Technical Brief

Browser Network Attack Methods

You see a browser. They see a door.

Browsers have taken workforce convenience, insight, and productivity to previously unimaginable levels. Unfortunately, they have also provided these same benefits to thieves. Every browser window becomes a new front door to your organization as unsuspecting users face the potential of interacting with malicious payloads all day, every day. These workers simply aren't as security-savvy as IT staff, yet they are forced to make decisions on how they interact with browser-based and -delivered content. But, knowledge is half the battle. By understanding how attackers think, you can improve your security posture.

McAfee® Labs reported 82,000,000 new suspect URLs in 2014—an 87% increase over the previous year.

Understanding Browser Attack Methods

Data thieves use the latest browser caching and scripting capabilities to mask and automate their malicious behavior. Typically, the intended target of their attacks is the treasure trove of intellectual property stored with the well-meaning web and email users. The bad guys know the browser is a new type DMZ and are banking on the fact that direct contact with their malicious web content will pay off.

Browser caching and JavaScript in PDFs and web forms serve business needs by not only improving usability and productivity, but also by automating processes using dynamic action triggers and remote data retrieval. JavaScript can also enforce conditional formatting, such as addresses and phone numbers, as well as auto-populating those fields. Attackers leverage these processes to mask attacks and malicious payloads. Broad support of JavaScript allows attackers to use one script to create multiple-platform payloads contained in popular file formats, such as PDF and Flash. Less time spent coding affords attackers more time to innovate and create new attacks. What's needed is an intelligent way to inspect PDFs and hidden scripts to determine whether there is criminal intent lurking within these downloads or email attachments.

Beyond Signatures: Raising Security Intelligence with Real-Time Inspection

Thieves are becoming more creative at modifying exploits that traditionally have been caught with signature-based detection. Today's security systems must be capable of efficiently determining the legitimacy of an unknown executable even if its signature has never been seen before. This requires signature-less detection capabilities that work together to block attacks at the web browser—before they take hold on endpoints and spread to other network resources.

intel Security

Intel Security offers several inspection technologies that perform rapid, lightweight inspection of web-delivered content to eliminate browser vulnerabilities and protect users.

These signature-less technologies include:

- Web content and URL filtering.
- Real-time deep file inspection.
- Real-time emulation.
- Advanced Adobe Flash inspection.

Web content and URL filtering
You can find anything you want on the web—and everything you don't. Intel Security's web- and content-filtering capabilities help keep users safe from the dark corners of the web using global intelligence to categorize web threats based on the reputation of web documents and URLs. This first line of defense helps protect users from themselves as they unknowingly click on malicious URLs or download malware-laden documents.

Deep file analysis
This next layer of protection allows security devices to perform deep analysis of inbound web content by understanding scripting behavior hidden inside a file.

PDF/JavaScript inspection
This real-time inspection engine provides deep file analysis with JavaScript detection to find and stop threats concealed in embedded scripts in PDFs. This is the first of many defenses in a multitier array of non-signature malware analytics from Intel Security. It uses a streamlined JavaScript environment to emulate script execution and predict runtime behavior. Files containing malicious scripts are blocked immediately and at all further appearances. By understanding and only blocking scripts with bad intent, businesses can continue to leverage the rich scripting flexibility within their existing PDF documents. Deep file inspection provides a zero-latency alternative to all-or-nothing script blocking and is far more cost-effective than routing all unknown files to a sandbox.

Advanced Adobe Flash inspection
Adobe Flash provides the ability to embed scripting, which is a favorite tool of hackers. By allowing a delivery mechanism (Flash) and remote action (scripting), hackers instruct the endpoint to access other downloadable payloads or exploit endpoint environments. Advanced Adobe Flash inspection is a lightweight inspection engine that uses heuristics to analyze the behavior and structure of Flash code (.swf, .cwf, .zwf). It detects various Flash exploitation techniques, such as vector spraying, presence of shell code, and similar methods and then determines the intent of browser-delivered Adobe Flash content before malicious payloads can be delivered to endpoints. In addition, Advanced Adobe Flash inspection also scans and detects malicious Flash files embedded within PDF files.

Real-time emulation simulates browser environments

Intel Security's real-time emulation engine allows immediate insight into all inbound web content via the browser and protects users during web sessions. It emulates a browser's working environment to study the behavior of incoming files and scripts. These emulators simulate code execution, provide hooks for malicious processes, and predict the resulting behaviors. In addition, intelligent heuristic analytics apply rules and pattern analysis to identify similarities between a suspect file and related groups of known threats. By sitting inline and working in real-time, this engine significantly minimizes the real-world effects caused when a user interacts with malicious web content.

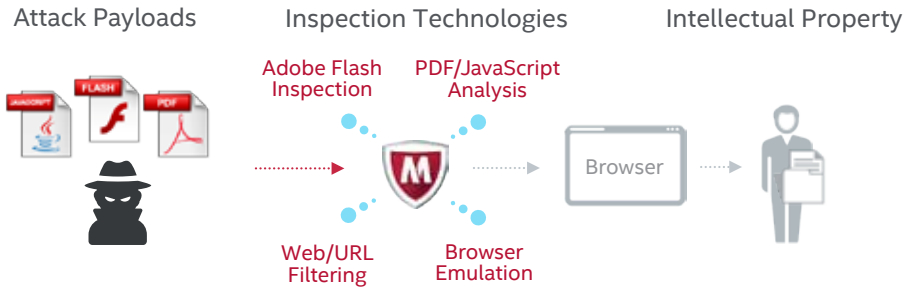

Figure 1. Browsers place users on the frontlines of the new DMZ, as workers directly interact with PDFs, Flash-enabled content, and embedded JavaScript code that can trigger malicious actions. Intel Security offers cutting-edge, signature-less inspection capabilities to detect and deter hidden browser attacks.

Learn More

Web browsers are a valuable productivity tool. However, without proper protection, they can quickly become a liability rather than an asset. Intel Security believes that getting inside the heads of thieves can help keep them from getting inside your network. That's why we have created *Dissecting the Top Five Network Attack Methods: A Thief's Perspective*. This insightful report uncovers the most common strategies and methods cybercriminals use to attack your network. In addition, it discusses how to effectively combat these attacks and protect your enterprise. Download it today at **www.mcafee.com/thiefs-perspective**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com