

All testing for Sniffer was executed on Windows 7 x86. At present it is not compatible with x64 version. We recommend further efforts to port the code for support for 64-bit processes, enhance detection of multiprocessing / sandboxing, and determine remote module addresses.

All testing during this period was focused on capturing web credentials and FTP credentials from Internet Explorer 8. Future efforts should focus on hooking the remaining functions and testing SMTP and POP3 credential stealing. Further research may be necessary to determine if it is possible to steal proxy credentials.

In testing, hooking Ws2_32!send and Ws2_32!recv was proven to be ineffective in most cases as the data was already encrypted, hashed, or obfuscated in some way. Examples have been provided of the logging that was done when logging into an FTP server and Gmail. While Gmail was captured, it is believed that other threads / processes are spawned as needed when communicating with the remote FTP server.

*Please note that personal Gmail credentials were used and that the results presented here should not be submitted for password cracking.