Criminal Code

FOCUS

Cybercrime

THOMAS WADLOW, INDEPENDENT CONSULTANT
VLAD GORELIK, SANA SECURITY

NOTE: This is a fictional account of malware creators and their experiences. Although the characters are made up, the techniques and events are patterned on real activities of many different groups developing malicious software.

"Make some money!" Misha's father shouted. "You spent all that time for a stupid contest and where did it get you? Nowhere! You have no job and you didn't even win! You need to stop playing silly computer games and earn some money!"

Being a runner-up in the World Programming Olympics should have been enough to get him a job interview, but nobody in Saratov was hiring programmers. With no jobs, there were no interviews to be had. Sick of thinking about the problem, Misha spent more and more time with his games. Not content just to play them, he used his programming skills to examine the software and see how it worked. One day, he spotted a flaw in one of the most popular multiuser games and saw how he could use it to his advantage. He wrote a small program that let him gain privileges and power in the game, and quickly became a force to be reckoned with in that world. It felt good, but he was smart enough not to simply brag about it. He logged on to some insider game boards and offered his program for sale.

Even these simple types of transactions require anonymity. Misha set up a private e-mail and

The Making of a Cybercriminal

Criminal Code The Making of a Cybercriminal

an account on Aurum, a gold-backed anonymous transaction system, to get paid. He didn't have to wait long for people to respond. One of the buyers, who went by the handle of LesOp0val, was particularly impressed with Misha's program. He asked Misha to do some "custom" work that "pays well." It was impossible to tell through these interactions where any of these people were located. To protect himself, Misha made sure that all his conversations were in Russian—that way he had to worry about only one set of laws.

The custom work was fairly simple. Build a downloader that could be controlled by an IRC message. The right command, encrypted properly, would activate the program and download a file from any URL on the Internet. LesOp0val was impressed with the results and how quickly Misha delivered. Misha's father was impressed with the money, a fact that secretly amused Misha because what his father saw was only a fraction of what he had actually been paid.

LesOp0val pointed him to an IRC channel, messaging with a smirk, "I hope you can keep up!" Misha quickly learned what he meant. The conversation was fast and furious, full of cryptic abbreviations and local slang. It was obvious that all of the participants were Saratov-born and -bred. No one else could figure out what was being said!

The people on the IRC channel were developers of various software and services. Initially the use of the software escaped him, but soon enough he realized that it was all about capturing personal information. The technology discussed was just as sophisticated as what he had seen in his advanced classes in school. Some of the people on the IRC clearly had strong computer science and math foundations; they laid out the problems and the solutions with some theoretical underpinnings. They talked about evasion of detection and response times. Some of the code was written to run in the kernel to avoid detection.

Once Misha posted enough messages to establish his credentials, he began hearing from other posters. He learned many things and soon became something of an authority on several techniques.

LesOp0val had more and more work for Misha. He even started explaining how the software was being used and had Misha figure out how to build it rather than just giving him a detailed commission. Misha's education came in handy. He broke up the software into modules and recombined them for different orders. But the workload

increased and it became clear that this was more than one person could handle. Misha pulled in a couple of his friends from school.

Slava fidgeted in his chair. Misha just sat, quietly smoking. After a moment, Dima returned with a tray full of drinks. Misha passed them around and said, "A toast, my friends, to our little group! May our project exceed our expectations." The bar was crowded, but their corner table was far enough from the others to make eavesdropping difficult. Misha drained his glass and slammed it on the table. They began planning—who would write what components, how it would all fit together, how they would sell it, and who would buy it. More drinks came. The conversation grew more and more excited, which drew the attention of a group of girls at the other end of the bar, and when the guys noticed that, the course of the evening quickly shifted from coding to other things.

THE COST OF DOING BUSINESS

Misha's father walked around the car, inspecting it, leaving no part unexamined. It was American, a glossy black Jeep Grand Cherokee, and it was the biggest car Misha's father had ever seen. "It's paid for?" he asked, skeptically. "In cash," Misha smirked. "All of this, from playing computer games...," his father said, shaking his head in disbelief. He was only beginning to suspect what his son really did. He had once read a newspaper article about *xakeps*, or computer hackers, as they were referred to in the West. Some called them criminals, but as his uncle used to say: "If you aren't caught, you aren't a thief!"

