



Case Study: blog.icann.org

BACKGROUND:

The ICANN blog, located at <http://blog.icann.org>, is the official web log of the Internet Corporation for Assigned Names and Numbers. Its intended purpose is to provide fast, direct communication between ICANN and the Internet community. Posting on the blog is open to anyone, no authentication is required. The blog is powered by the free web publishing platform, WordPress.

The blog receives varying number of posts and comments each month. Post topics range from meeting announcements, to technical analysis, to information on ICANN policies. Comments typically contain a wide variety of opinions on the subject posted, and come from people all over the world. ICANN maintains a strict comment policy which prohibits spam, abuse, libel, conjecture and nonsense. Posts which are classified as such are deleted without further regard.

On June 30th, 2008, the blog site looked similar to what is shown in Figure 1. However, on July 1st, 2008, the site had changed. Administrators of the blog received a notification via a trusted Jabber chat session: **"Your Machine looks funny, have you been hacked?"** Upon viewing the blog site a few minutes after receiving the notification, administrators found the site to look like what is show in Figure 2.

	
<p>Figure 1 – approximation of blog.icann.org before the hack</p>	<p>Figure 2 - blog.icann.org after the hack</p>

QUESTIONS:

- What policies or procedures do you have in place to detect defacing of your website?
- How would you be notified that your website has been defaced?
- What would your response actions be when you are notified your website has been defaced?
- How would you recover your website back to a known good state?
- How do you gain back the confidence lost in the integrity of your system once you have been hacked?

EPILOGUE:

What are our response actions when our website has been defaced? What are the priorities with regard to system integrity vs. evidence preservation? How do we recover it back to a known good state? How do we gain back the confidence lost in the integrity of our system?

The ICANN staff began to ask themselves these very questions and began to take action on the answers they came up with. An initial meeting of the technical staff followed 3 minutes after the initial notification. From this meeting it was determined to remove the content from public view while still preserving critical evidence for the forensics analysis that would be performed later. The affected box was isolated on the network within 12 minutes of initial notification, the blog.icann.org record was redirected to the main site icann.org within 20 minutes, and notification was made to the ICANN executive team 36 minutes after the initial notification the site had been hacked.

The engineering staff realized that they could not just restore the site from a back up without understanding how the attack/defacement was successful. They decided to preserve the evidence by making three sector by sector copies of the affected server. One was sealed for evidence and turned over to law enforcement officials, one was stored for informational purposes, and one was analyzed to determine the vector and scope of the attack.

7 hours and 39 minutes after the initial notification, the forensic analysis of the attack was complete. The staff found the website was susceptible to a WordPress vulnerability easily found, most likely, by an attacker armed with nothing more than Google.com and the knowledge of what to search for with respect to WordPress versions and associated vulnerabilities.

11 hours and 12 minutes after initial notification, a more in depth briefing was given to the ICANN executive team and board of directors. At 20 hours and 12 minutes after notification, the original disk and report was turned over to law enforcement agents. Finally, after 30 hours and 48 minutes, the site was rebuilt and the data was restored from a known good backup.

The law enforcement investigation is still ongoing.

ANALYSIS:

There was no documented response plan. Fortunately, ICANN had the right people, with the right experience, in the right place at the right time. The people involved in responding to the attack had been through similar experiences and knew what to do. More importantly, they understood the critical issues surrounding an attack (preservation of evidence and corporate priorities) and were able to take appropriate action. Had these particular people not been available for the response, a less coordinated outcome would most certainly have occurred.

TIMELINE:

13:48 (PST) First Notification arrived via Jabber
"Your Machine looks funny, have you been hacked?"

Initial internal confirmation takes a couple of minutes

>> What do you do when you get hacked?

13:50 CTO calls engineering staff into meeting room:
13:51 Event logging started

Discussions held on mitigation:

>> What are the priorities? Systems availability vs preservation of
>> evidence

(Initial fix, remove bad content from public access)

14:00 Turn off port on the switch to avoid tampering with machine 14:00
Dispatched engineer to physical location of server

14:03 Blog.icann.org DNS Changed to point to icann.org A record

14:08 Zone change complete blog.icann.org = www.icann.org

14:22 Initial heads up to communications department

14:24 Omblog.icann.org redirected to point to icann.org

14:24 Initial report delivered to Executive Team

(Permanent fix, restore systems, preserve evidence, understand attack)

Made copies of compromised disk (Sector for sector) One copy used for
analysis, one copy stored for information Original disk sealed

At same time retrieved back-up data.

Analysis of data and logs to understand compromise and evaluate risks when
restoring backups.

21:27 Analysis complete : Source of attack identified, nature of
compromise also clearly known.

>> Scripted attack against a known wordpress vulnerability. Targeted by
>> google search for wordpress version.

July 2nd 2008

01:00 More in depth executive and board briefing

10:00 Original disk and report filed with LEA

19:00 Scheduled restore of systems.

Investigation is ongoing.....