Hacker Intelligence Initiative, Monthly Trend Report #1

Hacker Intelligence Summary Report – Remote File Inclusion

We begin our first report by describing an attack which usually flies under the radar – Remote File Inclusion (RFI). Although these attacks have the potential to cause as much damage as the more popular SQL Injection and Cross-Site Scripting (XSS) attacks, they are not widely discussed.

HII has documented examples of automated attack campaigns launched in the wild. This report pinpoints their common traits and techniques, as well as the role blacklisting can play in mitigating them.

What is a "Remote File Inclusion" Vulnerability?

RFI is caused by insufficient validation of user input provided as parameters to a Web application. Parameters that are vulnerable to remote file inclusion enable an attacker to include code from a remotely hosted file in a script executed on the application's server. Since the attacker's code is thus executed on the Web server it might be used for temporary data theft or manipulation, or for a long term takeover of the vulnerable server.

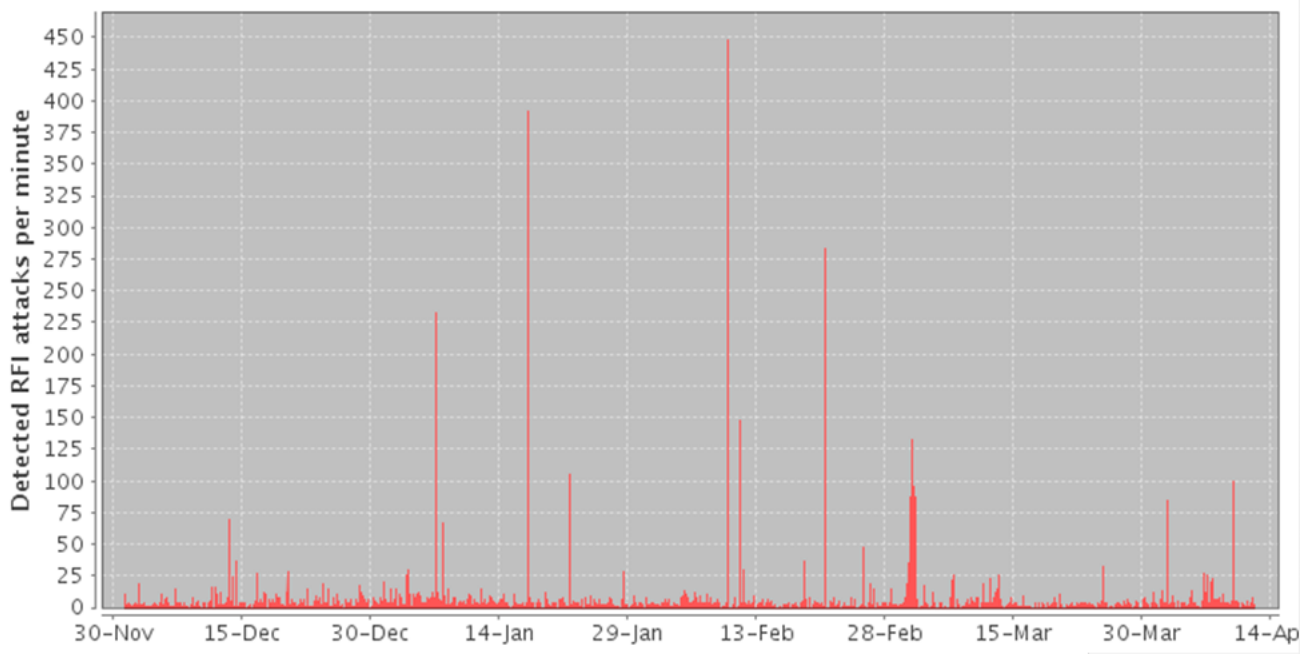
Current solutions such as Web Application Firewalls (WAF) deal with this threat and block the exploit using signatures that match the abused vulnerable application parameter. However, knowledge extracted from observed attacks would improve and enhance this solution.

Remote File Inclusion – an Anatomy of an Exploit

The RFI attack vector includes a URL reference to the remotely hosted code. Most attacks include two steps. In the first step the attack vector references a simple validation script, usually capable of printing some distinguished output to the HTML page. If the validation script is successfully executed by the server under attack then the attacker proceeds with a second vector that references the actual payload script. The servers hosting the scripts are either compromised servers or file sharing services.

Remote File Inclusion – Attack Frequency and Volume

As the following diagram shows, RFI attacks occur on a daily-basis. RFI attack traffic is spread over the course of a month, and there are 2-3 days of concentrated attack attempts every month.



The sporadic peaks of attack activity containing a high frequency of requests are usually from a single source, indicating that these attacks were issued by automatic tools.

The relative volume of RFI attacks is usually low. For sake of comparison, we measured the frequency of observed RFI attacks against the frequency of observed SQL Injection attacks between December 2010 and March 2011. Within the attack traffic, 1.7% was associated with SQL Injection, while 0.3% of the attack traffic was identified as RFI-related.

