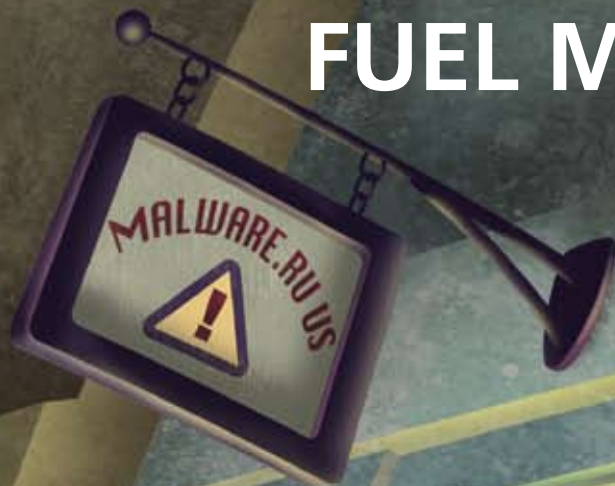


RUSSIA:
ECONOMICS,
NOT MAFIA,
FUEL MALWARE

By Dr. Igor Muttik



Many assume that the mafia and the secret police service (FSB, formerly known as KGB) must stand behind the attacks coming from Russia. But are these organizations really the prime movers? We'll answer that question in this article, but first we need to take a short look into the history of local malware development and the main forces behind it. We shall discuss current laws, as well as the successes and failures of law enforcement agencies. We shall also dive into the black market to know what is on offer and what one might expect to pay for malware, malware builders, associated tools, and the functionality they offer. Finally we'll make a few predictions about how this is likely to evolve.

A short history of malware development

The traditional focus of education in the Soviet Union was more on technical and practical sciences than on the humanities. For that reason in Russia and the other former republics of the U.S.S.R. there are many highly skilled young people with advanced knowledge of mathematics, computing, and programming. The combination of relatively low salaries, high unemployment, and wide availability of networked computers makes malware development an area that attracts quite a lot of people. Also, as in many other countries, "hackers" are perceived by the public as exceptionally clever individuals. Consequently, malware writers carry the aura of being special.

In the past Russian programmers created many sophisticated viruses. One of the most notable was a multipartite Zaraza virus (a.k.a. ЗАРАЗА), which used a novel technique of infecting disks by creating a duplicate of the io.sys file. This virus forced a redesign of anti-virus engines! Another exceptional virus—W32/Zmist—was written by a notorious, prolific, and imaginative virus writer who calls himself Z0mbie. This parasitic virus decompiles and reassembles files upon infection so that the virus is seamlessly integrated inside the host. Security researchers from all anti-virus firms unanimously agree that this technique is the hardest to detect.

In recent years financial motivation has played an increasing role in driving up the production of malware.¹ Spam and spam tools are also in demand. These areas also intertwine; for example, botnets are frequently used for spam distribution.

At the same time, there are many organizations in Russia that use low-level skills for legitimate purposes: for instance, top-notch vulnerability research (www.securitylab.ru) or widely used copy-protection technologies (<http://www.star-force.com>). The world-class software analysis toolkit IDApro (www.idapro.ru, www.idapro.com) is the leading program for reverse-engineering. Software protectors AsPack and AsProtect (www.aspack.com, www.star-force.ru) are frequently used to package commercial software. And, naturally, there are some gray sites (<http://www.wasm.ru>, www.xakep.ru) devoted to disassembling and modifying software, including an excellent resource for reverse-engineering (<http://www.cracklab.ru>). The skills used in these areas may come in very handy for malware development; a very high return on investment for computer crime could be the magnet that attracts many young, inexperienced people.

So what's stopping these young programmers from turning to crime? Let's have a look at the legal controls in this space.

A very high return on investment for computer crime could be the magnet that attracts many young, inexperienced people.

