BARRACUDALABS

Searching for Malware:

A Review of Attackers' Use of Search Engines to Lure Victims

Paul Judge

David Maynor

The Problem

Sites like Twitter, Yahoo!, Bing and Google all have some form of popular/trending search terms.

These terms can be co-opted by markets and malware authors to point to their own wares.

The sites can be used for spam, drive-by malware installs and phishing.

DEMO:

Examples of current terms and sites that have fallen prey to SEO poisoning.

How They Do It

BARRACUDALABS

A brief overview and example of previous term hijacking techniques.

BARRACUDALABS

Current ways to find the terms.

BARRACUDALABS

Flooding Web sites and social networks with specific terms and links.

BARRACUDALABS

And…We have malware!

BARRACUDALABS

DEMO:

A successful SEO poison.

How It’s Detected

Lists, Lists and more lists

BARRACUDALABS

White Lists

Black Lists

SPAM Lists

Vendor Proprietary Databases

These don’t always wor

BARRACUDALABS

Average time between infection and a URL showing up on a list could be days at best, weeks at worst.

DEMO:

List lag

BARRACUDALABS

Code analysis (All these sites have something in common; they are trying to hide their true intention.)

Code analysis of the Webpage including any JavaScript found can reliable detect a “suspicious” site

DEMO:

JavaScript analysis of a bad site

Correlation

How to tie this all together

Gaps in coverage:

How can the bad guys still slip through?

BARRACUDALABS

Future of Search Engine Malware

BARRACUDALABS

Attacker Countermeasures

Better Obfuscation

Using botnets and social networks to create an instant credible account

More targeted attacks: spear phishing for SEO poisoning

How Search Engines should respond – interactive discussion

THANK YOU!

http://www.barracudalabs.com/

BARRACUDALABS