DIGGING DEEP INTO THE FLASH SANDBOXES

Paul Sabanal
IBM X-Force Advanced Research
tsabanpm[at]ph.ibm.com, pv.sabanal[at]gmail.com
@polsab

Mark Vincent Yason
IBM X-Force Advanced Research
yasonmg[at]ph.ibm.com
@MarkYason

ABSTRACT

Lately we have seen how sandboxing technology is positively altering the software security landscape. From the Chrome browser, to Adobe Reader, to Mac and iOS applications, sandboxing has become one of the main exploit mitigation technologies that software has come to rely on. As with all critical security technologies, they need to be understood and scrutinized, mainly to see how effective they are, or at the very least, to satisfy one's curiosity. The sandbox implementations for Adobe's Flash Player certainly piqued ours.

Our talk will explore the internals of three sandbox implementations for Flash: Protected Mode Flash for Chrome, Protected Mode Flash for Firefox, and Pepper Flash. And of course, we will show that an exhaustive exploration of the Flash sandboxes will eventually yield gold as we discuss and demonstrate some Flash sandbox escape vulnerabilities we found along the way.

We start with a look at the high level architecture of each sandbox implementation. Here we will define the role of each process and the connections between them. In the second part, we will dive deep into the internal sandbox mechanisms at work such as the sandbox restrictions, the different IPC protocols in use, the services exposed by higher-privileged processes, and more. In the third part of our talk we will take a look at each sandbox's security and talk about the current limitations and weaknesses of each implementation. We will then discuss possible avenues to achieve a sandbox bypass or escape. Throughout all this we will be pointing out the various differences between these implementations.

1. CONTENTS

2. INTRODUCTION

During Black Hat USA last year, we gave a talk about Adobe Reader X's sandbox. In that talk we covered the sandbox implementation of one of the primary exploitation vectors used by malware. We also noted that ever since the Reader X sandbox's introduction there has been a remarkable decrease in PDF exploits released in the wild, and thankfully, this remains true up to this time. This year, we focus our sights on another popular exploitation vector - Adobe's Flash Player, and this time, we have three implementations of the sandbox to play with.

In doing this research, we asked ourselves the same things we did last year. What are the security implications with this new technology and what other things can an attacker do in spite of the restrictions imposed by the sandbox? What can still be done within these limits that, from an attacker's perspective, would still bring profit, or from a user's perspective, should be watched out for? Since we are investigating three different Flash sandbox implementations, we also asked ourselves how these implementations differ from each other.

To answer these questions, we dived deeply into the internals of the three Flash sandbox implementations. This paper documents our findings and discusses the internal mechanisms, limitations, and potential escape avenues for each sandbox implementation. We will also provide our thoughts and recommendations on the matter of sandbox security.

3. THE TARGETS

In this paper, we will discuss three different implementations of the Flash Player Sandbox. The targets are:

1. Flash Player Protected Mode For Firefox
2. Flash Player Protected Mode For Chrome
3. Flash Player Protected Mode For Chrome Pepper

Throughout this paper we will refer to them as Firefox Flash, Chrome Flash, and Pepper Flash, respectively.

Firefox Flash, an NPAPI [1] plugin, was first released as a beta on February 2012, and was officially released in June 2012. It is developed by Adobe in collaboration with Mozilla. It is based on the sandboxing code in Adobe Reader X, which we covered in our talk and paper [2] at Black Hat USA last year. Hence, there will be a lot of similarities between them. We will be using version 11.3.300.257 in this paper.

Chrome Flash, also an NPAPI plugin, has been around since December 2010 and is a result of collaboration between Adobe and Google. It is the default Flash player in Chrome. We will be using the version bundled with Chrome 20.0.1132.47 in this paper.

Pepper Flash is an implementation of Flash player using Google's Pepper Plugin API (PPAPI) [3]. It can be enabled through Chrome > Settings > Privacy > Content Settings > Plugins. The version covered in this paper is bundled with Chrome 20.0.1132.47 and is an experimental version. At the time of writing, Chrome Beta 21 has been released which includes Pepper Flash as the default Flash Player.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.