F-Prot/Frisk Anti Virus bypass - ZIP Version Header

Ref   : TZO-042006-Zango
Author : Thierry Zoller / Security Engineer
WWW   : http://secdev.zoller.lu
Article : http://secdev.zoller.lu/research/zango.htm

I. Background

http://www.zangocash.com

"ZangoCash (formerly LOUDcash) is recognized around the world as one of the best pay-per-install affiliate programs on the Internet. ZangoCash is a subsidiary of 180solutions which also includes Zango and MetricsDirect . Every day, 7,500-10,000 ZangoCash affiliates distribute our software to users who are then connected with more than 6,000 MetricsDirect advertisers."

II. Description

After the acknowledgement of an License Agreement, during Startup, the bundled EXE contacts several servers and downloads the required Adware components. The downloaded components are not checked for integrity or authenticity and are executed as soon as they are downloaded.

The Following procedures are exploitable :

1. Initial Install
2. Auto-Update function

The condition is exploitable in the following scenarios :

1. You have legitimate control over the DNS server
2. You have compromised a DNS server
3. You forge a cache poisoning attack against a vulnerable DNS server
4. You have access to the machine and change the HOST file

Redirecting static.zangocash.com to an IP address under your Control and creating the respective V-host allows you to deploy any type of executable on the machine where zango is being installed or currently is installed.

Why is this an Issue ?
Especially the auto update function is a problem, imagine a DNS server (not a split setup) is compromised or cache-poisened, every workstation with zango installed inside the company can be immediately compromised by downloading a executable from a malicious site.

III. Summary

Vendor contact : 01/02/2006
Vendor Response : xx/xx/xxxx

Vendor Response :
Thank you very much for notifying us of this bug in the current version of F-Prot Antivirus. A fix for this bug will be included in future versions of F-Prot Antivirus.

```
Reference : TZO-042006-Zango
Author    : Thierry Zoller / Security Engineer
WWW       : http://secdev.zoller.lu
```