Later that night, Misha's father was bragging to his friends at the corner beer stand. He told them of his boy's new car, and how he earned so much money just playing with the computer. Not like the old days, when a man had to work hard just to feed his family, and cars were impossible dreams for a working man.

None of them noticed the man standing nearby, whose sharp ears caught every word.

At 3 a.m. there was a knock on the door. As Misha opened the door, he was knocked to the ground, felt the knee on his neck and his arm twisted behind his back. He could only see feet going through his apartment and hear the sound of breaking equipment.

The local militia station was drab blue and smelled of vomit and urine. The inspector said, "My boys just got a little carried away with your equipment, you know how it is. You know you can't run a 'computer' business out

of your home without proper authorization. We are all reasonable people here, we can all work together.” Misha was shivering. The inspector continued, “Why don’t you go home and sleep on it—we know where to find you.”

In the morning, after surveying the damage from the “raid,” Misha sent a message to Les0p0val. The response was short and simple: “Pay them—it’s just the cost of doing business.”

BRANCHING OUT

“A guarantee? You want a guarantee?” Misha frowned at the screen. His negotiations with kru5h3r via IRC had

been going well, till now. Kru5h3r wanted a full-function rootkit that he could distribute to build a botnet. He was willing to pay, but he didn’t want his investment to go up in smoke if his rootkit signature found its way into popular intrusion detection software.

“Nobody gives a guarantee,” Misha thought, but as he was about to type that reply, something made him pause.

“That’s right... we offer them insurance!” Misha grinned. Slava looked at him in disbelief. “Of course, they pay for the custom rootkit, but for a little bit extra every month, we will give them protection from the signature databases. If their kit is spotted and tagged, we’ll give

Hacker Speak

133t, 1337, leet: A slang combination of numbers and letters used by gamers and hackers. Often referred to as leetspeak, where *leet* means elite. Leetspeak exists in several languages including English, Russian, and Chinese. The basic principal is to substitute certain letters and sounds—for example, *ph* for *f* as in phishing, or numbers for similar letters (3 for *e*, 4 for *a*, 5 for *s*, 7 for *t*, etc.).

Phishing: A form of e-mail fraud where an attacker generates e-mails that seem to be from a legitimate business asking users to log in or provide some information by directing them to fake Web sites that collect user data. Many phishing e-mails are generated by *spambots*, distributed networks of bots that send out the e-mails.

Bot: A piece of malware that is designed to carry out remote orders of its owners. Bots usually run on a compromised machine and use its resources to do tasks on behalf of its controller. The bots are often controlled through standard communication protocols such as IRC (Internet Relay Chat) or IM.

Botnet: A network of bots. These networks can grow to contain hundreds of thousands of machines. Botnets can be rented from an owner for a specific task. Some of the most common examples are spam distribution and distributed DOS (denial-of-service) attacks.

Bot herder: A person who controls and manages a network of bots.

Downloader, trickler: A component of the malware that fetches other pieces of malware onto a box from some location on the Web. If the downloader or trickler is not removed from a machine during malware removal, it is likely the same or new malware will reappear on the machine. Tricklers are also used to update the malware periodically for “better” and newer versions.

Rootkit: Software that is designed to hide the presence

of malware (or other programs on the machine). Rootkits can hide processes, files, registry settings, and even network connections. Modern rootkits use kernel-level components either to intercept system calls or to directly manipulate kernel structures to make resources invisible.

IRC (Internet Relay Chat): A peer-to-peer network where multiple people or computers can connect to the same channel and send and receive text messages.

Aurum: A pseudonym for a Web payment method that is backed by gold. It provides a high level of anonymity for the conducted transactions. Several real examples of this type of system exist and are used for anonymous, cash-like, nonreversible transactions.

Xakep: Russian word for hacker.

Militia: The local law enforcement in Russia.

Exploit, sploit: A hack into the system that takes advantage of a weakness, typically in software (e.g., a programming mistake).

Buffer overflow: An exploit that uses unchecked buffer or string manipulations to insert new code and pass control through to a running process. This is the most common type of exploit.

