WARREN COMMUNICATIONS NEWS Telecom & Media Intelligence www.warren-news.com

WARREN'S Washington Internet Daily

Covering Legislative, Regulatory and Judicial News Affecting Internet Business. From the Publishers of Communications Daily.

FRIDAY, OCTOBER 29, 2010

Cyberthreats in Wireless, Now Small, Seen as Soon Rivaling Those Against PCs

SANTA CLARA, Calif. — All signs point to spam and malware becoming in the next few years threats in wireless comparable to what they are in the PC world, an officer of an industry security group led by carriers said Thursday. Economics have held down abuse in wireless, but that is changing rapidly with handsets spreading everywhere and financial transactions over them booming, greatly increasing the value of stealing information from them and hijacking them, said Alex Bobotek, co-vice chairman of the Message Anti-Abuse Working Group.

Conditions are becoming "ripe for massive abuse," Bobotek said. And the wireless special interest group of his organization is growing, he said at MobiCASE, a mobile computing, applications and systems conference of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.

Online banks in eastern Europe have had to add second layers of authentication because a mobile trojan delivering a Zeus keylogger was undermining mobile transactions, said Bobotek, of AT&T Labs. About one in 1,000 SMS messages represents abuse of mobile origin, he said, a figure high enough to "be a call to action" against a "problem ahead."

It's "hard to say there's a hockey stick" in the growth curve of mobile malware, but Kaspersky Labs reported that mobile malware signatures rose to 1,400 the second half of 2009 from 200 two years earlier, Bobotek said. The numbers don't suggest "mayhem," but "this is nothing to ignore, either," he said. Certainly within five years, spam and malware will be problems in wireless like they've been in Windows PCs, which have drawn much more activity because they've presented a bigger target with more valuable information, Bobotek said.

Spammers and thieves involved in mobile are "so much smarter" than they were a few years ago, Bobotek said. "There's more core evil and technical competence in the attacks today." A sophisticated online cyberabuse marketplace of organized criminals like the one for PCs is starting to develop in mobile, he said. In the spring, an RFP was put out in an Internet forum for the development of malware to divert SMS messages to specified phone numbers, to bleed bank accounts, Bobotek said, and "in September we saw it out in the wild: There's a Symbian trojan." This is "very troubling," because it shows an "extremely sophisticated criminal organization" clearly connected to mobile malware, he said.

Meanwhile, antivirus software is used little in wireless and it isn't available for some products, Bobotek said. Abusers can have a field day even if mass attacks work only with mobile users with low intelligence

and mental disabilities, he said.

The threat is suggested by Glavmed.com, also known as "Canadian pharmacy," a "huge criminal organization shipping effective but counterfeit drugs" that recently disbanded mysteriously, Bobotek said. It had more than $150 million in annual revenue and advertised using affiliates who were paid 40 percent commissions and sent out

2.5 billion spam messages daily, he said. The group thrived on average revenue of 8 thousandths of a cent a message, Bobotek said.

Europe has a problem with what are called SIM boxes, which allow each of many SIM cards acquired to send out few enough messages to "fly under the radar" of carrier defenses, Bobotek said. The method, involving mainly prepaid SIMs, is used mostly for roaming fraud, but it's starting to be used to rip off mobile users, he said. "I think we're going to be hearing more about SIM boxes."

The worst problem last year was phishing using an e-mail-to-SMS technique known as smishing, Bobotek said. "The business case here is so strong," he said. Stealing $1,000 from 1 percent of a vast group of users provides "a lot of return," Bobotek said, using hypothetical numbers. "The attacks with the strongest business cases are going to linger," he said. "They're the hardest." — *Louis Trager*