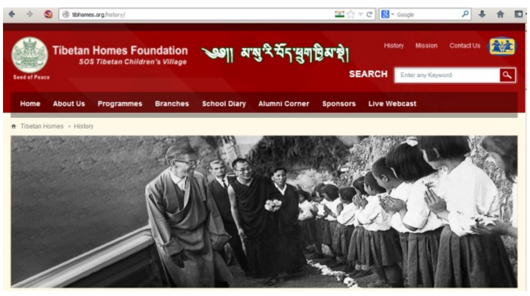
APT REPORTS INCIDENTS

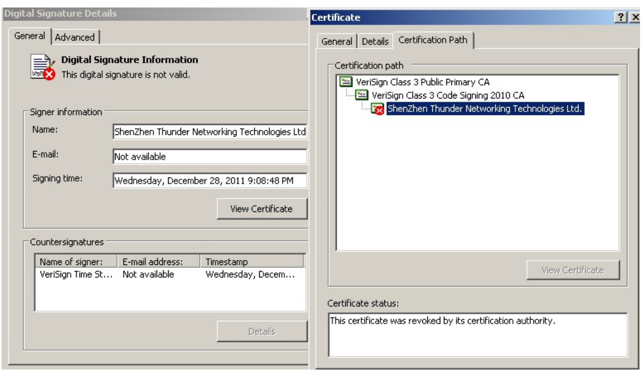
Winnti-Stolen Digital Certificates Re-Used in Current Watering Hole Attacks on Tibetan and Uyghur Groups

By Kurt Baumgartner on April 12, 2013. 4:31 am

A new-ish Flash exploit has been on the loose for attacks around the web. This time, the attackers have compromised a caregiver site providing support for Tibetan refugee children and are spreading backdoors signed with Winnti stolen certificates delivered with Flash exploits – the compromised web site is the NGO "Tibetan Homes Foundation". Previously, FireEye identified similar "Lady Boyle" related malicious swf exploiting CVE-2013-0634. A notification has been sent to the contacts of the web site, but apparently the malicious footer.swf file is still hosted at the Foundation's web site, so please do not visit it just yet. Also, be sure to update your Flash player to the latest version.


tibhomes.org/history/
Tibetan Homes Foundation
SOS Tibetan Children's Village
Seed of Peace
History Mission Contact Us
SEARCH
Enter any Keyword
Home About Us Programmes Branches School Diary Alumni Corner Sponsors Live Webcast
Tibetan Homes › History

This site certainly appears to be a classic example of a "watering hole" attack. F-Secure pointed out another Lady Boyle watering hole set up against a related Uyghur group, which has been targeted in tandem following the early March World Uyghur Congress. The delivered backdoors are shown to be signed with Winnti-stolen digital certificates in the F-Secure post, including the stolen MGAME certificate.
Here is an example of those same stolen certs reused for the backdoors in the Tibetan Homes Foundation incident. We see both the MGAME cert and the ShenZehn certs signing the backdoors, here are screenshots of the latter:



Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is not valid.

Signer information
Name: ShenZhen Thunder Networking Technologies Ltd
E-mail: Not available
Signing time: Wednesday, December 28, 2011 9:08:48 PM
View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	Wednesday, Decem...

Details

Certificate

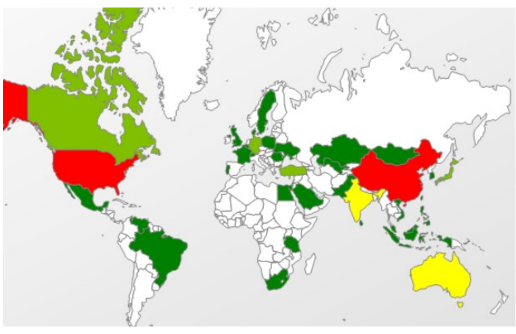
General | Details | Certification Path

Certification path
VeriSign Class 3 Public Primary CA
VeriSign Class 3 Code Signing 2010 CA
ShenZhen Thunder Networking Technologies Ltd.

View Certificate

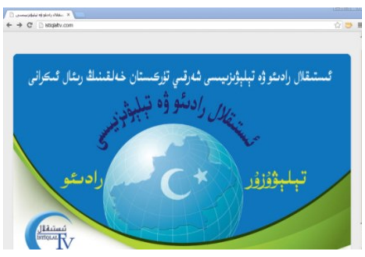
Certificate status:
This certificate was revoked by its certification authority.

Our products detect the Flash exploit+payload as Exploit.SWF.CVE-2013-0634.a. Here is a heatmap of our worldwide detections. Note that not all of these detections are Lady Boyle related, I estimate that at least a third of them are:



Other sites hosting the Lady Boyle swf exploit over the past couple of months have included "tibetangeeks.com", who recently cleaned up their site and posted a cooperative plea to their attackers, and "vot.org" or the "Voice of Tibet" which is also cleaned up. Currently cleaned up but previously serving "Exploit.SWF.CVE-2013-0634.a" were Uyghur related sites "istiqlaltv.com" and "maarip.org", with the same "LadyBoyle" swf path as the Tibetan Homes Foundation, i.e.:

hxxp://maarip.org/uyghur/footer(.)swf


istiqlaltv.com
ئىستىقلال رادىئو ۋە تېلېۋىزىيىسى شەرقىي تۈركىستان خەلقىنىڭ رېئال ئىكرانى
ئىستىقلال رادىئو ۋە تېلېۋىزىيىسى
رادىئو
تېلېۋىزور
ISTIQLAL TV

So, what we have is an active watering hole campaign implementing a fairly new Flash exploit and abusing digital certificates that were stolen as a part of the ongoing Winnti targeted attack campaigns on game developers and publishers.

Related md5:

BD9FD3E199C3DAB16CF8C9134E06FE12

215CEC7261D70A5913E79CD11EBC9ECC

12181311E049EB9F1B909EABFDB55427

ADOBE ADOBE FLASH APT TARGETED ATTACKS VULNERABILITIES AND EXPLOITS WEBSITE HACKS

Share post on:

Related Posts

Hunting APTs with YARA

Mokes and Buerak distributed under the guise of security certificates

Operation AppleJeus Sequel

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Enter your comment here

Name *

Email *

☐ Save my name, email, and website in this browser for the next time I comment.

☐ Notify me when new comments are added.

SUBMIT

☐ I'm not a robot reCAPTCHA Privacy - Terms

IN THE SAME CATEGORY

DNS Manipulation in Venezuela in regards to the Humanitarian Aid Campaign

Chafer used Remexi malware to spy on Iran-based foreign diplomatic entities

GreyEnergy's overlap with Zebrocy

A Zebrocy Go Downloader

DarkVishnya: Banks attacked through direct connection to local network

Email

☐ I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

SUBSCRIBE