OUR BLOG

The Tibetan Alliance of Chicago hit by cyber waterholing attack

Share

FRIDAY, AUG 16, 2013

Forcepoint

Websense Security Labs™ **ThreatSeeker® Intelligence Cloud** has detected that the website of the Tibetan Alliance of Chicago has been compromised to serve malicious code.

In the last two days, the **BBC** website reported news about a waterholing attack against the Central Tibetan Administration website. Over the last two years, attacks like these have targetted pro-Tibet websites and other human rights organizations around the world. A waterholing attack is one that targets users of specific websites with the aim to install malware on their systems (usually using a backdoor approach) to collect documents, email contacts, social contacts, and passwords. The frequency of these attacks prompted Websense Security Labs to check our collective threat intelligence for any other websites that are considered pro-Tibet to see if they are affected by this kind of attack.

In this blog we're going to analyze the Tibetan Alliance of Chicago website and illustrate how waterholing attacks are conducted.

One of the trends with targeted attacks in the last few years is that any installed malware binaries connect to dynamic DNS websites. One of the most interesting aspects of this specific attack is that a successful exploit downloads a binary that connects to a small Dynamic DNS service offered by none other than a German-based security appliances and services company, which reaffirms the notion that perpetrators pick and choose the parts of their attack infrastructure.

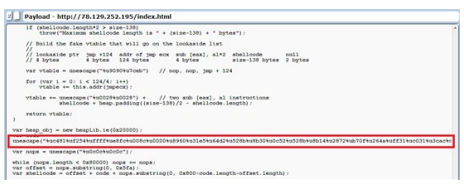
Although the website does not have a high Alexa rank, we thought it was worth consideration, because our analysis concluded that it wasn't a scattered attack, but a targeted injection to infect the users of that website. The website has been injected with two malicious iFrames as shown below:

We started to investigate the content of these two links above. The first (hxxp://78.129.252.195/images/Adobe/index.html) contains another iFrame that leads to a Firefox plugin named "Adobe Flash Player.xpi," although at the time of the analysis, the plugin wasn't available:

When we used Threatseeker to search for other instances of "Adobe Flash Player xpi," we detected other malicious websites, so we deduced that the aim of this iFrame was to try to install a malicious plugin using social engineering techniques. The second link (hxxp://78.129.252.195/index.html) caught our attention, because it seems to be malicious code exploiting the vulnerability **CVE-2012-4969** as shown below:

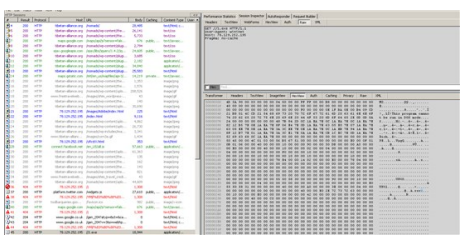
The code highlighted above shows another iframe that leads to hxxp://78.129.252.195/yRrztX.html with the following content:

From this, we could see the code used to trigger the Internet Explorer vulnerability addressed as **CVE-2012-4969** and spotted in other targeted attacks by a security researcher **here** in September 2012. The code within the page "index.html" uses the "heap spray" mechanism to run shellcode if the exploiting attempt succeeds. The following is the snippet of code that has been assigned the shellcode:

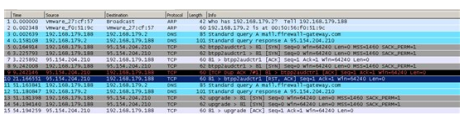


Once the shellcode is executed, it downloads and runs a malicious file on the compromised system. The shellcode appears to be using the Windows default user-agent 'wininet' to retrieve the malicious file, which in itself can be considered suspicious, because we don't normally see many legitimate HTTP requests that use this agent. We do see this user-agent being used by legitimate software, but it's not predominant.

Following is the Fiddler's session where you can see the binary file that was downloaded:



Analyzing the dynamic behavior of the malicious executable, you can detect a first call to the command-and-control point at *mail.firewall-gateway.com* located in the United Kingdom:

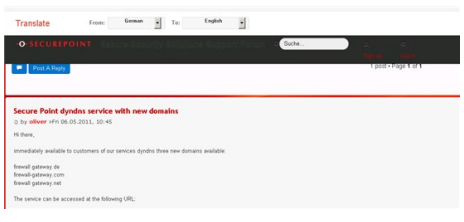


We conducted a quick investigation about the domain "firewall-gateway.com," and it appears to be mantained by the German service provider, Securepoint, that specializes in provisioning secure VPN endpoints and other kinds of network services offerings. This is what we saw from the WHOIS record:

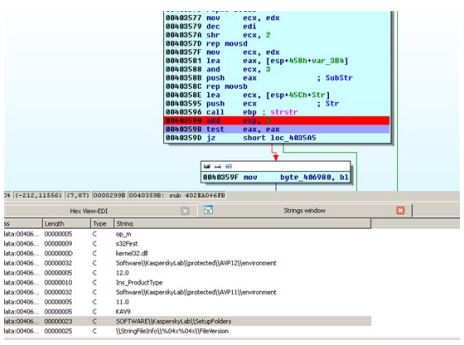
```
Domain Name:        FIREWALL-GATEWAY.COM
Registrar:          ASCIO TECHNOLOGIES, INC.
Whois Server:       whois.ascio.com
Referral URL:       http://www.ascio.com
Name Server:        DYNDNS.SECUREPOINT.DE
Name Server:        MHWSERV01.MHW.DE
Name Server:        NS.SECONDARY-DNS.DE
Status:             ok
Updated Date:       15-jan-2013
Creation Date:      14-jan-2010
Expiration Date:    14-jan-2014
```

:

In one of Securepoint's support forums, the announcement of the availability of a dynamic DNS service is still shown. The service appears to be available at **this** address. We believe it's an attempt to remain covert, because it is not by chance that the perpetrators chose their command-and-control point to be reached through a dynamic DNS service associated with a security company.



The detection rate of the binary file seems very low as reported by Virustotal. From a brief static analysis of the malicious binary file, you can detect a list of strings used to check the presences of Antivirus on the impacted system:



The binary file has a low AV rate detection rate, as reported by this Virustotal **report**.

In this blog we gave a brief example of what seems to be a waterholing attack that is aimed for a specific crowd, in this case, pro-Tibet users. We believe that the complexity of such attacks lies in direct relation to the security measures that are employed by the potential targets, in this case the attack isn't that complex but probably just enough to fulfill its ultimate purpose.

Websense customers are protected from injected websites and the different stages of this threat with our Advanced Classification Engine - **ACE**

Tags Cyber Attack Cyber Crime

About the Author

Forcepoint

More articles in X-Labs

The persuasiveness of a remote job

Robert Neumann