

Publicerad: 2007-01-26 16:34 Uppdaterad: 2007-01-27 09:34

Meeting the Swedish bank hacker

Av: [Linus Larsson](#)

For the price of 3,000 dollars, our reporter was offered his personal bank Trojan. In an interview with Computer Sweden, the hacker behind the recent Internet frauds against Sweden's Nordea bank claims responsibility for more intrusions. "99 percent of all bank intrusions are kept secret," he insists.

Symantec security expert Per Hellqvist helped Computer Sweden track down the inventor of the Nordea-trojan.

The same Trojan that stole eight million Swedish kronor from the Nordea bank was also used for a major attack in Australia. This is confirmed by the hacker who calls himself "Corpse", a developer of advanced Trojans. Computer Sweden's reporter met him in an anonymous chat.

With the aid of security expert Per Hellqvist of Symantec, Sweden, Computer Sweden tracked the Russian-speaking hacker. Using a pseudonym, our reporter claimed to be interested in buying his own Trojan, tailored for attacking an internet bank. It was soon obvious that "Corpse" knows very well that his application is used for major Internet banking frauds.

The bank accounts broken into are selected at random: "It's like roulette," he says in broken English: "Some accounts have a million dollars, some have one dollar. You never know who gets infected."

CS: The Trojan that some people call Haxdoor, is that yours? Does it have the same functionality?

"Corpse": Yes, Haxdoor (there are so many varieties) is mine.

"Corpse" himself sells the Haxdoor Trojan under the name A311 Death. Haxdoor is the name given to it by virus protection software vendors.

CS: Have you heard about the Nordea attacks? That was Haxdoor, wasn't it?

"Corpse": Haxdoor and Nuclear Grabber (a Haxdoor version without a back door).

CS: Quite impressive. Is that the version that I could get for 3,000 dollars?

"Corpse": Yes, and ...

CS: And...

"Corpse": [Provides a URL to information about the attack in Australia.] That's Haxdoor too.

CS: I get that for 3,000 dollars?

"Corpse": Yes, it's the same version.

Computer Swedens reporter meets Corpse.

Those attacks against Internet banks that are reported are, according to "Corpse", only the top of an iceberg. Banks cover up most attacks - something that attackers appreciate.

CS: Cool. Any more examples of attacks using Haxdoor?

"Corpse": The banks try to cover up 99 percent of all attacks, because they do not want to scare their customers. :)

As soon as the money is cleared, the program will be delivered, and scripts for picking up stolen information, such as one-time scratch pad access codes to the Nordea Internet bank, will be installed. "Corpse" will assist - support is included in the price.

Our questions about previous customers and about the perpetrators of the Nordea fraud seem to make "Corpse" uncomfortable:

CS: This seems simple, but don't you need a lot of people to do this?

"Corpse": There is only one developer, and that's me.

CS: Yes, but I mean your customers. Like the Nordea attack - was that one person or a bigger group?

"Corpse": I don't know ... some work on their own, some in groups.

When our reporter pretends to be worried about getting caught, "Corpse" sounds reassuring. At 150 dollars a month, he can provide servers in China, Europe or in the USA where the stolen information will be stored. That way, the attacks will be impossible to trace.

"Corpse": I can buy servers or web hotels for you.

CS: OK, won't that get you into trouble. Maybe it's easier to run anonymous servers in Russia?

"Corpse": Not in Russia. USA, China or Europe...

CS: Your security is important to me, because if you're caught, I might get caught. Aren't you worried about the police?

"Corpse": Don't worry about the police. Just use anonymous VPN or Socks, and it will be alright. :)

Some versions of the Haxdoor Trojan can hide themselves in the operating system with rootkit functionality. That means they're invisible to most virus protection applications. "Corpse" confirms that the version he is hawking works like this. The virus protection program from Norman, which Nordea bought and provides its Internet banking customers with free of charge, he dismisses outright.

CS: Are you familiar with Norman Antivirus? They say it can detect Haxdoor on an infected computer.

"Corpse": Anti-virus applications can't find the undetectable version.

The Trojan includes a graphic user interface that the attacker can use for designing a tailormade attack on a specific bank. "Corpse" confirms that the Trojan is activated when a specific phrase, such as "scratch code 1" appears on a web page. It picks up the information and forwards it. It's quite simple, he insists.

"Corpse": The interface is standard and requires no special skills. If you have any problems, I'll help.

Like any salesman, "Corpse" boasts about Haxdoors usefulness for successful bank frauds.

"Corpse": Yes, it will have rootkit and self-protection features.

CS: Good, how is it delivered?

"Corpse": As an rar or zip archive.

CS: By the way, will it also infect Vista? And how about older versions of Windows?

"Corpse": All versions are supported - Windows 98 (4/10/1998) and later.

CS: Including Vista?

"Corpse": Yes.

After one and a half hours of conversation, "Corpse" feels certain that the sale is in the bag, and that his intrusion program has made him another 3,000 dollars.

CS: This is very interesting. I need to do some planning, then I'll get back to you - OK?

"Corpse": OK.

CS: When are you usually online? We might be in different time zones.

"Corpse": 15-24 (GMT +0).

Translated by: Anders Lotsson.