zscaler | ThreatLabz

Security Research and Analysis Powering the Most Advanced Cloud-Delivered Protection

Blog

Friday, September 25, 2015

# Compromised WordPress Campaign - Spyware Edition

## Introduction

The Zscaler security research team started investigating multiple WordPress related security events earlier this month and came across a new widespread compromised WordPress campaign leading to the download of unwanted applications. This has been briefly covered by dynamoo and has been reported by some users on official WordPress forums.

During our research, we discovered that this campaign started in the first week of August, 2015 and has been fairly active since then resulting in over 20,000 security events to date from over 2,000 web pages. Majority of the WordPress sites affected by this campaign are running latest version 4.3.1 but the compromise could have occurred prior to the update.

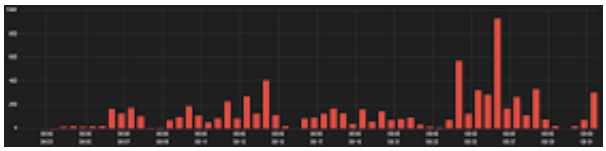

Figure 1: August 2015 WordPress Campaign hits

Figure 2: September 2015 WordPress Campaign hits

## Infection Cycle

The infection starts when a user visits a compromised WordPress site. The compromised pages will have injected JavaScript shown below:

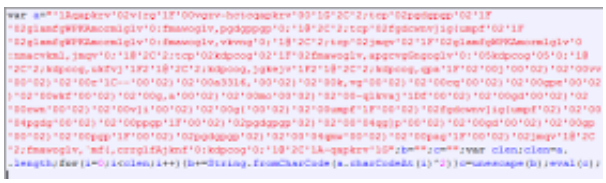

Figure 3: Injected malicious JavaScript code

The deobfuscated JavaScript code contains an iframe to the malicious server location:

Although the target domains varied across the transactions that we saw, the associated server IP address has remained

Figure 4: Deobfuscated JavaScript containing the iframe

the same.

**Target domains seen**

c11.n4.i.teaserguide[.]com
i.illuminationes[.]com
c11n4.i.teaserguide[.]com
kfc.i.illuminationes[.]com
kfc.i.teaserguide[.]com
xn--c11n4-ix3b.i.teaserguide[.]com
xn--kfc-rp0a.i.illuminationes[.]com
c114.i.teaserguide[.]com
rm3a.r.mega-us-pills[.]ws

The IP Address **91.226.33.54** associated with these domains is hosted in Latvia through a VPS hosting provider.

The injected iframe loads additional JavaScript that gathers information such as current system timestamp, timezone, and presence of Adobe Flash Player.

Figure 5: User system information gathering script

```
function flash() {
    if (navigator.plugins && navigator.plugins.length) {
        var type = 'application/x-shockwave-flash';
        var mimeTypes = navigator.mimeTypes;
        return mimeTypes && mimeTypes[type] && mimeTypes[type].enabledPlugin;
    } else {
        var sn = "ShockwaveFlash.ShockwaveFlash";
        try {
            var g = new ActiveXObject(sn + ".7");
            return true;
        } catch (h) {
            try {
                g = new ActiveXObject(sn + ".6");
                return true;
            } catch (i) {
                try {
                    g = new ActiveXObject(sn);
                    return true
                } catch (j) {
                    return false;
                }
            }
        }
    }
}
```

Figure 6: Function to check the presence of Flash Plugin and version information

The collected information is relayed back to the same server via a HTTP GET request. This is followed by a series of redirects leading to download of spyware or potentially unwanted applications (PUA) masquerading as legitimate applications.

Figure 7: Redirects from Latvia VPS server leading to PUA download

## Fake Flash Player - Win32.InstallCore

In one of the cases, we observed the user is prompted to update the Flash Player as seen below:

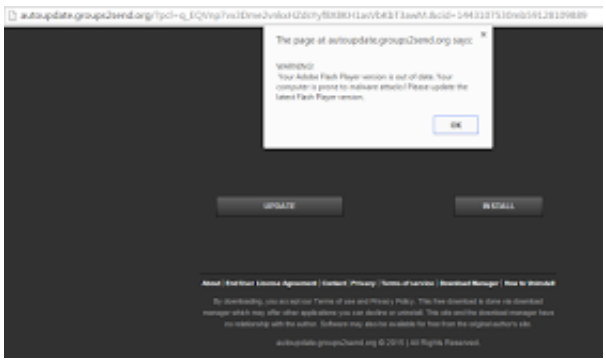

Figure 8: Out of date Flash Player warning

The page prompts the user to update or install a new flash player update. Regardless of the option the user selects, a fake Adobe Flash Player application is downloaded.

FileName : **Adobe Flash Player.exe**
MD5 : **fa75abf137224fc2c60b9b3c35c80a5e**

This file is a .NET Compiled executable which downloads and executes another setup file named FlashSetup.exe.

