

The following information may be useful regarding law enforcement responses to cyber crime.

Serious Nature of Transnational Cyber Crime

As the world grows more dependent on information sharing technology, keeping these systems viable and secure has become an increasingly urgent national priority. Our increased reliance on technology has created an irresistible target for criminal activity; this has transformed law enforcement's cyber mission to an undertaking which combats cyber crime not only within the borders of the U.S. but also cyber crime which originates transnationally and targets our infrastructure. To this end, the U.S. Government is forming key alliances with foreign law enforcement partners to jointly investigate cyber crimes that affect the U.S. and our allies across the globe.

Currently, the largest source of transnational cyber crime emanates from Eastern Europe. These hackers and programmers are the world leaders in creating and exporting the malicious computer code used to exploit the world's financial infrastructure and to compromise the infrastructure of the Internet itself. Annual losses to U.S. financial institutions are in the hundreds of millions of dollars and are growing exponentially.

Law enforcement recognizes that the cyber crime threat is not limited to the value of the data that might be compromised, stolen, or altered, but in the asymmetrical nature of such an attack. The damage that results from a cyber attack is much greater than the resources of time, money, knowledge, and planning needed to accomplish the attack. This asymmetry is aided by the anonymity, openness, connectivity, and speed of the Internet. Because of this, cyber crime can take place anonymously and rapidly from anywhere and affect anyone to a devastating degree. Because of the unique nature of this threat, the U.S. Government has sought innovative ways to protect U.S. citizens from these crimes.

To combat this crime problem, the FBI and the United States Secret Service have developed close working relationships with law enforcement partners within high value targets and with allies who are also victims of transnational cyber crime. U.S. law enforcement, in conjunction with key international partners, is singularly focused on preventing, investigating, and prosecuting violations of U.S. law. Since September 2007, it has conducted significant cyber investigations arrests, and prosecutions, including:

- the arrest of individuals in Hong Kong responsible for reaping high profits by hijacking the online brokerage accounts of unwitting U.S. investors;
- the extradition and prosecution of a Ukrainian national responsible for running a global identity theft ring with ties to Russian organized crime that stole and bartered immense quantities of personally identifiable information; and
- the extradition and prosecution of an Estonian national responsible for intruding into multiple U.S. restaurant and retail store chains and extracting data for hundreds of thousands of credit card accounts through the use of custom written malware.

Targeting of U.S. Financial Institutions

Over the past year, there has been a considerable spike in cyber attacks against the financial services and the online retail industry. There are a number of actions a firm can take in order to prevent or thwart the specific attacks and techniques used by these intruders. The significant characteristics of these highly successful attacks included initial use of an attack technique known as Structured Query Language (SQL) injection and the targeting of databases, Hardware Security Modules (HSMs), and processing applications to obtain credit card data or brute-force ATM PINs.

As a result of FBI and U.S. Secret Service investigations into these particularly damaging intrusions, the U.S. Government has identified a series of preventive measures financial institutions and other potential victims can employ to avoid becoming victims of this particular scheme. These measures were promulgated via US-CERT, the FS-ISAC, the Internet Crime Complaint Center (IC3), InfraGard and the USSS Electronic Crimes Task Forces (ECTFs). This information is still available on the IC3 web site (<http://www.ic3.gov/media/2008/081215.aspx>), and on various Internet sites, including Automated Merchants Systems, Inc. (<http://automatedmerchant.com/m/1000/1570/files/20090105-alert-ussf-fbi-advisory.pdf>). More information on InfraGard is available at www.InfraGard.net. More information on the ECTFs is available at <https://www2.einformation.ussf.gov/elib/welcome.nsf/Home>).