The Russian Cybermafia:
Boa Factory & CarderPlanet

by M. E. Kabay & Bradley Guinen

The paper written by Cadet Bradley Guinen of Norwich University for his CJ341 Cyberlaw & Cybercrime class provided the basis for this series of articles. Cadet Guinen and Mich Kabay collaborated closely in converting Guinen's essay into a series of articles for Network World Security Strategies. This second article started with a paragraph from the student's essay and has been rewritten and expanded by Mich Kabay.

* * *

At the 2009 BlackHat Conference USA< >, researchers Dmitri Alperovitch < http://www.mcafee.com/us/mcafee-labs/team/dmitri-alperovitch.aspx >, Vice President of Threat Research at McAfee, and J. Keith Mularski< https://365.rsaconference.com/community/connect/rsa-conference-usa-2009/blog/2009/04/22/interview-keith-mularski-public-policy-award-winner >, Supervisory Special Agent for the US Federal Bureau of Investigation's (FBI's) Cyber Initiative and Resource Fusion Unit < http://www.fbi.gov/news/stories/2009/march/fusion_031209 >and the National Cyber-Forensics & Training Alliance< http://www.ncfta.net/ > collaborated on a presentation entitled "Fighting Russian Cybercrime Mobsters: Report from the Trenches."< http://www.blackhat.com/presentations/bh-usa-09/ALPEROVITCH/BHUSA09-Alperovitch-RussCybercrime-PAPER.pdf > Page 3 of their report discusses Roman Vega of Ukraine, who also used the alias "Roman Stepanenko," but was more popularly known as "BOA", started a Website called boafactory.com in the late 1990's. They write,

> 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.

Another useful report that includes details of the Boa Factory and many other criminal gangs is the 56-page White Paper entitled "Cybercrime and Hacktivism" prepared by François Paget< http://fr.linkedin.com/pub/francois-paget/7/379/876 >, a Paris-based Senior Threat Researcher for McAfee and a prolific and brilliant commentator on the security scene.< http://blogs.mcafee.com/author/Francois%20Paget > On page 36 of his paper, Paget writes that "In June 2009, he [Vega] was extradited to the United States and turned over to the federal court. He is accused of embezzling more than US$2.5 million."

According to Alperovitch and Mularski, Vega/Stepanenko and several other criminals met in May 2001 at a restaurant in Odessa with a criminal calling himself "Script" and others to form a new organization called CarderPlanet. The site quickly became a bazaar for the "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."

David Munns, writing in his blog< http://blogs.creditcards.com/davidm.php > on the CreditCards.com site, has a detailed history of CarderPlanet in "The secret history of CarderPlanet.com and Dmitry Ivanovich Golubov."< http://blogs.creditcards.com/2008/05/secret-history-of-carderplanet.php > Originally written in

May 2008, the article was updated in August 2010 after "the arrest of Vladislav Anatolievich Horohorin, 27, aka 'BadB' of Moscow, Russia, one of CarderPlanet's founders. He was arrested as he boarded a Moscow-bound plane in Nice, France."< http://www.creditcards.com/credit-card-news/carderplanet-badb-data-thief-cybercriminal-arrested-1282.php > BadB, a cartoonist, posted aggressively anti-American graphics on his badb.biz carder site. He was described as one of the top five cybercriminals in the world and was indicted for "access device fraud and aggravated identity theft."< http://www.personal-finance.com/stories/vladislav-anatolievich-horohorin-charged-selling-stolen-credit-card-d >

Munns' article is full of unexpected and entertaining details of the case. Here are some highlights (lowlights?):

- "Script" launched an advertising campaign for CarderPlanet.com.
- Criminals arrested in 2004 with counterfeit credit cards claimed that "Script" was Dmitri Golubov, a "part-time student at Mechnikov University in Odessa, Ukraine…."
- CarderPlanet.com shut down in late The U.S. Secret Service, as part of "Operation Firewall," shut down that site and others in 2004,2004 but similar sites continued and grew despite crackdowns by many police forces from various countries including the USA's Secret Service in "Operation Firewall."< http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1146949_mem1,00.html >
- In July 2005, Ukrainian police arrested Golubov and found "found three computer hard drives and other electronics equipment that had been cooked in a wok" along with an electromagnetic-pulse generator designed to wipe magnetic information off disk drives.
- In December 2005, Golubov was released by a judge on the grounds that there was insufficient proof of his link to the pseudonymous "Script."
- Golubov started "a political party called the Internet Party of the Ukraine."

In a subsequent posting from May 2008, "Notes from the underground: The next generation of carders,"< http://blogs.creditcards.com/2008/05/notes-from-the-underground.php > David Munns continued his review of the credit-card fraud industry with a detailed and well-documented summary.

Next: the Russian Business Network (RBN) and the attack on RBS WorldPay.

* * *

Bradley Guinen< bguinen@norwich.edu > is due to graduate from Norwich University in 2013 with a BSc in Computer Security and Information Assurance. He is a proud member of the US Army Reserve Officer Training Corps< http://www.norwich.edu/cadets/armyrotc/index.html > at Norwich University, home of the ROTC< http://www.norwich.edu/cadets/rotcrequirements.html >.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >