Password Platypus Inc.

06/14/2005

Big Joe’s Plumbing

LM Hash

Good morning Big Joe, this letter is to inform you of possible vulnerabilities in your company computers involving passwords. We had not encountered the LM Hash algorithm previously, with the help of my employees and some quick research, we came to the conclusion that there exists major exploits in your site. Once having found a hash dump of your passwords there were certain concerns and weaknesses we think need to be addressed.

The LM hash algorithm is a relatively simple one, which can then reveal the passwords themselves with some handy computer work. We discovered a user within your company was using the password “armadillo” through a simple but processing heavy solution. We made our own version of the LM hash algorithm and hashed every word in the dictionary and compared every hash to the hashes of company computers. This was to ensure your employees use more complex passwords than single words with no special characters. This whole process took approximately 4-5

hours. At least they used a password longer than 7 characters as the LM hash algorithm makes it obvious when it is 7 characters or less and makes it easy for hackers to exploit that. The longer and more complex password makes brute forcing considerably harder. Adding 3-4 numbers adds an extra 999 to 9999 calculations for each word when going through a dictionary. Adding even one special character and one number anywhere in the password would increase the computing time tenfold and make it more secure against a brute force algorithm. I would encourage you to speak to your employees to make better passwords.

However most of the employees did use at least characters and numbers, which is better but still not great. At first we thought we could reverse the Lm hash process but discovered that was not possible. We did eventually make a better version of the brute force algorithm. Unfortunately the LM hash algorithm is a dead give away for its length. Based on this we were able to use this to make our algorithm more efficient. One big way was just by only comparing the first hash, as if it was the same as the hashes from the dump, we could translate it and guess the rest of the word as. The second part was finding the missing numbers or letter and numbers by using our missing letter or just

itertools to calculate every number added to the end of the word. Even with those better passwords this still was not hard to solve. Do you see why this is an issue? Even if most of your employees used characters and numbers too, even just one can compromise their account with the lack of special characters.

Anywho we will be coming over soon to replace your whole system.