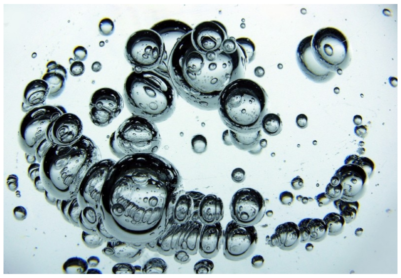
Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign

June 23, 2015 | by Erica Eng, Dan Caselden | Threat Intelligence



In June, FireEye's FireEye as a Service team in Singapore uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links to compromised web servers that served either benign content or a malicious Adobe Flash Player file that exploits CVE-2015-3113.

Adobe has already released a patch for CVE-2015-3113 with an out-of-band security bulletin (https://helpx.adobe.com/security/products/flash-player/apsb15-14.html). FireEye recommends that Adobe Flash Player users update to the latest version as soon as possible.

FireEye MVX detects this threat as a web infection, the IPS engine reports the attack as CVE-2015-3113, and the SHOTPUT backdoor is reported as Backdoor.APT.CookieCutter.

APT3

The China-based threat group FireEye tracks as APT3, aka UPS, is responsible for this exploit and the activity identified in our previous blog post, Operation Clandestine Fox. This group is one of the more sophisticated threat groups that FireEye Threat Intelligence tracks, and they have a history of introducing new browser-based zero-day exploits (e.g., Internet Explorer, Firefox, and Adobe Flash

Player). After successfully exploiting a target host, this group will quickly dump credentials, move laterally to additional hosts, and install custom backdoors. APT3's command and control (CnC) infrastructure is difficult to track, as there is little overlap across campaigns.

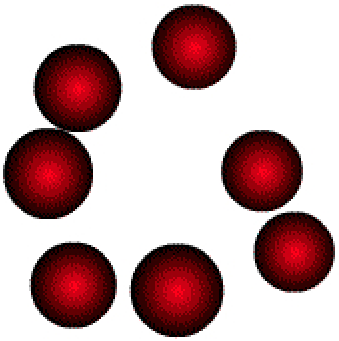
Activity Overview

In the last several weeks, APT3 actors launched a large-scale phishing campaign against organizations in the following industries:

- Aerospace and Defense
- Construction and Engineering
- High Tech
- Telecommunications
- Transportation

Upon clicking the URLs provided in the phishing emails, targets were redirected to a compromised server hosting JavaScript profiling scripts. Once a target host was profiled, victims downloaded a malicious Adobe Flash Player SWF file and an FLV file, detailed below. This ultimately resulted in a custom backdoor known as SHOTPUT, detected by FireEye as Backdoor.APT.CookieCutter, being delivered to the victim's system.

The payload is obscured using xor encoding and appended to a valid GIF file.



Attack Vector

The phishing emails used by APT3 during this campaign were extremely generic in nature, almost appearing to be spam. An example email body:

```
Save between $200-450 by purchasing an Apple Certified Refurbished iMac
through this link. Refurbished iMacs come with the same 1-year extendable
warranty as new iMacs. Supplies are limited, but update frequently.
```