YGN ETHICAL HACKER GROUP

Article

NEXT-GENERATION PHISHING ATTACK

By

d0ubl3_h3lix

May 13, 2006

Nowadays all advanced web sites such as Google, Yahoo allow us to use their web services APIs. The notable example is G-Lite, which is not an official Google mail for embedded systems. G-Lite uses Google APIs to let us use mobile version of Gmail.

Subsequently later, almost all community/social networking sites come to use service APIs to invite our contacts without having to open our mailboxes and send each contact.

While this seems pretty much convenient to users, bad guys use the method to bulk steal users account information. No technical hacking skills. No need to hack Google or Yahoo servers. After they gain your account information, they passively sneak a look into your daily mails for sensitive information. They sell your information to third parties. They even have tools to automate such malicious actions.

General public are always lack of security knowledge. They simply tend to fill in their mail account information. Their accounts are then compromised without their knowledge.

This is a serious risk. This is a next-generation kind of phishing attack. Microsoft IE 7 phishing filter does not work in this case. This kind of compromise bypasses all phishing scanners.

The only way to protect is not to believe any sites that ask your account information. Who can you believe in this world? No one is to be trusted. If you are a network administrator, please educate your users about this phishing risk. If you are a webmaster, please do not develop this kind of implementation. Even if you do not steal users' credentials, bad guys inject a Trojan code that passively steals your users' account information via your developed implementation.

To be secure, every security advice should be followed. If not, this opens doors for attackers. Attackers are always thinking how to attack and bypass security measures.