# Russia home to text message fraud "cottage industry"

August 2 2013

Researchers have discovered that bilking people by infecting Android mobile phones with viruses has become a cottage industry in Russia in a criminal model that could be replicated elsewhere. While the text-messaging malware industry appeared centered in Russia, the model could be duplicated in other countries where conditions allow, according to Lookout Mobile Security.

Researchers have discovered that bilking people by infecting Android mobile phones with viruses has become a cottage industry in Russia in a criminal model that could be replicated elsewhere.

Members of Lookout Mobile Security were at the infamous Def Con hacker gathering in Las Vegas on Friday to share what they uncovered about a text-messaging fraud operation they dubbed "Dragon Lady" in reference to Cold War-era US military reconnaissance aircrafts.

"The mobile malware trade in Russia is highly organized and profitable," Lookout said, referring to malicious software designed to infect smartphones.

"We recently investigated a veritable industry of malware businesses with startup-like behaviors."

Businesses referred to as 'Malware HQs' accounted for more than half the overall mobile malware detections by Lookout during the first six months of this year, according to researcher Ryan Smith.

Malware HQs openly recruit 'affiliates' that could be anyone and provide simple do-it-yourself tools to distribute viruses with tactics such as booby-trapped websites or Twitter posts.

Once on smartphones, viruses fire off premium text messages behind the scenes, with HQs getting the money and sharing it with affiliates who hooked the victims.

Lookout discovered that some HQs promote playful competition between affiliates with websites that show rankings and promise prizes for top performers.

"We've seen evidence that these affiliate marketers have earned between $700 a month to $12,000 a month from these scams," Smith said in a report summarizing Lookout's findings.

He estimated that there are thousands of individual distributors and

potentially tens of thousands of affiliate websites promoting custom SMS malware.

"Malware HQs handle the tough stuff like releasing new Android code and configurations every two weeks, malware hosting, shortcode registration, and marketing campaign management tools," Smith said in his summary.

"Like any other large business, Malware HQ organizations provide customer support, post regular newsletters, report downtime or new features, and even run regular contests to keep their affiliates engaged and motivated."

Those falling prey to the scam were typically Russian speaking Android phone users searching online for free games, applications, music, videos or pornography, according to Lookout.

Pages rigged with malware are designed to reject visits from countries not targeted by the crooks, who prefer victims in places where fees for premium text messages are paid immediately instead of through billing by telecom service providers.

While the text-messaging malware industry appeared centered in Russia, the model could be duplicated in other countries where conditions allow, according to Lookout. gc/rcw