

- [News Archive](#)
- [Network Map](#)
- [Overseas Sales](#)
- [Photo Sales](#)
- [Sitemap](#)
- [The Age Shop](#)
- [Subscriptions](#)
- [Property Data \(APM\)](#)

Inside the hackers' den

Asher Moses
October 9, 2008

HUNCHED over a computer terminal in his pyjamas, "Frank" makes more money than a small-time drug dealer without ever having to worry about being caught or even leaving the house.

Constantly covering his tracks via a complex web of internet servers, he is part of a global network of cyber thieves who together fleece billions of dollars from unsuspecting internet users every year - using little more than an internet connection, free software and some spare time.

Speaking to the *Herald* on the condition of anonymity, he and other experienced hackers say banks' attempts to stamp out credit card theft are doomed due to the ease with which clients' computers can be compromised.

In today's e-commerce world, you can have your bank details stolen just by visiting your favourite websites. Hackers use automated tools to scan websites for vulnerabilities, injecting databases with a few lines of tainted code.

Whenever someone visits the compromised site, in the background their computer is redirected to a site hosting malicious code and infected with a virus, giving hackers backdoor access to the computer.

Among a plethora of nasty features, the virus reports back to the hacker with a log of every keystroke the victim makes.

The BusinessWeek website was the most recent high-profile victim in September, but security companies estimate hundreds of thousands of other reputable web pages, including some belonging to the United Nations, have been infected in recent months.

BusinessWeek fixed the problem after widespread publicity but not before thousands of visitors were potentially exposed.

Once a personal computer is infected, the hacker can control it remotely using a web application. The computer can then be brought into a botnet of "zombie" computers and be used to infect other machines.

"You can simply type in '.card' into the command line and it will display all credit cards used on that computer," said Odin, the administrator of the Evilzone.org online hacking forum where many online troublemakers talk shop.

"Which means any card you use for any website you go to, you're screwed, no matter if it has a

little 'lock' to the right of the address bar saying that it is 'secure'."

Hackers can also infect computers by sending out spam emails with either the virus attached or a link in the body that is activated when clicked.

Makers of internet security programs are in a constant battle with virus writers to block the latest threats, but new variants appear constantly and even the most frequently updated anti-virus program cannot block all threats.

"If the virus is undetectable by anti-viruses, you can say it's the latest game from Epic Games and stick the virus onto the game," Odin said. "That is called binding, when you bind a program onto another program. Bind the virus with a worm and you've got 10-20 victims in the first hour."

A worm automatically spreads the virus via email, instant messaging programs such as MSN and peer-to-peer file sharing programs such as Lime Wire.

Hackers use invitation-only internet forums to trade tools and techniques, and even to gloat about their conquests.

Evilzone.org, one of the few public hacking forums, allows people to trade viruses, information on vulnerabilities and "exploits", spamming tools, mailing lists and tutorials on how to use them.

There are also tips on how hackers can stay anonymous by accessing the internet through proxy servers, which load up web pages on their behalf but hide the source computer's identifying information.

Most members of forums are careful to restrict conversations to theory, using more private instant messaging programs to discuss buying and selling their stolen wares.

Frank, who has been part of the hacking scene for two years after one of his friends introduced him to a private forum, said spammers were "the main men behind the whole carding economy".

He said they "don't have to be skilled at all" and only required a mass-mailing tool, mailing lists and authentic-looking scam pages. They then fire off messages to thousands of people purporting to be, for instance, a bank representative, asking them to verify their user name and password.

Even if only a tiny percentage of people are duped, it still results in a large windfall for the scammer. The practice is known as phishing.

"Right now with \$100 I could go and buy mailing software ... a hacked host, a scam page and a mail list and I could probably get 50 Bank of America accounts in a week," Frank said.

"I would sell these from \$150 to \$500 each in clean cash, usually via Western Union or WMZ [Web Money], or I could ask for 5 per cent of the balance once the person has successfully cashed out the bank account."

There are myriad ways hackers can cash out once they have obtained stolen bank accounts or

credit card details.

Frank said buyers and sellers set up deals using instant messaging programs such as ICQ and transferred money using facilities such as Western Union.

Australian credit card numbers (including the expiry date and three-digit verification code) typically sell for \$2 to \$3 each. For more money, hackers also sell "dumps" of cards' magnetic strips - obtained using a credit card skimmer - which others can write on to blank cards, using them to buy goods from brick-and-mortar stores.

But to safely extract money from a credit card without having a physical card, buyers have to be more creative than simply using a service such as Western Union, Odin said.

One way is to find a partner and create two accounts on an online poker site, loading up one of the accounts with cash from a stolen card. The pair then enter a heads-up game and the cashed-up player purposely loses, making the other account rich. They then cash out and split the profits.

The tangled web they weave - understanding the lingo

CARDING theft and fraud committed using a credit card.

SKIMMING stealing credit card information during a legitimate transaction, often using a device hidden in a store's card reader.

PHISHING ATTACK being tricked into disclosing your password and details to online criminals.

VULNERABILITY A security hole in a piece of software that makes the computer susceptible to infiltration by hackers.

EXPLOIT A tool used by hackers to take advantage of vulnerabilities in software.

BOTNET an army of infected computers controlled remotely by hackers and used for distributing spam and viruses to hijack other computers.

ZOMBIE COMPUTER One of the infected machines that make up the "botnet".

PROXY SERVER A buffer between the hacker and the open internet that connects to web pages on behalf of hackers, helping them to cover their tracks.

TROJAN malicious software that can hijack a computer or alter an otherwise safe web page.

KEYLOGGER a trojan or software that records every computer keystroke to capture personal details, including passwords.

IRC stands for Internet Relay Chat, the key online software used by those who trade in illegal data.

MONEY MULES people who cash out credit card accounts in exchange for a share of the proceeds.

- [Email](#)
- [Print this story](#)