FileName : **Flash Setup.exe**
MD5: **87234af45b30740309c8bffcdf2167dc**

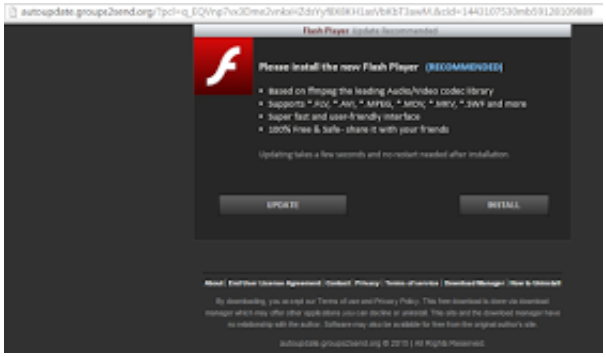

Figure 9: Fake Flash Player download

The downloaded file flashsetup.exe is a variant of Potentially Unwanted Application **Win32.InstallCore**. During the installation of the Adobe Flash Player, several other websites offering other unwanted scareware applications are displayed. One such case where the spyware installer prompts the user to download and install Windows 7 PC Repair tool is shown below:

Once


Figure 8: Scareware Windows 7 Repair utility

the spyware installation is complete, the user is redirected to the legitimate Adobe page indicating that the installation was not successful prompting the user to start over. If the user chooses to start over the installation, Adobe Flash Player will be installed from the genuine Adobe site.

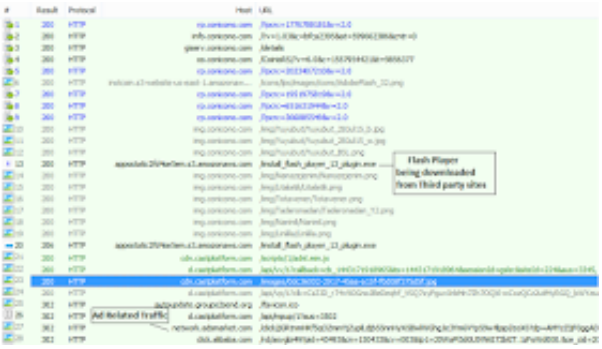


Figure 9: Download from third party sites & adware traffic from PUA

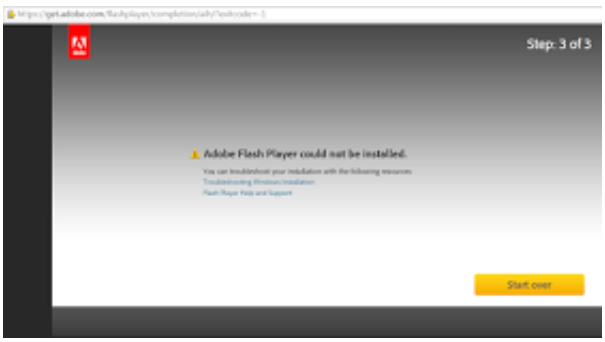


Figure 10: User redirected to legitimate Adobe Flash Player

### Fake MediaDownloader update - Win32.DownloadAssistant

In another case, the webpage prompts the user with a fake MediaDownloader software update which is a variant of PUA **Win32.DownloadAssistant**.

FileName: **Setup.exe**

MD5: **a885f33c308721831498a2ac581bd91c**


Figure 11: Fake MediaDownloader Update

The end result is same where a potentially unwanted application is downloaded and installed on the victim machine. These applications have the capability to download additional malicious or unwanted applications.

We also saw instances of fake web browser plugins being downloaded and installed. Below is an example of a Google Chrome Plugin - NewTabTV plus.

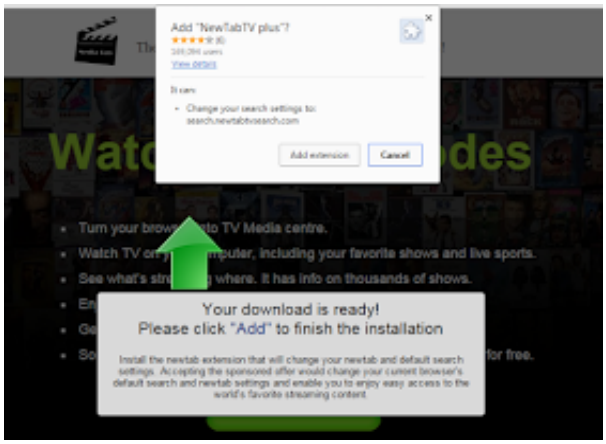


Figure 12: Fake Google Chrome Plugin download

The compromised sites involved in this campaign are distributed worldwide and not limited to one particular region.


Figure 13: Geo distribution of the compromised WordPress sites - September 2015

## Conclusion

WordPress, being one of the most popular Content Management Systems & Blogging platform, remains an attractive target for cybercriminals. Unlike previous campaigns involving Malware Authors and Exploit Kit operators, the end payload getting served in this campaign involves spyware and potentially unwanted applications. These applications may seem innocuous but can facilitate malvertising based attacks through unsolicited advertisements.

Zscaler ThreatLabZ is actively monitoring this campaign and ensuring that Zscaler customers are protected.

Analysis by Jithin Nair and Sameer Patil

Sameer Patil at 9:26 AM

Share G+1 0

No comments:

## Post a Comment

Home ›

View web version

**About Us**

- Julien Sobrier
- rubin azad
- Uday Pratap Singh
- Pradeep Mp
- Loren Weith
- Jithin Nair
- Abhaykant Yadav
- Tarun Dewan
- Dhruval Gandhi
- Amandeep Kumar
- Dhanalakshmi Pk
- Ed Miles
- viral
- Chris Mannon
- Sameer Patil
- Webmaster
- Deepen Desai
- Nirmal Singh
- John Mancuso
- Amit Sinha
- Shivang Desai
- Avinash kumar
- Manish Mukherjee

- Michael Sutton