Carders: People who steal and monetize credit card information.

Reshippers: People who are hired to receive goods bought with stolen credit cards and resend them to another location. Most reshippers are not aware that they are actually doing anything illegal. They are typically hired through “Work at home” ads and communicate with their employers over the Web or e-mail. Some reshippers are also asked to use their personal bank accounts as a staging area for money transfers. At the end of their employment it is not uncommon for the reshipper’s identity to be stolen as well.

Criminal Code

The Making of a Cybercriminal

them another one that does the same thing, but doesn't match the known signature. They pay us a subscription fee through Aurum, so it all stays nice and anonymous."

Later, they would discover the best part of their "insurance policy" was that their rootkits were spotted only once in a long while, often enough that people paid the insurance, but not so often that replacing them was much work.

Demand was increasing, far beyond the ability of Misha and his friends to meet. With the boom in spam and phishing, it seemed like every xakep crew and freelancer in Russia wanted access to their botnets or wanted to buy software to help set up their own. It was time to branch out. Misha began spreading the word on various 133t boards and soon had a collection of programmers ready to work with him. He kept some of the core modules proprietary to his original group, especially the crypto ones, so that he could keep control of the results.

He found programmers by trolling the boards and working his contacts, looking for talent he could cultivate. "Script kiddies," people who could use exploits created by others, were all over the place online, of course, but Misha and his crew looked at them with nothing but contempt. The real money was in organization. It wasn't about bragging rights or looking cool in the eyes of your peers. It was all about the money.

Business was good. Misha had long since moved out of the small apartment that the militia had raided into a much more luxurious one. He had the best booze, fashionable clothes, a great car that was the envy of his friends, and best of all, the attention of beautiful women. His lifestyle was not without problems and certainly not without expenses. His father would have been shocked to know how much he paid the militia every month to avoid another raid, how much it cost to keep the loyalty of Slava and Dima, and the doorman and maid at his apartment. But the money that Misha sent his family, as small as it was compared with the other costs, kept them safely out of his business.

Recently, another expense had crept in, in the form of white powder that Misha kept hidden behind a bookshelf. At first, it was just for the girls, but from time to time he enjoyed it himself. Those times were growing more frequent, a fact he couldn't really admit to himself.

BETRAYAL

A message on one of the xakep IRC channels caught

Misha's eye. It was from a bot herder called *tachka*, who offered a service for sending mail to every e-mail address in Russia for the equivalent of \$500 American. There was something about *tachka*'s pitch that sounded familiar.

Keeping his thoughts to himself, Misha used one of the many pseudonym IRC accounts he had crafted over the years to try and contact *tachka*. Eventually he succeeded and established a dialog with him. *Tachka* was clearly Russian and probably from Saratov, like Misha himself. Messaging him was like talking to an old friend from his neighborhood, a fact that worried Misha much more than it comforted him.

The things that *tachka*'s botnet could do were suspiciously familiar as well. Misha set up a small network of captured machines all across the Internet to see if his new friend could infect them with his code. Through another pseudonym, he casually mentioned the net on a message board that he knew *tachka* frequented.

Tachka took the bait, and the evidence was clear. The code from *tachka*'s bot contained several of the modules Misha had kept proprietary, adapted to this new purpose. Only Slava and Dima had access to that code. He had trusted his partners, and now he was betrayed.

Immediately, he began backing up his files to flash memory modules that he could hide easily. He also started a series of message exchanges with *tachka*, casually inquiring about his code base. After a few days of this, he was convinced that the mysterious *tachka* was actually his old friend Dima. He said nothing to Dima in person, but something in his manner must have given him away. Dima's phone went offline, he stopped responding to messages or e-mail, and was nowhere to be found at his usual hangouts. Of much more concern was the simultaneous disappearance of Slava and *LesOp0val*.

Their botwar was bloody enough, at least in the virtual sense. It caused enough damage to make several news reports around the world. Misha's attempt to seize sole control of the group's botnets had been initially successful, but he had not counted on the backdoor access that Slava and Dima had carefully hidden in the code. He countered by releasing several viruses he had been playing with on his own, which took down quite a few of the machines owned by his former partners, as well as thousands of others worldwide.

