January 2004 to September 2015

f-secure.com/weblog/archives/00002466.html

F-SECURE LABS

<<< NEWS FROM THE LAB - Monday, December 3, 2012 >>>

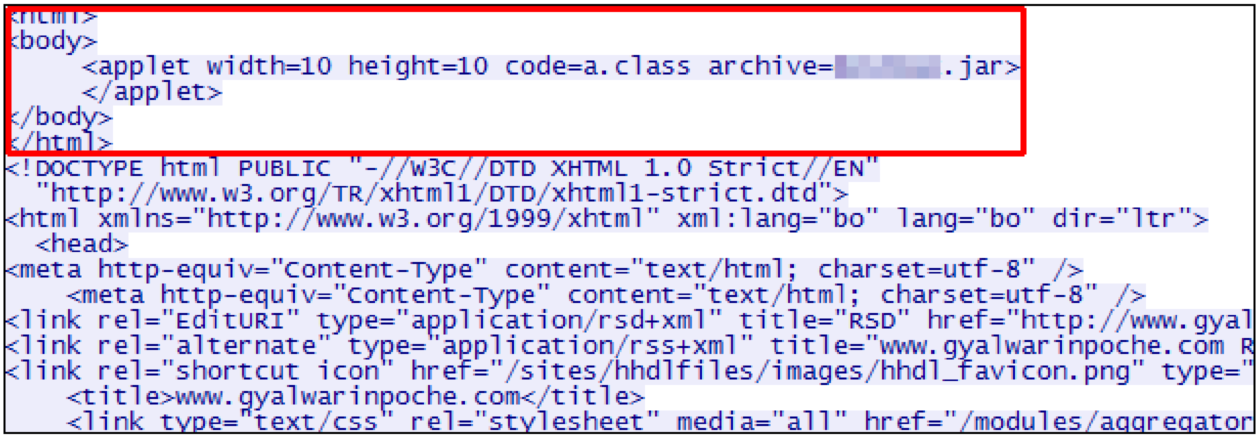
ARCHIVES | SEARCH

New Mac Malware Found on Dalai Lama Related Website

Posted by Sean @ 11:08 GMT

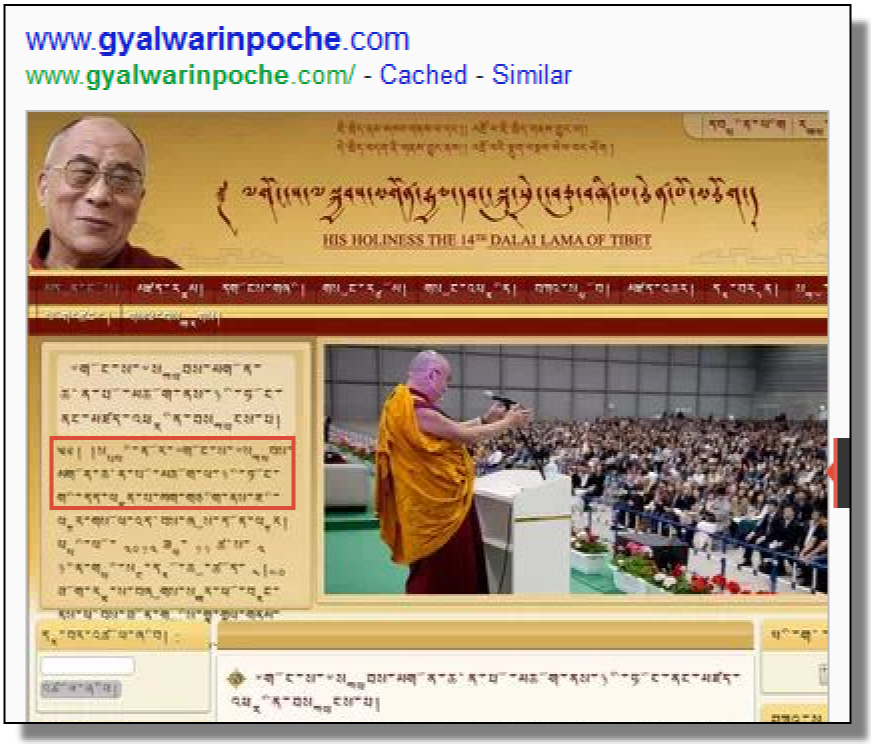
Acting on a tip, a member of our Threat Research team (Brod) has discovered a Dalai Lama related website is compromised and is pushing new Mac malware, called Dockster, using a Java-based exploit.

