Same R-73eN, who originally reported WinRAR SFX archives vulnerability, which is neither WinRAR nor SFX vulnerability, informed us about his findings on WinRAR registration reminder window security.

Trial WinRAR version displays a registration reminder window, which can include HTML code received through http from our and our partner trusted sites. According to R-73eN, if local user network is compromised, so a malicious man in the middle can modify contents of web pages opened by users, if MS Internet Explorer is compromised and contains unpatched security holes like MS14-064, it is possible for a malicious person to inject a harmful code to WinRAR registration reminder window.

So such attack requires two conditions:

1. Completely compromised local network, when somebody can intercept http pages opened by users and send any malicious contents to their browsers instead.
2. Internet Explorer without security patches vulnerable to malicious pages.

We consider such hypothetical situation as a local network and browser vulnerabilities. If both network and browser are compromised, it is enough for user to open any http page in a browser or in any application utilizing http browser components to be attacked and it is only a matter of time until it happens. We can argue about http vs https security here, but as long as http protocol is in wide use and not deprecated, its security should be provided on a lower level than applications utilizing http engine provided by system. Necessary steps can include DNSSEC, ARP spoofing detection and prevention, latest security patches.

We would like to publish this information to our users in advance of another possible wave of mass media publications blaming WinRAR for network security issues or system vulnerabilities patched a long time ago.