

Russian organized crime, Russian hacking, and US. security

Phil Williams

Computer intrusions extend from cyber-vandalism and the defacement of web sites at one end of the spectrum to cyber-war and massive attacks on critical infrastructure at the other. Located somewhere between the teenage hackers and national information warriors at the extremes, however, is a variety of other threats including cyber-terrorism and cyber-crime. While the threat from terrorists has been given considerable coverage, that from organized crime has attracted far less attention. Yet this threats is global in nature reflecting both the globalization of computerized information systems and the pervasiveness of organized crime. Indeed, there are indicators of a growing overlap between organized crime and cyber-crime with some criminal organizations diversifying their activities into an area that will become increasingly lucrative as e-commerce expands.

Nowhere is this trend more obvious than in Russia. In 1994 a young Russian hacker in St. Petersburg broke into the Citibank computer system in Boston and stole \$10 million. All but \$400,000 was eventually recovered. Nevertheless, there has been considerable speculation that organized crime was behind the incident. Since then a growing number of intrusions suggests that Russian criminals are either recruiting or coercing hackers into breaking into Western systems. Whether this is for purely criminal purposes, for industrial espionage, or for state espionage is not always entirely clear. Whatever the case, the United States appears to be the major target. Several major intrusions into US systems have been traced back to Russia including those that became the subject of Moonlight Maze and the well-publicized Microsoft hack. According to some reports, the FBI believes that 40 companies in 20 states have been identified as targets of Russian organized crime groups. Activities include extortion, fraud, and theft, and it is estimated that over 1 million credit card numbers have been stolen by the groups. In some cases, computer intrusions highlighting data vulnerabilities are followed by offers to fix the security holes for a large fee; of extortion. In other cases, the stolen credit card numbers are used to perpetrate a series of frauds.

Against this background, this paper seeks to illuminate the relationship between Russian organized crime and Russian hackers. In order to do this it looks first at the political, economic, social and cultural context that might lead to some kind of fusion between Russian organized crime and Russian hackers. Second, it examines the reasons that Russian organized crime is diversifying its activities into various forms of cyber-crime. Third, it develops a typology of possible relationships between criminal organizations on the one side and Russian hackers on the other – drawing where possible on actual case studies. Fourth, it identifies the range of activities that seem likely to result from the coalescence of Russian organized crime and Russian hackers, as well as some of the likely targets and modalities of operation. Finally, it identifies both critical components and continued shortcomings of the nascent United States response to this challenge – discussing both the law enforcement component and other measures that could prove useful.