1 "Money changes everything," Sage Vol. 1, Issue 1, Page 13. http://www.mcafee.com/us/local_content/white_papers/threat_center/mcafee_sage_v11_en.pdf

Current laws

Russian laws covering crimes related to computing came into force in June 1996 (in Chapter 28 of the Criminal Code of the Russian Federation). Some amendments were made in November 2001. There are three key paragraphs, and they cover the following crimes (this is not an official translation):

- #272) Unauthorized access to computer data if that causes a loss, blocking, modification, copying, or disruption to the operation of a computer, system, or a network.
- #273) Deliberate creation of computer programs or change of existing programs if that causes a loss, blocking, modification, copying, or disruption to the operation of a computer, system, or a network. Also using and distributing corresponding programs or computer media with such programs.
- #274) Interfering with the normal operation of a computer, system, or a network by a person who has access to a computer, system, or a network that causes a loss, blocking, modification, copying, or disruption to the operation of a computer, system, or a network if this causes significant harm.

Penalties start from a mere fine or a community service, but for crimes that cause serious consequences (or if they were committed by an organized group) punishment can include imprisonment for a period of four to seven years.

In 2006, the Russian legislative body—the Duma—enacted laws protecting personal data (<http://www.akdi.ru/gd/proekt/097697GD.SHTM>) and data protection (<http://www.russianlaw.net/law/laws/t3.htm>). The former requires consent from a person for using personally identifiable information (with very few reasonable exceptions). This is very much in line with common international practice.

In July 2006 lawmakers also passed a law that requests advertisers to follow the “opt-in” model of distributing advertisements. That temporarily caused a drop in spam levels in Russia, but in about four months the volume returned to its usual level—about 80 percent spam in normal email traffic (<http://www.cnews.ru/news/top/index.shtml?2007/02/19/236529>).

As we can see, legislation is on the rise and is gradually covering the hot spots. But does it work in the area of malware production?

Successes and failures of law enforcement

There is a Russian saying that the severity of the laws is offset by the fact that it is not necessary to obey them. Thus we need to perform the acid test and check to see how these laws are applied in practice.

As with all high-technology crimes, the laws are always a bit behind current developments in their misuse. Russian computer crime laws, though, are fairly generic and were used to prosecute one spammer (<http://www.ifap.ru/eng/projects/as02.pdf>) even though the implications of spam were not in the thoughts of lawmakers when the respective laws were first enacted.

Another hacker was prosecuted—under paragraph #273—for unauthorized modifications to a computer system (www.internet-law.ru/intlaw/crime/tumen.htm), and a student was charged with running a Web site that offered about 4,000 malware samples for download.

Concerning international computer crime, a court in the Saratov region, 530 miles southeast of Moscow, has sentenced three Russian hackers to eight years in prison each, as well as a \$3,700 fine (http://www.whatreallyhappened.com/archives/cat_computersinternetsecurity.html). Their crime was attempting to extort \$4 million from world Internet companies.

Computer-based crimes frequently cross national boundaries. Sometimes the criminals do so, too. When they do, they become subject to local laws and can be apprehended and prosecuted. In August 2007, U.S. authorities reported an identity theft ring that specialized in targeting rich Americans. The head of the group was arrested in New York when he flew from Russia to the States to retrieve \$7 million in gold that he thought had been purchased with money stolen from one of his victims (<http://www.informationweek.com/security/showArticle.jhtml?articleID=201800899>).

Attacks across borders on Web servers are quite common. They are usually made to compromise the servers and to plant malware (or malicious links to malware). In one case Web administrators from several countries noticed attacks originating from the same network registered in St. Petersburg.² Such a coincidence indicates that the frequency of this activity is quite high.

At the August 2007 Internet Security Operations and Intelligence III conference, in Washington, one of my colleagues heard that the overwhelming majority of major e-crime scams appear to be linked to Russian or ex-Soviet cybercriminals.

