A recent Federal Government announcement from the US Cert Organization (working with the the Department of Homeland Security and the U. S. Secret Service) raises serious concerns related to recent massive credit card compromises. Basically, vulnerabilities in Remote Access software, from IBM, Apple and other vendors, can be exploited to gain access to user's desktops and laptops. After user machines have been compromised, they can be used to install the Backoff malware on Point of Sale (POS) appliances (e.g, card swipe terminals in stores). Once installed, this malware captures and returns financial information such as names and credit care information, including the 3-digit security code on the back of the card, to the criminals.

The attacks that are reported in the media are centered on the corruption of POS machines which makes sense since this is where financial information is collected. For example: http://www.pcmag.com/article2/0,2817,2461779,00.asp?kc=PCRSS03069TX1K0001121).

However, this method of attack could also be used to install malware similar to Backoff in UI applications. One such application where useful information is collected is an initial claims filings where names, SSNs, addresses and (possibly) bank account information can be found.

At the present time, Anti/Virus (A/V) software is not effective at detecting this attack. However, major A/V vendors are aware of the problem and patches should be installed as soon as they become available. It is possible to determine whether the Backoff Malware is installed. Additional technical details, including methods to detect whether compromise has occurred can be found in the government report found at: http://www.us-cert.gov/sites/default/files/publications/BackoffPointOfSaleMalware.pdf