Router compromise, rogue remote control? Easy, says ISE

April 21 2013, by Nancy Owano

Belkin N900 router

(Phys.org) —Router hacking is joining the ranks of computer security headaches, where the wireless router becomes the key target for those seeking to trespass into someone else's network. The remote attacker can take full control of the router's settings or just bypass authentication and takes control. The attacker is free to modify traffic as it enters and leaves the network. Wrote Michael Mimoso in *Threatpost*, from Kasperksy Lab, "Hackers love to attack Java. Why? Well, not only because it is full of holes, but because it's everywhere, embedded on endpoints, Web browsers, mobile devices and more. The same goes for attacking wireless routers; they're buggy and they're everywhere."

Earlier this week, that turned out to be more than a quip as, beyond Kasperksy Lab, other researchers exposed critical security vulnerabilities in small office and home office (SOHO) routers and wireless access points. The research was from Baltimore, Maryland-based Independent Security Evaluators. Their key findings: All of the 13 routers they looked at can be taken over from the local network (four never requiring an active management session) and 11 of the 13 can be taken over from the WAN (two never requiring an active management session).

Actually, there is a another important takeaway from their research: The wireless router hacking vulnerabilities they examined do not take a pile of expertise. "Our research indicates that a moderately skilled adversary with LAN or WLAN access can exploit all thirteen routers," they said. But while attackers may not need esoteric skills to break into routers, the ISE experts said the average end user can do little to fully mitigate such attacks."Successful mitigation often requires a level of sophistication and skill beyond that of the average user (and beyond that of the most likely victims)."

ISE's team said the vendors of these networking devices should be in the front of the line for mitigation actions. Actions they can take include preparing firmware upgrades that address the issues, instructing their

registered users how to upgrade device firmware; be timely in the issue and customer notification of patches; and design a method for automatic firmware updates with the opportunity for users to opt out; and perform regular security audits to ensure devices are as hardened as possible.

ISE has also announced its future plans toward focusing on SOHO routers. All signs are that they will stay on the case. "Six months after releasing the advisories for the 13 routers, ISE will upgrade the firmware on all 13 routers and perform a reassessment to determine what—if any—impact deeper scrutiny from the security community has brought to the SOHO router industry." According to ISE, its next study may include more than the 13 routers seen so far.

This research was conducted by Jacob Holcomb and directed by Stephen Bono and Sam Small. Jacob Thompson, Kedy Liu, Jad Khalil, and Vincent Faires also contributed.

More information: securityevaluators.com/content …oho_router_hacks.jsp