² “Go Away, Russian Business Network!” *Dusting My Brain*. <http://dustingmybrain.com/archives/002375.html> and “More on the Russian Business Network!” *Dusting My Brain*. <http://dustingmybrain.com/archives/002379.html>

In July 2007 the Russian exploit package MPack caused massive compromises of Web servers in Italy. (You can read a nice graphical description of how this works at Symantec’s blog.³) Dealing with such attacks requires the close cooperation of lawmakers, law enforcement agencies, and ISPs across national boundaries—a monumentally difficult task.

Another serious problem that law enforcement agencies face is that finding resources and funding for computer-crime units is far from trivial. (This is a common problem all over the world.) Because the authorities are not as successful in combating computer crime as people would expect them to be, non-governmental and even international bodies have appeared to help (<http://www.crime-research.org/about/>). The Computer Crime Research Center offers a document detailing the state of computer crime laws in former Soviet republics (http://www.crime-research.org/library/Criminal_Codes.html).

A similar non-governmental organization, the Open Forum of Internet Service Providers, created a set of fair network-use rules in 2002. These were adopted as a precedent (<http://www.ofisp.org/documents/ofisp-008.html>) in confirming a court decision regarding the ISP MTU-Intel terminating Internet access for a spammer.

In July 2005 the story of how the most prolific Russian spammer—Vardan Kushnir—was killed was circulated by the media. The widespread belief that his murder was related to spam distribution collapsed after the real killers were detained in August 2005.⁴ It’s ironic, though perhaps typical of how media works, that unfounded speculations received much wider publicity than the facts that became available once the murder case was closed.

Black market price list



Figure 1: This site offers malware for sale and even asks for visitor feedback in a small poll.

If one is looking for custom-made malware, it is not difficult to find—there are even specialized Web sites that advertise such services. We also encountered several requests for malware in some forums.

Clearly, because there are buyers and sellers, there is a market. On this same site in Figure 1 we found poll results asking visitors whether they are interested in offers of bank accounts, logs, PayPal, eBay, etc. Surprisingly 67 percent (149 votes) said “Yes.” The site offers the following “specialized” markets:

- Bots
- Bruters (apparently brute-force crackers)
- Flooders
- Grabbers
- Infectables (viruses and worms)
- Keyloggers
- Sniffers
- Spam software
- Sploits (exploit demos and vulnerabilities)
- Trojans

Financial malware



Figure 2: Shopping for malware: What’s available?

This site offers a total of seven entries, including the following:

- PG Universal Grabber (Power Grabber Version 1.8): supports Microsoft Internet Explorer and compatible browsers, installs itself and eliminates installation traces, bypasses firewalls, is invisible and undetected, sends logs immediately after a POST, loads external files, updates bots, blocks selected sites, self-destructs after n-th restart, encrypts URLs
- Grabber toolkit: “everything for a novice carder”—builder, key generator, provides stats through an administrative page
- Grabber Ghost Version 2.0: when activated changes URLs returned by search engines or when specific keywords are used

3 “MPack, Packed Full of Badness,” Symantec Enterprise Weblog. http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html
4 “Vardan Kushnir,” Wikipedia. http://en.wikipedia.org/wiki/Vardan_Kushnir

Bots and builders

Bots (Figure 3) on the market:

- WDLX Version 1.1: includes a downloader that uses a URL specified in a builder, installs itself, and waits for a live Internet connection. After a time specified by the purchaser, runs the program and removes all traces of its activity
- Xloader: fools firewalls, provides detailed statistics via php-scripting
- Multithreaded distributed denial of service (DDoS): new multifunction, multithreaded bot for Unix, Linux, and related operating systems

And their prices, in U.S. dollars:

- Bot builder with DDoS functions: \$250
- Bot build: \$35
- Bot: \$25
- Downloader (5K–6K in size): \$10
- Form grabbers: \$350
- Keylogger: \$20–\$30
- WebMoney Trojans/builders: \$60

