All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Return of the telnet return

Some years back, I became concerned about the use of terminal emulators in telnet, ssh, and other related sessions. It seems that by returning byte sequences to the terminal emulator you could set the colors and other parameters so as to not display what was being done, then send escape sequences to cause the terminal emulator to issues character sequences as if typed by the user, then re-enable visualization. The net effect is that a remote host can take control over the user's session to it, causing arbitrary command execution by the terminal emulator on behalf of the user without the user ever knowing what took place.

The telnet return

I call this the telnet return because the returned content from a telnet session is used to attack the initiator of the session. Unlike so many attacks we hear about commonly, this is a case of a seemingly minimal trusted program we rely on for reaching out in a safe manner (e.g., over an encrypted session) being used against the originator of the action.

Return of the return

In the last few weeks, I have started to hear rumor then more complete descriptions of exploitation of similar trusted programs for attacking a wide range of remote control functions. This is a bad thing...

In truth, the days of this being a concern had left my immediate stream of consciousness. While it's somewhere in the long list of attack mechanisms, hidden within some larger category no doubt, the return of this returned content attack methodology reminded me of the days long gone when we worried about some of the subtleties rather than just listening to all the ridiculous foolishness of bad programmers making silly mistakes.

Back to the future again

It seems that, after a long wait, those launching attacks are returning to the roots of trust in the systems and methods we use to operate systems. This brings mixed feelings to my mind. I am saddened that humanity hasn't moved on from the desire to harm each other by launching attacks on computers, but this is likely to remain the case for as long as people are people. On the other hand, I am interested to see that threats are starting to recall or recreate the notions that have existed for a very long time. The old ways recognized the fundamentals to a far greater extent than is commonly acknowledged today, and even though we haven't really worked to solve the well known problems of old, at least defenders are starting to notice them when they happen. For years these sorts of attacks went largely unnoticed even when they were openly published and discussed. But apparently this is changing.

Summary

Attackers are starting to, in a more obvious fashion than recently, use returns to previously trusted initiating programs and protocols to exploit the initiator. Hopefully, this time defenders will take notice and start to think through what they do in more depth than we have lately. But I have always been an optimist...

Copyright(c) Fred Cohen, 2013 - All Rights Reserved