F-Secure DNS Integration Project Proposal

Vince Rosas

Southern New Hampshire University

Table of Contents

Problem Statement

F-Secure Corporation, founded in 1988 and was initially created to provide training and consulting services (Austin, Lyytinen, Penttinen, Saarinen, & Applegate, 2009). Shortly after the company was created, a grad student from Cornell University, Robert Morris Jr, created a worm program that exceeded his own expectations. This worm caused havoc in systems all over the world and caused damages of up to $53,000 USD per site infected (Austin, Lyytinen, Penttinen, Saarinen, & Applegate, 2009). This helped propel security software companies to the forefront. F-Secure, then called “Data Fellows” began adding security products a few years later as the threat of viruses grew. 30 years later, the threats faced by computer users are much more advanced than simple viruses and worms. Often, threats come from users clicking on malicious links than file attachments. Some companies will counter this by blocking all internet access except explicitly allowed sites. This can be time consuming and difficult and can cause problems when users need to access sites that are not already allowed. On top of this, this solution only works when on internal networks. To combat this, F-Secure can offer a custom Domain Name System, or DNS, to protect clients and customers. The custom DNS would be maintained by F-Secure and regularly updated to block known malicious websites. This helps on multiple levels since blocking traffic to known malicious websites, it will prevent connections for remote access trojans, botnets, and website spoofing.

Significance

By adding this service to F-Secure’s portfolio, it will greatly increase the security of any device protected by F-Secure software. For desktop and laptop computers, this helps mitigate the threats from phishing attacks as well as reduce the damage done should an infection get passed the antivirus scanner undetected. Definition and heuristic based scanners may still let viruses

through if it is a new virus and there are no definitions or has new behaviors that have not been identified by heuristic engines. It adds another layer of protection and one that is harder for malicious actors to circumvent. Future versions of the service could use a DNS address that can be added to home or business routers, further expanding the devices protected by the new service. This way, instead of protecting only Windows, macOS, Android, Linux, or iOS, all devices can be protected including printers, scanners, managed switches, cameras, and even IoT devices such as access control, smart speakers, and streaming devices. Many of these simpler devices, such as Amazon Fire TV or Apple TV boxes are running versions of Android or iOS and are vulnerable to much of the same malware that affects the phones. Even printers have a basic webserver that hosts the device's web interface and can therefore be compromised. Once F-Secure is managing the DNS of its users' network-wide, this will enable even more opportunities such as ad blocking and DNS-over-HTTPS further enhancing the security and privacy of its end users.

Objectives

The objective of this project is to add a custom DNS protection service F-Secure's software platform, including Windows, macOS, mobile operating systems, and network-wide. The goal is to allow F-Secure to offer a tiered add-on service to customers directly, making them less reliant on the ISP channel for revenue. Due to the complexities of mobile app development and setting up network-wide DNS filtering, the scope of the project will be limited to Windows and macOS clients.

Deliverables

The final deliverable of the project will be the addition of a custom DNS protection service to the existing F-Secure software platform. Initially this will only be for Windows and

macOS devices but will be added to mobile apps at a later date. This will also require creating, maintaining, and regularly updating a database of known malicious websites that end users can rely on to protect their computers and mobile devices.

Methodology

This project will utilize the waterfall methodology. This method focuses heavily on gathering requirements and following a linear path (Project Manager, n.d.). This method requires each phase be completed before the next one is started, and each phase has specific deliverables that must be signed off on before continuing. The phases in the Waterfall method are: Requirements, Design, Implementation, Verification, and Maintenance (Project Manager, n.d.). Gathering accurate requirements is most important as all future phases are based on this. The initial version will require integration into the current F-Secure software platform. Each phase in the process will be tracked through Gantt charts and submission of deliverables at the end of each phase.

Risks

The risks associated with this project are alienating existing ISP partners by offering the service directly to consumers as an upgrade. This could be alleviated in the future by allowing ISPs to have their ad services whitelisted once network-wide DNS protection is available. Another risk with this project is not properly maintaining the threat database to ensure the protection of the end users. Alternatively, a legitimate website may be added to the database and be blocked accidentally.

References

Austin, R. D., Lyytinen, K., Penttinen, E., Saarinen, T., & Applegate, L. M. (2009, February 26). F-Secure Corporation: Software as a Service (SaaS). *Harvard Business Review*, p. 22.

Project Manager. (n.d.). *Waterfall Methodology - Tools and Strategies*. Retrieved from Project Manager: https://www.projectmanager.com/software/use-cases/waterfall-methodology