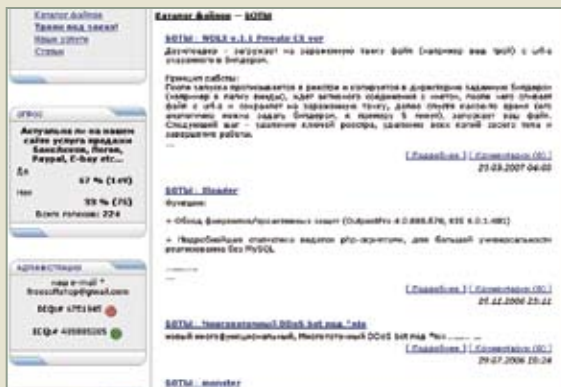


Figure 3: Bots for sale

Custom malware

This advertisement (Figure 4) was posted to multiple forums, offering the following services:

- Breaking into Web sites and forums: \$50
- Guaranteed break-in into mailboxes on mail.ru and yandex.ru: \$45
- Mass deployment of Trojans and spying programs: \$100
- Spam distribution: \$70

Spam-related services

This site (Figure 5) offers "spam services," offering collections of email addresses, at these rates:

- 400,000 companies: \$55
- 1,800,000 individuals: \$100
- 90,000 companies in St. Petersburg: \$30
- 450,000 individuals in Ukraine: \$50
- 6,000,000 Russian individuals: \$150
- 4,000,000 addresses at @mail.ru: \$200

The service generously offers discounts for payments made via WebMoney.