That brought the issue to the attention of the operating system vendor, who would issue a patch a month later to close the key vulnerabilities involved. The patch

had little effect in the short run, because most people didn't bother to install it at first, and by the time they did, the war was mostly over. The group's major assets, the buffer-overflow code and 'sploit base, the crypto tricklers and extensive botnets, as well as their reputation, lay exposed and in ruins.

"It was just business, Mishka," Slava said. The bar was crowded, which was why it was chosen for this meeting. They were standing close, so no one could overhear their conversation. "You were getting crazy on us. We had to protect ourselves," he said directly into Misha's ear.

"Crazy? You want to see crazy?" Misha hissed back.

"We want to move on," Slava said calmly, sipping his drink. "We can keep playing this game if you want, but LesOp0val said to tell you that from here on, if you want to play, it gets real." He reached into his shirt pocket and passed Misha a small photograph of Misha's baby sister, playing. It was clear that the photographer had been able to get very close to the girl. The implication of that and Slava's cold smile was clear. LesOp0val's friends could and would do more than take pictures if they chose to visit her again.

"Turn it over," Slava said. On the back of the photo was written a figure, in American dollars. "LesOp0val said to tell you: 'Pay it. It's the cost of *just* doing business.'" Slava swallowed the last of his drink and left the bar.

Misha was on his own now, but unfortunately his expenses were almost the same as when he was with his old group, and now his reserve money was almost gone. The militia still demanded payment, and his family needed ever-more cash, as did his remaining female friends. Fortunately, he still controlled a few small botnets and could put them to work. It took him very little time to plug into the network of "carders" that had recently sprung up in Russia. There was quite a sophisticated infrastructure detailing how to get credit card numbers by using his botnets for phishing, trojans, and even good old-fashioned social engineering.

Once he had the card numbers, there were lots of ways to turn them into money. Misha set up a network of reshippers—people who would sign for deliveries, then reship the boxes internationally to other destinations, where they could be sold on the black market or even directly to retailers. Many of these reshippers were in America and Europe. Misha even went so far as to place ads in a number of American newspapers offering "promotional jobs that pay \$70-\$80 per processed shipment; health and life benefits after 90 days." Of course, reshippers rarely lasted 90 days before figuring out that they weren't going to be paid. Or they got caught.

It wasn't long before the cash started flowing in again for Misha.

FULL CIRCLE

These days, Misha was too busy to play online very much, but one weekend he gave himself the luxury of an all-night gaming session. As he moved through the shared world, he was surprised by another character who seemed remarkably powerful and well equipped with money and weapons. Rather than challenge him, as Misha might have done as a student, he suggested an alliance. The player, whose handle was g05ha, agreed.

The two cut a wide swath through the RPG (role-playing game), and Misha noticed that his partner rarely suffered much damage in combat. He messaged g05ha about this, and the boy responded that he had figured out how to hack cheat codes in the game to give himself an edge. He offered to share a few with Misha.

"I have a better idea," he messaged back. "How would you like to work on some programming projects for me?"

Misha asked g05ha to work on a problem for him, specifically how to post to Web sites that were protected by captcha guards. A captcha was, in theory, a way to distinguish a human being from a computer program. It put up a distorted image of some text and required a person to type in the text seen there. The idea was that even a sophisticated computer vision system couldn't read the distorted text, only a human could. If the entity connecting to the Web site could read the captcha text, that entity must be human.

"How did you solve the captchas?" Misha asked.

"Simple," g05ha messaged back. "I built a porn site. It gets hundreds of visitors per hour. More every day. You want to see some pictures, you solve a captcha! Some of them are from sites I want to log in to...."

Misha read the reply with a whistle, thinking that this boy will go far. Time to give him another project.... Q

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

THOMAS A. WADLOW is a network and computer security consultant, and author of *The Process of Network Security* (Addison-Wesley Professional, 2000).

VLAD GORELIK is the chief technology officer at Sana Security, where he has spent the past several years leading the company's efforts in creating technology to fight malware. He holds multiple patents and patent applications in software technology and computer security.

© 2006 ACM 1542-7730/06/1100 \$5.00