Cracking Stats for Q1 2014

written by Karl Fosaaen | June 2, 2014

During many of our penetration tests, we gather domain password hashes (with permission of the client) for offline cracking and analysis. This blog is a quick summary of the hashes that we attempted to crack in the first quarter of 2014. The plan is to do this again each quarter for the rest of the year to see how we did overall for the year.

There was a relatively small sample for this quarter: just three sets of domain hashes that added up to 10,050 hashes. We are frequently in environments with twice as many users (20k and up), so this is a pretty limited set. One of these sets had LM hashes stored along with the NTLM hashes, making our cracking efforts a little bit easier. Of these hashes, 2,583 were duplicates, leaving 7,184 unique hashes. Of the 10,050 hashes, we were able to crack 7,510 (74.73%).

Cracked Password Length Breakdown:

As you can see, the cracked passwords peak at the eight character length. This is pretty common for a minimum password length, so it's not a big surprise that this is the most common length cracked.

Some more interesting finds:

- Most Common Password (606 instances): Password1
- Longest Password: 19 characters – visualmerchandising
- Most Common Length (3,356 instances): 8 characters
- Instances of "password" (case-insensitive): 122
- Instances of [ClientName] (case-insensitive, no modifications, and redacted for obvious reasons): 284
- Instances of "winter2014" (case-insensitive): 3

- Instances of “winter14” (case-insensitive): 4
- Instances of “spring2014” (case-insensitive): 5
- Instances of “spring14” (case-insensitive): 8

In terms of effort that we put in on each of these hashes, we ran our typical twenty-four hour process on each of the hash files during each of the pentests. Since we keep a dictionary of all of the previously cracked hashes, this made it easier to re-run some of the cracking efforts with the already cracked hashes as a start. We added in some additional cracking time to really go after these hashes, but that was mostly brute force effort.

I put together an hcmask file (to use with oclHashcat) of our top forty password patterns that were identified for this quarter. You can download it here – Q1Masks. I plan on keeping up with this each quarter, so check back in July to see how this mask file has changed by second quarter and how well we’ve done over the first half of the year.

For more information on how we built our GPU-enhanced password cracking box, check out this presentation we recently did at Secure360:

GPU Cracking – On The Cheap

For a general outline of our password cracking methodology check out this post:

GPU Password Cracking – Building a Better Methodology