Fighting Russian Cybercrime Mobsters: Report from the Trenches

Online crime today is a huge business. Reported losses to the FBI in 2008 by US consumers were recorded at almost $265 million from over 275,000 individual complaints[1]. Yet, this estimate doesn't even begin to address the likely hundreds of millions more in annual worldwide consumer losses that either go completed unreported or get lost in the bureaucratic jurisdictional chaos that is our current national and international cyber law enforcement institutional structure. It also doesn't account for the billions more that are absorbed each year by financial institutions, retailers and other corporate organizations and undoubtedly passed on to consumers in the way of additional fees and higher prices.

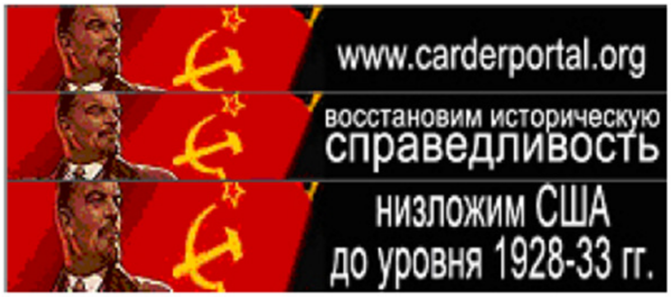
YEAR	COMPLAINTS RECEIVED	US DOLLAR LOSS
2008	275,284	$265 million
2007	206,884	$239.09 million
2006	207,492	$198.44 million
2005	231,493	$183.12 million
2004	207,449	$68.4 million

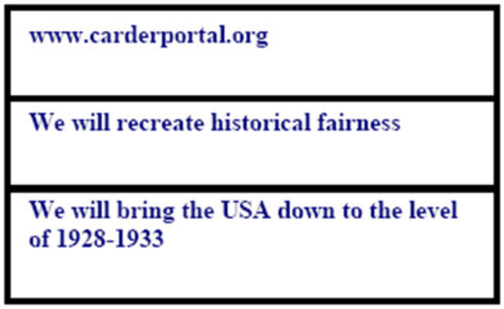
The rate of increase in cybercrime losses measured through complaints received by FBI's Internet Crimes Complaint Center (IC3)

Much of this crime today is transnational, organized, and highly secretive, with major criminal groups operating in over 30 countries spread across 6 continents (no cybercrime has been detected yet to originate from Antarctica). However, not unlike the Sicilian Mafia that got its start in lawless 19th century Sicily, or Al Queda, which organized and became a potent and lethal force in war-savaged and ungoverned 1980s Afghanistan, the most sophisticated

[1] DoJ/IC3 2008 Internet Crime Report. http://www.ic3.gov/media/annualreport/2008_ic3report.pdf

cybercriminal organizations emerged in the last 1990s and early 2000s in Eastern Europe and, particularly, in countries tracing their history to the former Republics of the Soviet Union. In those places at that time you could find all the necessary conditions for the emerging of an effective, organized and dangerous criminal activity operating in cyber space: severe lacking of laws and investigative and prosecutorial focus on cybercrime, highly educated and technologically empowered segments of population with the capability to conduct sophisticated criminal operations, and relatively limited economic opportunity to make an honest living comparable to what could be earned through illicit means. This volatile combination contributed to a tide of individuals from Eastern Europe, who, feeling confident in their safety and impunity from pursuit by domestic or international law enforcement, joined by the thousands the various online criminal enterprises that started to prop up in early 2000s. In addition to the substantial financial motivation, many of these criminals successfully suppress any ethical anxieties they may feel about stealing someone else's entire life savings by hiding behind extreme nationalist justifications. Anti-western and moral relativist expressions are all too common among members of this community: statements along the lines of "They deserve what they are getting after what they've done to us" and "We are taking back what's rightfully ours" can be easily found on Eastern European cybercrime forums in posts bragging about the successes of their latest enterprising schemes.


www.carderportal.org
восстановим историческую справедливость
низложим США до уровня 1928-33 гг.



