Supplementary Submission to

House of Representatives

Communications Committee

Inquiry into Cybercrime

November 2009

Web Management InterActive Technologies Pty Ltd
P.O. Box 1073, Capalaba, Qld, 4157
Voice Phone: 07-3823-5150
Fax Phone: 07-3823-5152
Email: info@wmit.net

Proposal for an Australian Protected Network

Thank you for the opportunity to supply a Supplementary Submission to the committee.

Of particular import for this submission is recent events in the news and responses to my advices to website owners when it is found they have had security breaches.

On this recent weekend, a total of approximately 50 websites were notified that they had breaches in their security and hidden links had been put on their sites. These links are usually of a Pornographic or Viral nature. Not all websites can be contacted of course, because without a central database like the Australian Protected Network for website providers to register contact details, the system relies only on contact details available via the internet.

One website responded in a positive manner, but since they were a US Financial institution and did not want to be named, they declined my request to quote them to the Cyber Crime Committee. I include the non-identifiable portion of this communication below -:

From: XXXXXXXXXXXX@XXX
Sent: Sundav. 15 November 2009 11:10 PM
To: XXXXXXXXXXXXXXXXXXX
Subject: RE: XXXXXXXXXXXX

I've corrected this issue; however, I'm confused how you found it in the first place without knowing it was there. This was next indexed by any search engines due to proper use of .htaccess and robots.txt and crawling of the website doesn't find the link as well. There is no theme or template alterations providing internal links to this web page. How did you come across this in the first place and what is your resolve for bring it to our attention. Our company is working with law enforcement as this is a lending based website based in the US. Any help would be appreciated as we continue to track down the source.

-----Original Message-----
From: XXXXXXXXXXXXXXXXXXX
To: XXXXXXXXXXXX@XXX
Sent: Sat, Nov 14, 2009 8:58 am
Subject: XXXXXXXXXXXX

```
Name:    XXXXXXXXXXXXXXXXXXX

Email:   XXXXXXXXXXXXXXXXXXX

Subject: Intrusion Detected.

Message: Our systems have detected links on the net that may indicate your
website has been compromised. It might pay you to check that your website hasn't
had an intruder. One of the links looks like this  -:

www.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.html

I hope you don't have too much trouble fixing it.

This has just been a friendly advisory in the hopes of building a safer net :)

James :) Collins,
Web Management InterActive Technologies Pty Ltd.
```

XXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX

In further communications, they were quite grateful and appreciated the “heads up”, but this, like many similar Cyber Crimes, will go largely unreported and unnoticed. The expansion of this function will make significant inroads as the Australian Protected Network becomes a hub for contact and monitoring.

There has also been a recent Newspaper article which might interest the committee. It particularly highlights the defence of the nation aspect of the proposed Australian Protected Network. I include it as an attachment to this submission.

The article takes a very balanced view of the threats that we face on a National front. It cites examples where cyber warfare has already been used and asks the question as to whether we will remain unprotected or not.

James Collins

Managing Director,

Web Management InterActive Technologies Pty Ltd.

Report: Countries prepping for cyberwar

By **Elinor Mills**

STORY HIGHLIGHTS

- McAfee: Countries are amassing cyberweapons, conducting espionage
- Report based on interviews with experts in international relations, security
- Experts are seeing increased intelligence gathering, according to report
- Threats of cyberwarfare have been debated for decades

RELATED TOPICS

- Internet
- Computer Security

(CNET) -- Major countries and nation-states are engaged in a "Cyber Cold War," amassing cyberweapons, conducting espionage, and testing networks in preparation for using the Internet to conduct war, according to a new report to be released on Tuesday by McAfee.

In particular, countries gearing up for cyberoffensives are the U.S., Israel, Russia, China, and France, the says the report, compiled by former White House Homeland Security adviser Paul Kurtz and based on interviews with more than 20 experts in international relations, national security and Internet security.

"We don't believe we've seen cases of cyberwarfare," said Dmitri Alperovitch, vice president of threat research at McAfee. "Nations have been reluctant to use those capabilities because of the likelihood that [a big cyberattack] could do harm to their own country. The world is so interconnected these days."

Threats of cyberwarfare have been hyped for decades. There have been unauthorized penetrations into government systems since the early ARPANET days and it has long been known that the U.S. critical infrastructure is vulnerable.

However, experts are putting dots together and seeing patterns that indicate that there is increasing intelligence gathering and building of sophisticated cyberattack capabilities, according to the report titled "Virtually Here: The Age of Cyber Warfare."

"While we have not yet seen a 'hot' cyberwar between major powers, the efforts of nation-states to build increasingly sophisticated cyberattack capabilities, and in some cases demonstrate a willingness to use them, suggest that a 'Cyber Cold War' may have already begun," the report says.

Because pinpointing the source of cyberattacks is usually difficult if not impossible, the motivations can only be speculated upon, making the whole cyberwar debate an intellectual exercise at this point. But the report offers some theories.

For instance, Alperovitch speculates that the July 4 attacks denial-of-service on Web sites in the U.S. and South Korea could have been a test by an foreign entity to see if flooding South Korean networks and the transcontinental communications between the U.S. and South Korea would disrupt the ability of the U.S. military in South Korea to communicate with military leaders in Washington, D.C., and the Pacific Command in Hawaii.

"The ability of the North Koreans to disable cybercommunications between the U.S. and South Korea would give them a huge strategic advantage" if they were to attack South Korea, he said.

There have been earlier attacks that smack of cyberwarfare too. Estonian government and commercial sites suffered debilitating denial-of-service attacks in 2007, and last year sites in Georgia were attacked during the South Ossetia war, orchestrated by civilian attackers, the report says.

The report concludes that if we aren't seeing it already, cyberwarfare will be a reality soon enough.

"Over the next 20 to 30 years, cyberattacks will increasingly become a component of war," William Crowell, a former NSA deputy director, is quoted as saying. "What I can't foresee is whether networks will be so pervasive and unprotected

that cyberwar operations will stand alone."

Find this article at:
http://www.cnn.com/2009/TECH/11/17/cnet.cyberwar.internet/index.html?eref=rss_world&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+rss%2Fcnn_world+%28RSS%3A+World%29

☐ Check the box to include the list of links referenced in the article.