Page source from gyalwarinpoche.com:



```
<html>
<body>
    <applet width=10 height=10 code=a.class archive=[redacted].jar>
    </applet>
</body>
</html>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="bo" lang="bo" dir="ltr">
  <head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://www.gyal
<link rel="alternate" type="application/rss+xml" title="www.gyalwarinpoche.com R
<link rel="shortcut icon" href="/sites/hhdlfiles/images/hhdl_favicon.png" type="
    <title>www.gyalwarinpoche.com</title>
    <link type="text/css" rel="stylesheet" media="all" href="/modules/aggregator
```

Here's a screenshot of gyalwarinpoche.com from Google's cache:

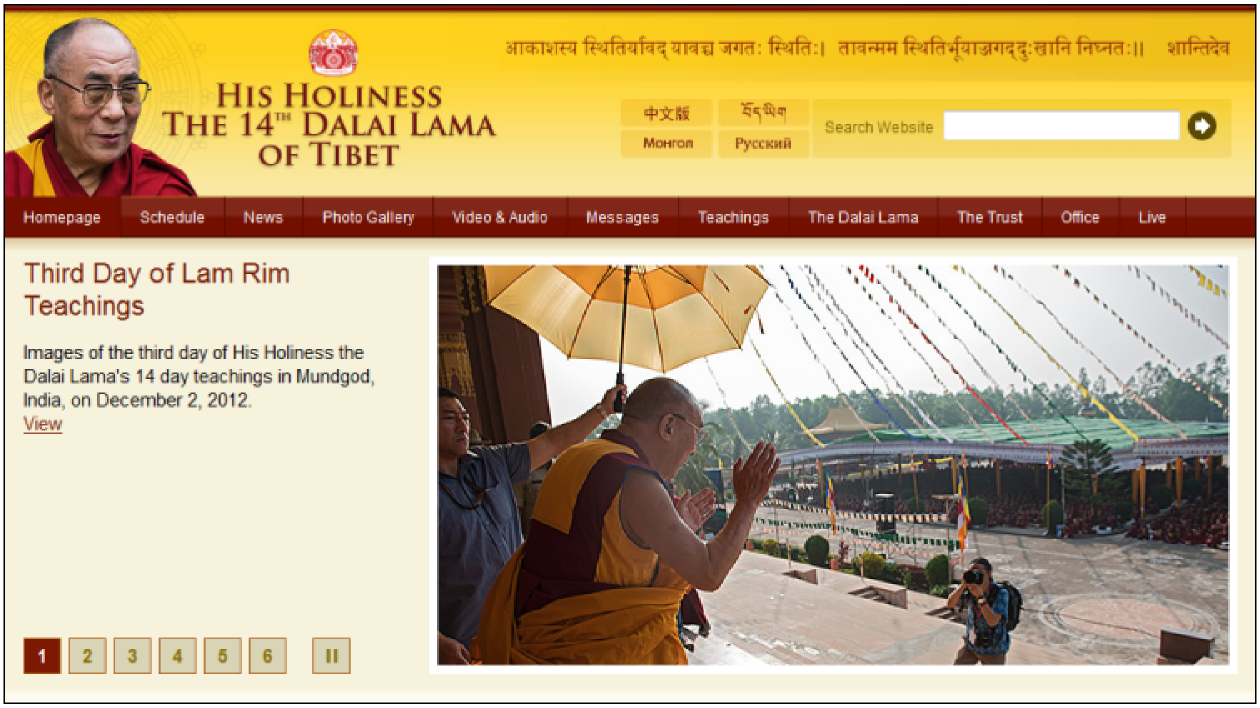


www.gyalwarinpoche.com

www.gyalwarinpoche.com/ - Cached - Similar

Note: Google's November 27th snapshot also includes a link to the malicious exploit (so don't visit).