Remote File Inclusion – Attack Origins

We have observed RFI attacks that originated from hundreds of sources. Usually, an attacker initiated only a small number of RFI attacks. However, some attackers initiated a disproportionate number of attacks: the 10 most active attackers issued 51% of the observed attacks.

Most of the attackers were active against the observed Web applications during just a short period (less than a day). However, some attackers were active and repeatedly sent RFI attack vectors over a long period of weeks and even months.

As the following chart shows, most attack traffic originates from the United States.

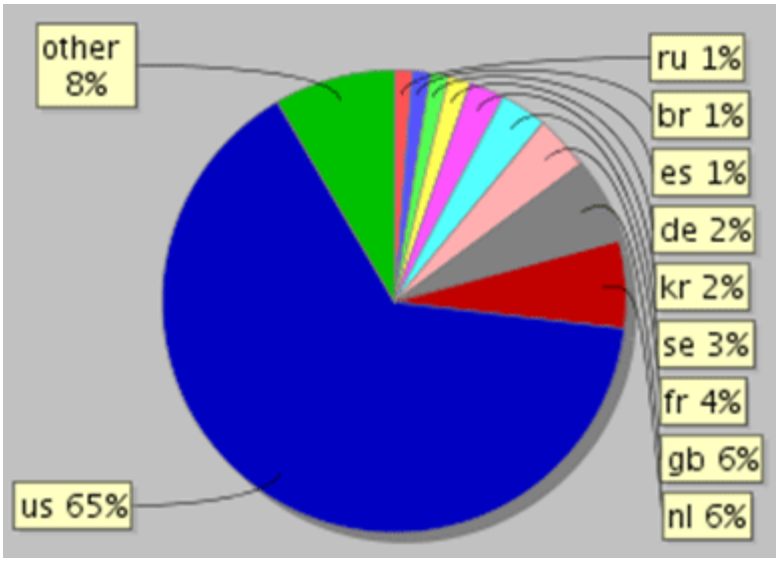


Diagram 1: RFI attack traffic origins by country

Remote File Inclusion – Attack Targets

Several observed Web applications were targeted by a large number of attackers. The attackers operated independently of one another with the goal of seeking exploitable vulnerabilities on the Web. Furthermore, each Web application was usually attacked by several attackers. We see this as an indication that active RFI attack tools are repeatedly trying to discover and exploit whatever RFI vulnerabilities they can detect on the Web.

We also noticed that there is a correlation between the number of RFI attacks targeted at a site and the popularity of a site, as well as a correlation between the number of RFI attacks targeted at a site and the total attack activity directed at it.

Remote File Inclusion – Malicious Scripts

We have observed hundreds of URLs that attackers attempted to remotely include within the Web applications. While the scripts are hosted at many locations, many of them are duplicates of each other, so the number of actual scripts that used in the attacks is small (20-30).

A detailed analysis of the scripts shows that most of them are intended to simply collect information from an attacked Web server and send it to the attacker. However, there are also a few highly sophisticated scripts that include ways for the attacker to take complete control over a vulnerable server.

Most of the observed RFI vulnerabilities were in Web applications that used the script language PHP. Therefore, most of the scripts intended for inclusion were also written in this language.

Remote File Inclusion – Observations Summary

1. A large portion of RFI attacks were part of a comprehensive high-volume attack on a Web application during a very short period (like an hour). This behavior is typical of automatic attack tools.
2. Many attack sources repeatedly initiated RFI attacks during long periods of time (weeks or months). This is indicative of automatic attack tools.
3. Most attacked sites were targeted by several sources.
4. Many RFI attack sources targeted multiple sites.
5. Similar copies of included script files are deployed on different compromised servers. The embedded URLs which reference these servers are used interchangeably between different attacks.
6. Many RFI attacks were interleaved with other attack vectors. For example, a Directory Traversal was used to identify RFI vulnerabilities of the application.

Remote File Inclusion – Protection from Attacks

The most common protection mechanism against RFI attacks is based on signatures for known vulnerabilities in the Web application. From our observations it is apparent that can we can improve the detection and blocking of such attacks by creating a blacklist of attack sources and a black list of URLs of remotely included malicious scripts:

1. Advanced knowledge of RFI attack sources enables the WAF to block an attack before it even begins.
2. A blacklist of the referenced URL enables the WAF to block exploits targeting zero-day vulnerabilities of applications.
3. The blacklist of IPs constructed from the RFI attack observations could be used to block other types of attacks issued from the same malicious sources.

Hacker Intelligence Initiative Overview

The Imperva Hacker Intelligence Initiative will be going inside the cyber-underground and providing analysis of the trending hacking techniques and interesting attack campaigns from the past month. A part of Imperva's Application Defense Center research arm, the Hacker Intelligence Initiative (HII), is focused on tracking the latest trends in attacks, Web application security and cyber-crime business models with the goal of improving security controls and risk management processes.

Imperva
3400 Bridge Parkway, Suite 200
Redwood City, CA 94065

Tel: +1-650-345-9000
Fax: +1-650-345-9004
www.imperva.com