



Contact Us

- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us

- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News

- Press Room
- E-mail Updates
- News Feeds

Be Crime Smart

- Wanted by the FBI
- More Protections

Use Our Resources

- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Apply for a Job

Headline Archives

'DARK MARKET' TAKEDOWN Exclusive Cyber Club for Crooks Exposed

10/20/08



The "Dark Market" website

Last week the FBI and its global partners wrapped up a two-year undercover cyber operation that resulted in 56 arrests worldwide, the prevention of \$70 million in potential losses, and the confirmation that while there might be honor among thieves, in the end, they are still just thieves.

Here's what happened:

...A discerning group of cyber criminals

established a forum on the Internet called "Dark Market," where they bought and sold stolen financial information such as credit card data, login credentials (user names and passwords), and even electronic equipment for carrying out financial crimes.

...At its peak, this vast criminal network had over 2,500 registered members, who all believed they were operating in a protected cyber environment because they went to great lengths to vet members and to weed out undesirable elements.

...What they didn't know was that one of the site's administrators and most respected members, who called himself Master Splyntr, was one of us—an undercover FBI agent who had infiltrated the site posing as a cyber crook.

"It was a group of people who trusted each other," said the undercover agent after the arrests. He explained that there are two types of cyber criminals: those who steal, but not from one another, and "rippers," who steal from anyone.

Keeping the rippers off the Dark Market site, the agent explained, gave the other members a false sense of confidence. "They did a good job of trying to be secure, and they felt secure. There was honor among thieves, so to speak."

"What's worked for us in taking down spy rings and entire mob families over the years—embedding an undercover agent deep within a criminal organization—worked beautifully in taking down Dark Market. And once again, our global partnerships paid off."

FBI Cyber Division Assistant Director Shawn Henry

Master Splyntr was on the site nearly every day, anywhere from one hour to 15 hours a day. Dark Market was like an exclusive club for cyber crooks, a meeting place for getting advice and brokering deals. During his time online, the undercover agent said, "we saw millions of dollars being exchanged." At the same time, the operation prevented the millions of dollars in losses by tipping off potential cyber crime targets.

From the outset, our agent pointed out, "the goal was to infiltrate the organization." The operation was extremely successful in developing intelligence on Dark Market's leading members and the ways in which they conducted their far-flung crimes.

Throughout the operation, we worked closely with our international law enforcement partners, including the U.K.'s Serious Organised Crime Agency, the Turkish National Police, and the German Federal Criminal Police.

"What's worked for us in taking down spy rings and entire mob families over the years—embedding an undercover agent deep within a criminal organization—worked beautifully in taking down Dark Market," said our Cyber Division Assistant Director Shawn Henry. "And once again, our global partnerships paid off."

As for our undercover agent who became a trusted member of the forum, he explained that he often had to think like a crook when signing on as Master Splyntr. "But at the same time," he added, "you remember what your job is—to get the criminals."

Resources:

