Moving From Poisoning the Ocean to Poisoning the Watering Hole

Tuesday, October 30, 2012

Article by Chris Wysopal

RSA has published, "THE VOHO CAMPAIGN: AN IN DEPTH ANALYSIS" which describes an APT style campaign against several targets.

The campaign used malicious content on several websites dubbed "watering holes" in order to compromise the campaign target's client machines.

Injecting malicious content into vulnerable websites that will then become a drive-by client attack to a website visitor is old news. I wrote about this in my blog post, "SQL Injection Tangos with Heap Overflows", back in Dec 2008.

What I see new here is the watering hole concept where the websites that are compromised to host the malicious content are chosen because they are more likely to be visited by the ultimate targets.

I wish they had discussed how these websites were compromised. We now live and work in a shared digital ecosystem and web sites that allow their content to be poisoned harm the ecosystem as a whole.

Using the watering hole analogy, if you are the owner of a location where people congregate to drink you need to keep the beverages safe and clean. Unfortunately digital safety is decades behind food safety. If you own a website you need to understand what SQL Injection and XSS are.

Water hole poisoning is a refinement of content poisoning attacks much like spearphishing is a refinement of phishing to go after specific targets.

I expect to see much more of this in the future as attack patterns get optimized to make attack campaigns more targetted and hence more efficient and less detectable.

Cross-posted from Veracode

Possibly Related Articles: