Forcepoint

Technical Report

File Content Sanitization For Thwarting Malware

Introduction

We're all increasingly dependent on the internet to do our jobs, to educate our children, to run businesses, and even to help with our health care. That's why modern cyberattacks increasingly target users through web browsers. Hackers are using techniques like embedding malicious URLs within files and other content on "good" domains to circumvent web security infrastructure.

While site attacks can't be predicted, there are ways to contain the damage by isolating end-user internet browsing sessions from endpoints and networks—called remote browser isolation (RBI). This safeguards user access from anywhere to web and cloud services, prevents malicious cloud and web-borne threats, and protects critical data and IP to eliminate security gaps. RBI helps dramatically decrease zero-day exploits and phishing threats to endpoints and networks. Forcepoint RBI integrates with Forcepoint Web Security and Network Security products to offer the ultimate layer of defense for web browsing. By integrating with Forcepoint Web Security and Forcepoint NGFW, traffic from trusted clients to clean websites is allowed to take a direct route, while more potentially risky traffic is routed through the strongest malware defenses available. This means IT teams can worry less and users can always access any websites they need, even compromised ones, without putting the network in danger.

With RBI, URLs can also be rendered in read-only mode to prevent credential phishing, and data-sharing activities on websites. And C-level executives, IT admins, and others who are frequently targeted by cybercriminals? They can have all their web traffic isolated to provide the highest degree of web security.

Malware Downloads

Phishing and ransomware attacks have rapidly expanded since the start of the pandemic. Phishing attacks are designed to deliver malware (ransomware, data theft, etc.), while some are designed to harvest credentials to enable system access. The problems continue despite increased investments in training and technology and significant time and effort spent by security teams responding to incidents.

All of this underscores a need for advanced capabilities like Content Disarm and Reconstruction (CDR) technology. It can easily sanitize files as they are downloaded to better protect the end users. CDR ensures that any files downloaded from the web are clean and safe to use, neutralizing one of the worst threats to businesses today—phishing campaigns that try to convince users to open infected attachments. Only the clean file is delivered, with any potentially malicious code removed. In conjunction with RBI, CDR provides comprehensive malware protection for both web browsing activities and file downloads.

CDR File Sanitization Process:

1. Identify the incoming file type e.g. image file, Word document, etc. and break the file down into its elements

2. Identify and remove any file elements that do not comply with file type specifications

3. Build a new, clean file with the remaining content

Original saved for backup

4. Deliver the clean file to the user

Benefits of CDR?

- → Prevent malicious code, even zero-day threats
- → No impact on user experience and productivity
- → Can be applied to a variety of file formats (e.g., images, pdfs, audio/video file formats, archives, html, and office documents)
- → RBI and CDR together can drastically reduce an organizations attack surface

forcepoint.com/contact

[File-Content Sanitization RBI Technical Report] 21Dec2021