www.carderportal.org
We will recreate historical fairness
We will bring the USA down to the level of 1928-1933

Banner Ad from CarderPortal.org from September 6, 2004

Roman Vega

One of the first individuals to create a sustainable business model based on cybercrime was a certain Roman Vega of Ukraine, a.k.a. Roman Stepanenko, a.k.a. "BOA" (now known as inmate #59198-004 in the Federal Bureau of Prisons), who started a website called Boa Factory (http://www.boafactory.com) in the late 1990s. Boa Factory was a one-stop clearing house for buying and selling virtually all assets produced by financially-motivated online criminal activity of that time. One could get plastic cards, raw "dumps" (magnetic stripe data from bank and credit cards), traveler's checks and even counterfeit passports. Vega was eventually arrested while vacationing in Cyprus (a popular European destination for Russian and Ukrainian tourists) in June 2004, extradited to California and charged with a 40-count indictment of wire fraud and trafficking in stolen credit cards. Another indictment in New York for access device fraud and money laundering followed 2 years later and convictions eventually secured.

Brooklyn Metropolitan Detection Center:
Roman Vladimir Vega's current place of residence

Eventually, Boa Factory evolved into another organization called CarderPlanet (http: //www.carderplanet.com), which was founded in May 2001 and operated through August 2004, at which point it was shut down by senior members of the group following high profile arrests of key members earlier that summer (including Boa). CarderPlanet was reportedly organized following a meeting at a restaurant in a Ukranian port city of Odessa between Roman Vega, his protege, individual going by the nickname 'Script', and several others. Together, they became the administrators (or 'Capo di Capi' as they chose to call themselves) of the forum and evolved it into a mature marketplace for purchase, review and distribution of cybercriminals goods and services, as well as providing tutorials for new members looking to get a quick 'Getting Started' guide to online fraud schemes.

Dmitry Golubov prior to his arrest

US Postal Inspection Service (USPIS), in conjuction with Ukranian internal security forces, arrested Dmitry Golubov in July 2005, who they claimed was the real individual behind the Script online persona. Golubov was charged with fraud and held in Ukranian jail through December 2005, until which time he was released by the court after several members of the Rada (Ukranian Prliament) submitted character witness testimony on his behalf. A case against him was completely dismissed some months later. After his release, Golubov organized a political

Dmitry Golubov, IPU Party Leader

organization and called the Internet Party of Ukraine (IPU: http://www.ipu.com.ua/), advertising a platform which includes fighting corruption and crime in Ukraine.

In October 2004, FBI, Secret Service and USPIS concluded "Operation Firewall", the first significant transnational cybercriminal investigation. It netted dozens of arrests, resulted in the shutdown of Shadowcrew, an English-based alternative to CarderPlanet and indirectly caused the termination of CarderPlanet itself. The success of that operation and the others that followed it, such as Operation Cardkeeper of 2006 which targeted Polish online organized crime, and DarkMarket investigation aimed at the US and Western European criminals and concluded in October 2008 with arrests of almost 60 alleged criminals, brought significant changes to the online criminal scene. A number of individuals, realizing that the situation has drastically changed, have left the 'business' and took their careers into a different direction. Those that remained, have gone underground, communicating only with trusted insiders within their organizations and resorting to encrypted communication channels.

It is easy to discount the importance of these successes, which altogether have resulted only in a few hundred arrests and even fewer number of convictions, from the tens of thousands of cybercriminals believed to be operating today. Yet, there is no convention that, in addition to the direct financial loss they have prevented and were able to recover, these law-enforcement operations have succeeded in substantially changing the landscape of the battle. No longer can criminals, even those operating in Eastern Europe, seemingly far out of reach and in perceived safety from US law enforcement, count on ability to operate with impunity and must instead constantly watch over their shoulder. As international cooperation improves and these operations become more frequent, their deterrent value will likely result in a significantly improved Internet landscape, which is more secure from online crime, in the years to come.