U.S Department of Homeland Security

United States Secret Service

PRESS RELEASE

May 14, 2008
Contact: (202) 406-5708
GPA 10-08

ADDITIONAL INDICTMENT ANNOUNCED IN SECRET SERVICE NETWORK INTRUSION INVESTIGATION

(Washington, D.C.) – An indictment returned today in New York adds new charges of wire fraud conspiracy, wire fraud, conspiracy to possess unauthorized access devices, access device fraud, aggravated identity theft, conspiracy to commit computer fraud, computer fraud and counts of interception of electronic communications to those already returned in a high-profile cyber investigation by the United States Secret Service.

The 27-count indictment returned in Central Islip, N.Y., charges Albert Gonzalez of Miami with illegally accessing the computer systems of a national restaurant chain and stealing credit and debit card numbers from that system. Today's indictment supersedes a one-count complaint against Gonzalez unsealed earlier this week. The original indictment, returned on March 12, 2008, and unsealed on Monday, May 12, charges Maksym Yastremskiy, of Kharkov, Ukraine, and Aleksandr Suvorov, of Sillamae, Estonia, with the same criminal violations.

In September 2007, corporate officials with Dave & Busters, Inc. (D&B) notified the Secret Service of a network intrusion targeting payment terminals at 11 different D&B restaurants located throughout the United States. The suspects were able to compromise customer credit card data that was subsequently resold for use in additional credit card fraud schemes worldwide. An extensive investigation involving multiple U.S. Secret Service offices nationwide definitively linked the three suspects to the intrusion.

"This case demonstrates the global nature of cyber crime. With internet capabilities expanding rapidly around the globe, the reach and potential for criminal intrusion are greater than ever," said Secret Service Assistant Director Michael Stenger. "Cooperation among investigators throughout the Secret Service and our domestic and international law enforcement partners, has led to these significant arrests. By combining our investigative resources, we can transcend borders and more effectively address evolving criminal methods."

-more-

The indictment alleges that in or about May 2007, Yastremskiy and Suvorov gained unauthorized access to D&B cash register terminals and installed at each restaurant a "packet sniffer," a malicious piece of computer code designed by Gonzalez to capture communications between two or more computer systems on a single network. The packet sniffer was configured to capture “Track 2” data as it moved from the restaurant's point-of-sale server through the computer system at the company's corporate headquarters to the data processor's computer system. At one restaurant location, the packet sniffer captured data for approximately 5,000 credit and debit cards, eventually causing losses of at least $600,000 to the financial institutions that issued the credit and debit cards.

Acting on information provided by the U.S. Secret Service, Turkish officials arrested Yastremskiy in Turkey in July 2007. He remains in jail on potential violations of Turkish law. A formal request for extradition of Yastremskiy to the United States has been made to the Turkish government. At the request of the U.S. Secret Service, Suvorov was arrested in March 2008 by German officials while visiting that country. He remains in jail in Germany, pending German action on a formal U.S. extradition request. U.S. Secret Service officials arrested Gonzalez in Miami in May 2008. Gonzalez was previously arrested by the Secret Service in 2003 for access device fraud.

The United States Secret Service was originally founded in 1865 for the purpose of suppressing the counterfeiting of U. S. currency. Over the years it has grown into one of the premier law enforcement organizations charged with investigating financial crimes. The Secret Service has taken a lead role in the developing area of cyber crime, establishing working partnerships in both the law enforcement and business communities to address such issues as protection of critical infrastructure, internet intrusions and associated fraud.

###

EDITOR’S NOTE: For questions concerning this release, please contact the United States Secret Service Office of Government and Public Affairs at 202-406-5708.