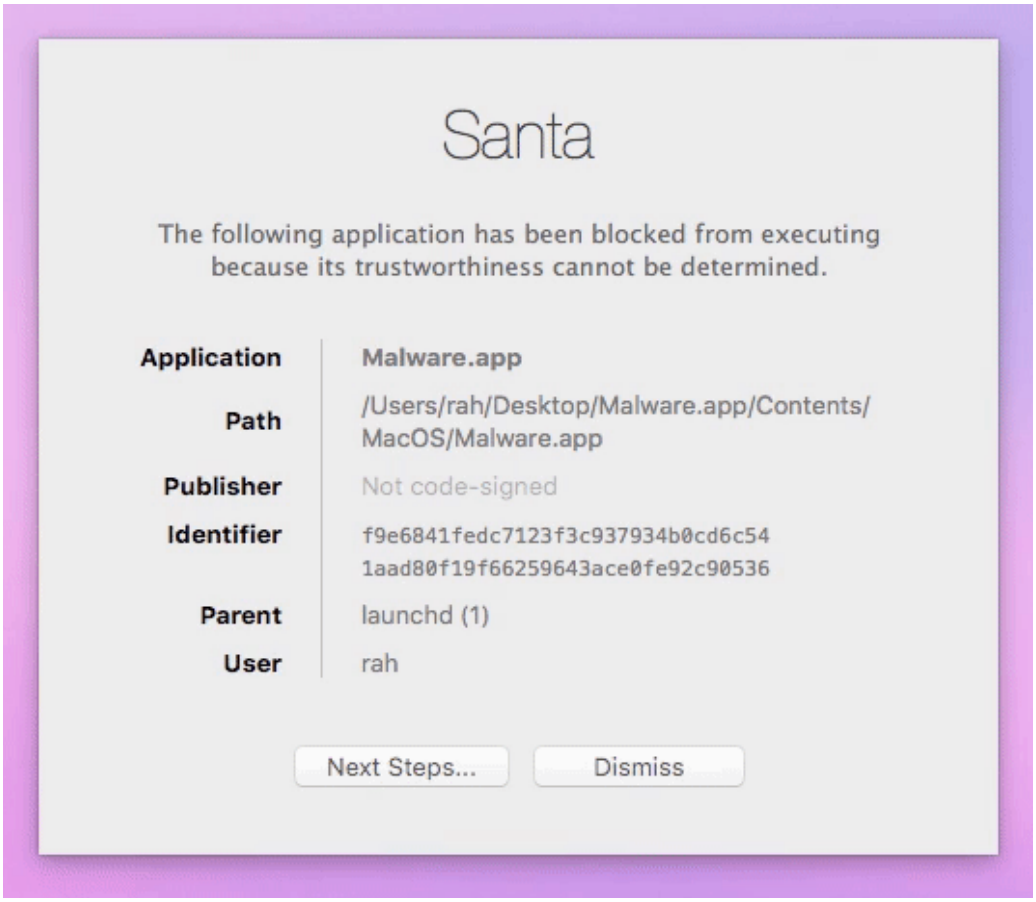
Santa Application Whitelisting/Blacklisting for macOS, Security Whitepaper



Prepared by Allister Banks. Last Updated August, 2016

Background

This whitepaper describes how Google's Santa, a binary whitelisting/blacklisting system in active deployment on Github, protects macOS from malware, ransomware, and other unwanted applications. It is in 'lockdown' mode on thousands of computers worldwide, and used by many organizations in lieu of other products that can't guarantee as high a success rate and low system impact.

Executive Summary

The majority of antivirus and anti-malware systems that commercial vendors offer are an afterthought on macOS, burdened by poor performance and slow or non-existent detection. As of macOS 10.6, Apple bundles a system with the marketing name XProtect, which uses loose criteria to know an infection is present. It also relies on being paired with their Gatekeeper quarantine and application restriction feature so launching an unsigned application presents a warning to the user, but Apple's judgement can still overridden in many cases. The better model that Santa uses is to only whitelist apps that have registered developer certificates with Apple, while also being able to use the specific sha256 fingerprint of the app to deny its use if found to be malicious. This allows you to be certain only trusted applications are in use, and the user will be prompted if anything else runs without your permission or knowledge, obviating the need for antivirus while being more effective in its mission.

Client Features and Operation

Santa consists of three main parts: a kernel extension (driver), the user-facing 'block' GUI (and associated userland daemon), and the command line santactl tool for management. We'll only be going over server-less operation, but the public release of Google's server component is anticipated.

Kernel

In order to efficiently intercept application or compiled binary launches, a signed kernel extension is provided with each stable release. It takes advantage of this prioritized position to perform some other checks on binaries, uses robust API's and caching to ensure low-impact operation, and even includes file integrity monitoring. This requires privileged access to 'stream' events and filter them against its rules engine.

Santa.app

As pictured on the first page, when an application matching a block rule is launched, the Santa app displays information about why the operation has been denied. This includes messages customizable per rule or globally, and can show information like the developer certificate used to sign the app. This works at the command line as well, if an attacker was trying to be tricky by opening a Terminal window for a moment to perform some other action.

santactl

santactl's primary tasks are on-demand syncing with a server, gathering information on binaries, and interacting with the rules database. As is the case when the kernel extension performs duties outside of normal unknown app blacklisting, it can also help identify DMGs by collecting metadata about their source, in addition to generating what is slated to be a portable config format for exporting/importing rule criteria.

Complimentary Products & Compliance

osquery can gather logged data from Santa for aggregation, and covers many other inventory-specific tasks that a host intrusion detection system would need. One of the tables of data the community has contributed is a logging parser for Santa's logs, so that even when rules allow an application launch, the metrics can be captured with one tool. Zentral is a server component that provides a way to push blacklists to Santa, and supports osquery as well.

Compliance

PCI-DSS 5.1 and 5.1.1[1] warns that "It is important to protect against ALL types and forms of malicious software", but only requires detection and removal of known executables. Santa takes this one step further by only ALLOWING 'known-good' software to run, and ensures that patches or new macOS version do not need to be held back because a vendor's solution hasn't been updated. Often patches are only available for the most current macOS, making this even more critical.

Anecdotally, government employees have been required to have antivirus installed in order to use e.g. VPN software, to the detriment of system resources and sometimes resulting in downtime as false positives harm productivity. Of the NIST guidelines, both AT-2 and SI-3[2] call out controls against malware, which Santa is more than capable at containing.

As per HIPAA Administrative Simplification 164.312 and 164.306[3], and in response to incidents worldwide where protected health information is jeopardized by ransomware, stopping malicious applications from launching is a strong control to put in place. It especially helps as data in transit is often not backed up and can be exposed to access by rogue processes from unauthorized parties.

Conclusion

Once you've gathered information about software in your environment, which often can be satisfied by approving the certificate of only a small collection of vendors, IT can be confident that nothing you haven't approved will run on the workstations in your fleet. Santa ensures things that would harm data safety or customers privacy don't get a chance to occur, and provides a user-facing way to educate end users when something malicious tries to jump the fence, making them more vigilant about behavior as well.

---

[1] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

[2] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[3] http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf