Protecting a Major UK Financial Institution from Zero Day and Undetectable Threats with Content Threat Removal for Web Gateways

DEEP SECURE

Background

This major UK financial institution needed to balance the needs for user productivity and instant access to information with the requirement to repel cyberattacks from those intent on compromising its systems.

Over 4000 users within the organisation required access to a range of critical internal systems, as well as needing rapid access to information downloaded from the Web.

In this highly regulated environment, the organisation employed a wide range of cyber security controls and policies but inevitably was a prime target for cyber criminals.

The risk of compromise via a zero day or even a completely undetectable exploit concealed in seemingly harmless digital content, downloaded from the Web was ever-present.

Challenge

Eliminate the zero-day threat from Web-borne content while enhancing user productivity

Users at the financial institution accessed the Web via a McAfee Web Gateway which enforced a range of security controls including detection-based anti-virus, user authentication, acceptable usage policies and URL filtering, amongst other features.

To combat the risk posed by malware concealed in business documents and downloaded via the Web, the organisation had deployed a leading sandboxing solution and downloads were sent to the sandbox for checking before being delivered to the user.

"We knew that zero-day and undetectable attacks could be concealed in everyday documents and images and downloaded via the Web."

There were two drawbacks to this approach. The sandboxing solution was not always effective and sometimes potentially malicious content concealed in documents was allowed into the network.

A much more significant concern was the impact the sandbox was having on user productivity. It could take up to 15 minutes from the user clicking on a link to download a document, and them receiving it from the sandbox.

"The challenge was to balance the need for users to get rapid access to business content, with the absolute imperative that the content should be totally threat-free."

Solution

Deploying Deep Secure Content Threat Removal for Web Gateways with the McAfee Web Gateway

Instead of relying on the sandbox, the organisation installed Deep Secure Content Threat Removal for Web Gateways alongside its McAfee Web Gateway.

The Web Gateway operates as before but now it passes digital content – Office documents, PDFs, and images to Content Threat Removal for Web Gateways. Using a unique process called content transformation, the valid business content is extracted from the downloaded document or image, the original is discarded, and a brand-new document or image is created and handed back to the Web Gateway for onward delivery to the user.

This approach maximises security. Every file that is transformed is guaranteed 100% threat-free of even zero day or undetectable threats such as those concealed in images using steganography.

The entire process from requesting a download to receiving the document on the desktop takes milliseconds and therefore far from adding latency into business processes it has accelerated workflows and enhanced productivity.

"Office documents, PDFs and images allowed in over the Web are processed by Content Threat Removal for Web Gateways, to ensure they are completely threat-free."

Results

Open downloaded content without fear of compromise

Despite extensive penetration testing, the financial institution's experts have been unable to find a way to beat the protection provided by Deep Secure Content Threat Removal and the solution is now live across the organisation.

The content transformation process is totally transparent to the organisation's users who receive business content that is fully revisable and pixel perfect. Users can now access digital content over the Web without delay, and open downloaded content without fear of compromise.

Having started with Content Threat Removal for Web Gateways the organisation is now looking to extend this concept into other use cases, ensuring all business documents are threat free across different communication flows including file transfer, web services and email.