The gyalwarinpoche site doesn't seem to be as "official" as dalailama.com:



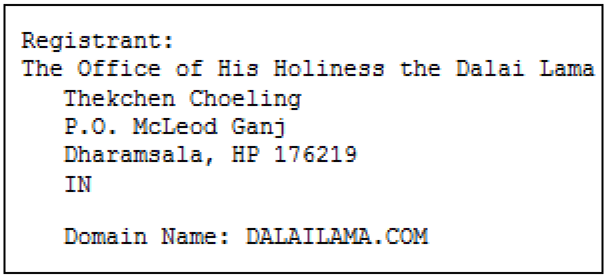
Third Day of Lam Rim Teachings

Images of the third day of His Holiness the Dalai Lama's 14 day teachings in Mundgod, India, on December 2, 2012.

View

But it's been around since 2009/2010 and the name is the same as the Dalai Lama's YouTube channel.

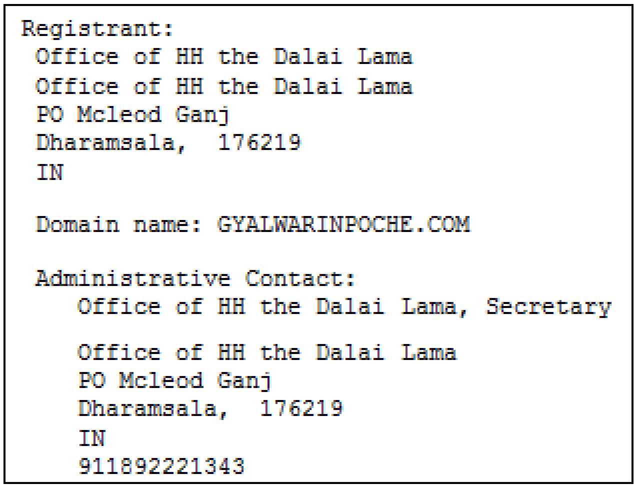
And the Whois information is similar:



```
Registrant:
The Office of His Holiness the Dalai Lama
   Thekchen Choeling
   P.O. McLeod Ganj
   Dharamsala, HP 176219
   IN

   Domain Name: DALAILAMA.COM
```

dalailama.com



```
Registrant:
 Office of HH the Dalai Lama
 Office of HH the Dalai Lama
 PO Mcleod Ganj
 Dharamsala,  176219
 IN

 Domain name: GYALWARINPOCHE.COM

 Administrative Contact:
    Office of HH the Dalai Lama, Secretary

    Office of HH the Dalai Lama
    PO Mcleod Ganj
    Dharamsala,  176219
    IN
    911892221343
```

gyalwarinpoche.com

The Java-based exploit uses the same vulnerability as "Flashback", CVE-2012-0507. Current versions of Mac OS X and those with their browser's Java plugin disabled should be safe from the exploit. The malware dropped, Backdoor:OSX/Dockster.A, is a basic backdoor with file download and keylogger capabilities.

This is not the first time gyalwarinpoche.com has been compromised and it certainly isn't the first time Tibetan related NGOs have been targeted. Read more here and here.

There is also an exploit, CVE-2012-4681, with a Windows-based payload: Trojan.Agent.AXMO.

MD5 info:

Exploit:Java/CVE-2012-0507.A — 5415777DB44C8D808EE3A9AF94D2A4A7
Backdoor:OSX/Dockster.A — c6ca5071907a9b6e34e1c99413dcd142
Exploit:Java/CVE-2012-4681.H — 44a67e980f49e9e2bed97ece130f8592
Trojan.Agent.AXMO — c3432c1bbdf17ebaf1e10392cf630847