From: Andy Derrick
Posted At: Tuesday, April 06, 2004 2:55 PM
Posted To: spywareworkshop2004
Conversation: Input for conferance consideration
Subject: Input for conferance consideration

As an affiliate marketer whos work is undermined by many of these applications and as a consumer who has been dupped by companies claiming my internet connection speeds would be increased with the use of their product (NOT), I take a strong position against these type of applications.

While consumers should be aware of what they agree to, many internet users simply click on "Accept the terms" instead of really reading the fine print. My request for consideration revolves largely around this issue. Consumer education in my opinion will a key component of limiting the damage done from these applications. I would propose that any application that fits a description of spyware or theftware be required to have it's own installation procedure and that the product be clearly labeled for consumers to consider before installation of the program.
My own poll of asking users found to be infected with parasites shows:
*) 61% never knew the program was installed
*) 16% were unaware of issues
*) 8% said they would unistall
*) 12% said they would not be uninstaling
*) 3% thought my notification was just more popup crap.

These results indicate a serious problem in my opinion. Many of these aplications are installed as an add on to some "freebe application" with a broad reaching usually non specific implied consent of use. It appears to me that many of the folks pushing these freebe applications are becoming more and more of a front for distribution of these applications as well.

Free software and bundled applications can provide value to the consumer but when schemes are put in place to maniupulate the system and the consumer by them "accepting terms of agreements" that gives applications the right to use the persons computer resources for their own need as well as installing and unistalling software without explicit consent from the consumer then things have obviously gone to far in my opinion.

Many of these applications do not just invade the privacy of consumers, they effect big businesses as well. The information obtained is used to either directly harrass the consumer while they surf issuing popups, is also sold to others and is used for spamming purposes and in components where contextual advertising and BHO's are involved, even allows direct targeting of trademark names, web site domain names and specific copyrighted text that someone has worked to provide to be easily undermined and taken advantage of. It seems that these companies say they provide a valuable service to consumers and businesses that utilize their servive but on the other hand, you have consumers complaining, big businesses complaining and lawsuits being filed and the only one who really benefits - is the provider of a crappy application that steals from others work and harrasses consumers usually to no end.

Many of these applications are the eqivalent of driving to work with a rolling billboard attached to your windshield that not only displays adware but can change the course of your driving and forceably pull your car into the shop of whoever the billboard desires. Most people think they are just getting somehting for free and have no comprehension of the impact from using the so called free service.

Adding in that many of these applications have no unistallation procedures or are very difficult to "fully uninstall" adds further complications. Components that utilize BHO's also offer further issues in that "they constantly run" and have been shown to be a major contributor towards a PC's stability and negatively effecting performance of consumers PC's. "Complete application removal" via uninstall procedure should be mandatory for these applications with penalties that can be enforced for the failure to completely uninstall an application.

These are some serious issues and I'm glad to see the FTC getting involved in looking more closely at these applications and considering the damage they do to both consumers and businesses. I can only hope that swift actions will be taken to protect the many consumers and businesses that are being negatively effected by these applications.

In closing I only want to add one more thing and that surrounds the basic premise that these companents provide a valuable service. I'm reminding of this artical (**http://www.clickz.com/experts/crm/analyze_data/article.php/1547791**) which discusses a business model that is basically - "pay me to not kill you". As an active affiliate marketer, I've seen this plan clearly implemented by these applications to in essence almost force the use of their service. By using the service, your site can be eliminated from targeting by your competitors, by not using the service you are fair game for people to target your business and its trademarks (in what I perceieve as more than unfair). I have seen merchants drop relationships with parasites and claim they will be no longer doing business with them only to be so agressivley targeted ! they turned tail and rejoined with the parasites to eliminate the targeting.

These applications should be allowed to openly interfere in someone business to the point you have to pay them to not kill you. Businesses having to pay mobsters for protection was seen as a threat that would effectivley limit growth of commerce a long time ago and laws were put in place accordingly. It's high time the FTC and the government take steps to protect consumer interest and online commerce where these aplications predominently exist as well.

I appreciate your consideration in these matters and hope that you act swiftly in regard to the ongoing damages that are done on behalf of these applications.

-- Andy Derrick --