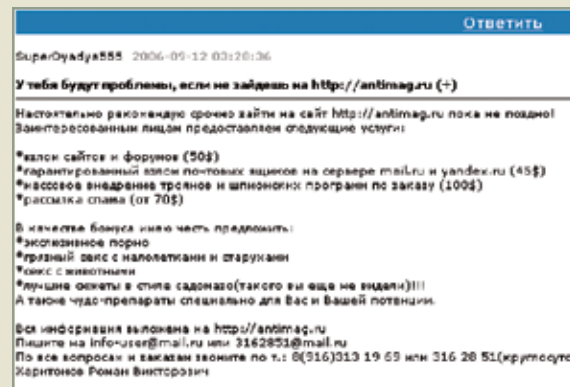


Figure 4: Choose your exploit

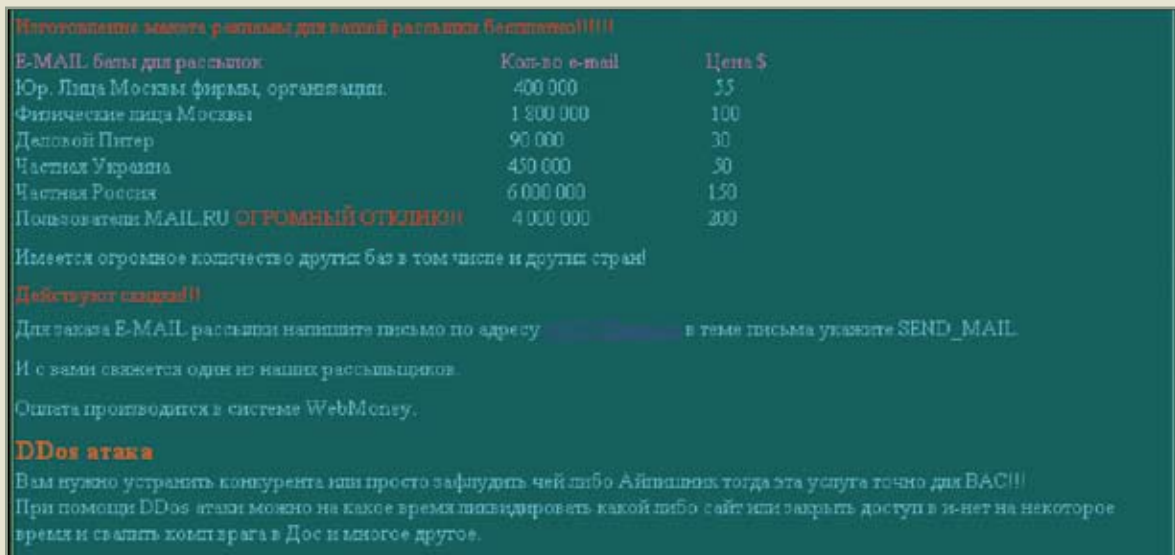


Figure 5: All the spam you could ask (and pay) for

DDoS attack on Estonia

In April and May 2007, there was a major DDoS attack targeting many government Web sites in Estonia. Investigators believe the attack was triggered by the relocation of the "Bronze Soldier," a monument that memorializes a Russian unknown soldier of the Second World War.⁵ Estonian authorities had decided to move the statue from the center of Tallinn to a suburban cemetery. This caused civil unrest in Tallinn; one person was killed. Later, closer to the anniversary of the Victory in Europe Day (from the Second World War, celebrated on May 9), a DDoS attack started that lasted for several days. Many major Estonian Web sites were unavailable during this period. The prevailing opinion of the security experts is that this attack was committed by a group of individuals and was fuelled by their patriotic feelings.⁶ More technical details about the attack can be found here.⁷ No trace to any Russian government involvement was found nor is a link likely to be found, even if there were one.^{8,9} Mutual accusations of cyberattacks followed this incident.¹⁰

Conclusions

At McAfee® Avert® Labs, we have a good feeling for what is fueling the creation of computer malware. All countries that combine relatively poor computer users with wide availability of the Internet and good computer skills are contributing to the problem; examples include China, Russia, Brazil, and Ukraine.

It is obvious to us that the Russian mafia and FSB are not behind the increase in malware, spam, and phishing attacks coming from former USSR. The mafia, however, must be interested in supporting computer crime—due to its extremely high return and low risk. At the same time it would be surprising if the new edition of the secret police had no department specializing in computer security and did not invest in research on computer warfare. The same should apply to the military. Nonetheless, we see economic factors as the primary cause of the development of malware in Russia and the other former Soviet republics.

Predictions

With enhancements in legislation, a strengthening economy, lower unemployment, and stronger law enforcement in Russia we expect a gradual decrease in the rate of malware production. Other former Soviet countries and even China are likely to follow the same pattern. At the same time, current trends in malware counts clearly indicate an acceleration of production in almost all regions of the world. Even if the production of malware in Russia falls to "western standards," it will still be considerable.

We are not likely to see a general decrease in malware numbers any time soon. Computer crime is too profitable and poses too few risks at the moment. And contrary to a common opinion, it is not just a technological problem—it is very much a social and economic problem. As it frequently happens, things are likely to get worse before they start to get better. We believe in the long term that major changes may occur if we can reach global agreements on using the Internet (for example, compulsory Internet ID cards). More likely change for the better will come from advances in computer security, in both hardware and software areas.



Dr. Igor Muttik is Senior Architect for McAfee Avert Labs. Dr. Muttik holds a Ph.D. in physics and mathematics. His studies of the

first computer viruses led to his joining Dr. Solomon's Software, which was later acquired by McAfee, Inc. In addition to his research work on malware, Dr. Muttik is a frequent presenter at security conferences around the world.



5 "Bronze Soldier of Tallinn," Wikipedia. http://en.wikipedia.org/wiki/Bronze_Soldier_of_Tallinn

6 "Estonian DDoS—a final analysis," Heise Security. <http://www.heise-security.co.uk/news/90461>

7 "Estonian DDoS Attacks—a summary to date," Arbor Networks. <http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>

8 "DDoS attacks on the Estonian servers were not a cyber war," Heise Online. <http://www.heise.de/english/newsticker/news/91095>

9 "Massive DDoS attacks target Estonia; Russia accused," Ars Technica. <http://arstechnica.com/news.ars/post/20070514-massive-ddos-attacks-target-estonia-russia-accused.html>

10 "Malware Evolution: April–June 2007," Viruslist.com. <http://www.viruslist.com/en/analysis?pubid=204791956>