Secret Service Steps Up Its Activity against Cyber Crime

December 15, 2011

In recent testimony before the Senate Judiciary Committee, Pablo Martinez, the Secret Service's Deputy Special Agent in Charge, testified regarding recent trends in cybercrime and the efforts of the Secret Service to combat those emerging threats.

That's right, besides its responsibility to protect the President and other VIP's, the Secret Service plays a little-known role in combating cybercrime. In fact, the Secret Service currently has nearly 1,400 special agents in its Electronic Crimes Special Agent Program.

The Secret Service was the original guardian of our financial systems. That authority has been reinforced by various acts of Congress, which expanded the Secret Service's responsibility to include access device fraud, as well as concurrent jurisdiction over identity theft, computer fraud, and bank fraud.

Martinez touched upon three timely issues: the current porous legal framework, the emerging threat of syndicated cyber-criminal organizations, and the trend of criminals to focus their efforts on smaller businesses and individuals.

The current regulatory framework consists of a patchwork of overlapping and interwoven state laws, a regime with many gaps. Therefore, the Obama administration has proposed additional measures to protect consumers from identity theft and to simplify the current framework to permit easy and efficient reporting and investigations of data breaches.

Similarly, speaking in November 2011 at a conference sponsored by the Economic Crime Institute of Utica College, Keith Prewitt, the Secret Service's Deputy Director, said the Secret Services "has observed a marked increase in the quality, quantity, and complexity of cybercrimes."

"While many cybercriminals steal money and information," Prewitt said, "there are those who also seek to destroy, disrupt, and threaten the delivery of critical services."

Martinez noted in his testimony that "Secret Service investigations have shown that complex and sophisticated electronic crimes are rarely perpetrated by a lone individual."

Rather, online criminals gather in organized networks and use clearly defined roles, much like an online Mafia, in planning their criminal enterprises that predominantly consist of stealing data and selling it for a profit. In an effort to combat these online criminal syndicates, the Obama administration has proposed that computer fraud should be added as a predicate offense under the Racketeering Influenced Corrupt Organizations Act (RICO).

The existence of organized syndicates in the cyber crime world increases both the complexity of investigating these cases and the potential damages caused to businesses and individuals. For instance, there are now illicit Internet carding portals, or “carding forums,” that allow criminals to trade their stolen personal financial data and to traffic their stolen information internationally.

Originally, cyber criminals would attempt to steal information from larger companies because they could obtain a tremendous amount of information with a single breach of the security system. However, as larger companies have adopted more sophisticated protections against cyber crimes, cyber criminals have likewise adapted and are now more focused on small and medium-sized businesses.

These smaller businesses often lack the resources to employ the sophisticated protections deployed by larger businesses. This makes them easier targets. For example, a study of trends of cyber crime has shown that cyber criminals are now focused on Point of Sale (POS) systems and compromising financial accounts, which later leads to subsequent fraudulent transactions on those accounts.

While there were more data breaches in 2010 than in recent years, the amount of compromised data actually decreased because the average size of the compromised databases was smaller. The Secret Service and other agencies are continuing to try to adapt as the criminals and their behavior are changing.

There is also the possibility that an amendment providing a private right action to pursue relief for victims of computer fraud will be added to existing federal law on computer fraud. We will continue to monitor these developments.

Crime in the Suites is authored by the Ifrah Law Firm, a Washington DC-based law firm specializing in the defense of government investigations and litigation. Our client base spans many regulated industries, particularly e-business, e-commerce, government contracts, gaming and healthcare.

The commentary and cases included in this blog are contributed by Jeff Ifrah and firm associates Rachel Hirsch, Jeff Hamlin, Steven Eichorn and Sarah Coffey. These posts are edited by Jeff Ifrah and Jonathan Groner, the former managing editor of the Legal Times. We look forward to hearing your thoughts and comments!