(Approx. 797 words)

A Cautionary Tale

David Kretchmar, Computer Hardware Specialist

Sun City Summerlin Computer Club

<https://www.scscc.club>

dkretch \*\* gmail.com

Recently I helped a club member regain control of their Yahoo Mail account after they had been hacked by possibly one of the most sophisticated computer intrusions I have seen to date. The user became aware they had been compromised when people whose names were in the Yahoo Mail personal contact list reported receiving suspicious emails purportedly from the hacked individual's Yahoo account. No doubt those emails contained a link to malware that would have planted itself on any computer on which the infected link was opened.

The user immediately did the correct thing; they changed their Yahoo password.

Subsequently, the user could not log into their Yahoo mail account, instead getting a message that their account was locked and they would have to wait a period of time (the countdown "clock" appeared to start at one hour) before attempting to unlock it. The user encountered this lock and countdown when trying to access their account. The timer was an interesting clue since Yahoo's advertised lockout period for a user's repeated incorrect password attempts is either 12 or 24 hours, not one hour. There is a countdown clock available for Yahoo and Google advertisers that could be set to run for one hour or any preselected time.

## A Google Chrome issue?

This user was attempting to access their Yahoo Mail via their favorite browser, Google Chrome. On a hunch, I tried to access the Yahoo account using Microsoft's native internet browser, Microsoft Edge. The user manually entered their Yahoo username and the new password, and they got into their account with no problem! Yet the Yahoo account contained virtually no recent email. I then downloaded and installed the Mozilla Firefox web browser with the same results.

My suspicions turned to the Google Chrome internet browser installed on their computer. I checked the area in Chrome where browser infections are known to attack and reside: Extensions (Settings, More tools, Extensions). I turned off or deleted all potentially problematic Extensions, yet the problem persisted. I then reviewed each application installed on the system and saw nothing suspicious.

Chrome seemed to be operating fine except for the Yahoo Mail issue. This begged the question, "Why does Chrome present problems with Yahoo while two other browsers work?" The problem HAD to be with Chrome. I reset the Chrome browser and deleted cached data, but the problem persisted.

I deleted the Chrome browser, restarted the computer, then downloaded and reinstalled Chrome. The same problem persisted. That pesky timer seemed to continue its countdown, and since I had been working on the issue for almost an hour, the lockout appeared to be about to expire. When the countdown clock dropped to less than a minute, I continued to attempt to log in continuously, finally getting Yahoo to accept the user's login and the new password, and the problem was solved. I had hit the program precisely when the lockout ended before the hacker or hacking program could kick in.

Even after accessing the Yahoo Mail account, the inbox was empty. I sent an email from that Yahoo account to that same account, and it seemed to send OK but never appeared in the inbox. Yet it appeared as sent mail. I checked to filter settings on Yahoo Mail and saw that any mail containing the Yahoo email address of the affected account, including every email going into that account, was being diverted to Trash. Removing that filter was an easy fix for the rest of the problem.

## Conclusions and Recommendations

The malware that caused the problem was probably accessed via a link in an email from a trusted friend. This is how most malware is spread. Remember, friends of the club member received an email from the club member that no doubt contained the same malicious link.

To prevent email account lockouts, a user should limit the number of times they try to enter a password. If an account holder gets a "bad username or password" message 2 or 3 times, they should use the "Forgot Password" feature to reset the password. The password is virtually always the problem with email accounts since we keep the same username (email address) all our lives.

Consider using a password manager like the good one built into Google Chrome. This will make it easier to use strong passwords that are almost impossible to hack, as well as make your life easier when you log in to sites. Also, a "keyboard logger" that records keystrokes cannot capture passwords.

Don't count on antivirus software to protect you from hacks. The hacked user discussed in this article was running Malwarebytes Pro and Windows Security, two of the best PC defenses available today.

