The Russian Cybermafia:
RBN & the RBS WorldPay Attack

by Bradley Guinen & M. E. Kabay

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.

* * *

The Russian Business Network (RBN) is infamous for its involvement in malicious software, DDOS attacks, hacking, child pornography, and spam. Much like other Russian cybercrime syndicates the Russian Business Network had its roots in the old fashion selling hacking tools and services that could even penetrate many U.S. government systems.< http://www.bizeul.org/files/RBN_study.pdf > Since then the RBN has scaled up its operations to include the creation of a program called Black Energy, which is a tool used to control a botnet, a large group of infected computers, which in turn are used in an assault on a targeted Website to paralyze it and shut the site down.

In a report by Siobhan Gorman and Evan Perez in December 2009, the *Wall Street Journal* published claims< http://online.wsj.com/article/SB126145280820801177.html > that the FBI was "probing a computer-security breach targeting Citigroup Inc. that resulted in a theft of tens of millions of dollars by computer hackers who appear linked to a Russian cyber gang." The report implied that Black Energy was being used in the attack.< http://www.computerworld.com/s/article/9142578/Report_Russian_gang_linked_to_big_Citibank_hack >. However, within hours of publication, "Citigroup and a federal law enforcement source … refuted a claim that the bank's customers lost millions of dollars in an advanced cyber heist over the summer, leaving lingering questions over details of the alleged attack."< https://www.networkworld.com/news/2009/122209-citigroup-law-enforcement-refute-cyber.html >

Even though that particular attack turned out to be illusory, the RBN really did organize an extraordinary attack known as the RBS WorldPay< http://rbsworldpay.us/ > scam in November 2008.< http://www.networkworld.com/community/node/38366 >. Eastern European criminals were able to hack past WorldPay's sophisticated encryption system used on payroll debit cards and extract information pertaining to these cards.< http://www.justice.gov/opa/pr/2009/November/09-crm-1212.html > They used the stolen data to create hundreds of fake automated teller machine (ATM) debit cards. Then simultaneously around the world, the organized crime group used these fake ATM cards to withdraw the maximum amounts permitted. They stole about $9M dollars from more than 2,100 ATMs in over 280 cities, in countries such as the United States, Russia, Ukraine, Estonia, Italy, China, Japan, and Canada in 12 hours. A year later, eight men were indicted by a federal grand jury in Atlanta.< http://threatpost.com/en_us/blogs/us-takes-down-9-million-rbs-worldpay-hacking-ring-111009 >

In August 2010, one of the accused, Sergei Tšurikov, 26, of Tallinn, Estonia, was successfully extradited to the United States to stand trial.< http://www.justice.gov/opa/pr/2010/August/10-crm-908.html > Unfortunately, in Russia, the alleged leader of the gang involved in the scheme, Victor Pleschuk, 28, was merely given a four-year suspended sentence (probation) and ordered to pay restitution of U$8.9M to RBS WorldPay.< http://www.networkworld.com/news/2010/090810-report-rbs-worldpay-hacker-gets.html >

Readers can estimate for themselves the likelihood that Pleschuk will ever successfully repay this amount.

[Mich Kabay adds:]

In my opinion, international cybercrime will continue to grow. With many countries in the world governed by corrupt bureaucrats and jurists ready to accept bribes< http://www.oecd.org/department/0,3355,en_2649_34855_1_1_1_1_1,00.html > to overlook or even support criminal groups that bring revenue into their countries – and their personal pockets – it is unlikely that we will see a significant reduction in such activities in the foreseeable future.< http://www.scribd.com/doc/49339270/2011-EECTF-European-Cyber-Crime-Survey > And just wait until the People's Republic of China gets more heavily involved: a totalitarian country with no discernable rule of law< http://catdir.loc.gov/catdir/samples/cam033/2002073483.pdf > but with the largest population on the planet is already a significant source of enormous cyber-criminality.< http://news.techworld.com/security/8871/chinese-hacking-threat-set-to-grow/ > The cyberfraud epidemic is only going to get worse.

* * *

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/ >