Dr.WEB®
since 1992

Defend what you create

The blind are not afraid of snakes

Caution! Threat! Banking Trojan Trojan.Carberp!

One possible way to get infected with Trojan.Carberp

This is a real incident that occurred in December 2012 in a company located in Moscow.

1. An accountant was reading articles on a health-related website. Her computer had a remote banking system (RBS) installed on it.
2. The browser froze and displayed a window containing a warning about a program malfunction.
3. Without thinking, the accountant clicked one of the window's buttons to get rid of the annoying window and get back to her article.
4. But the browser was still stuck, and the accountant called the system administrator to come take a look.
5. He logged in under his administrator's domain password and solved the problem with the browser. The accountant was able to continue reading the important article. A Trojan, that had penetrated the accountant's computer unnoticed, was activated by the accountant when she clicked the button in the browser window. Thus, criminals were able to obtain the passwords to the banking system and the remote banking system (RBS).
6. The accountant didn't use the RBS for a few days, but several million roubles were stolen during that period.

Just 1 to 3 minutes are enough for a Trojan to steal passwords and money from a victim's account.

What are banking Trojans?

These are dangerous malicious programs designed to:

- steal passwords for banking and payment system access and money from bank accounts;
- download other malicious programs;
- paralyze a computer when remotely commanded to do so by a criminal.

Trojan.Carberp is the most dangerous of these programs.

Currently plugins exist for most types of RBS.

Attention! Due to the nature of this scheme, which is used by attackers to infect systems, small and medium-sized companies are most likely to be in danger.

What is the main target of banking Trojans?

Money.

It's the only thing the hackers are interested in.

Before stealing money, a Trojan's owners collect information about their future victim. They know the company's account balance at any given time, transfer amounts, and the reasons why variations in the account occur (the same reasons will be used to make fraudulent payments), receive information about all the payments made by the company's accountant. Thus, the victim is tracked 24/7 before their account is drained. Fraudsters obtain the following information:

The Trojan's owner has information about the victim's account and access to all information stored on the infected computer.

Whether an RBS password was stolen

- Bank account
- Bank account balance
- The amount of a transfer
- The reason for payment
- RBS compromised system (name)
- WWW address of the RBS
- Victim's IP address
- Used web browser

Whether a debit card was compromised

- The bank BIN
- Account of the client or victim
- Address of the e-payment system to which the compromised card belongs
- Card number
- Card expiration date
- Cardholder's first and last names
- CVV2/CVC2

Who needs it?

Today's malware are developed by professional virus writers; this is a well-organized criminal business involving many highly skilled software and application developers.

An organized criminal group works to develop and «promote» a Trojan, with the developers located in one country; the servers that distribute the Trojan in another; the organizers in a third country; and the «partners,» who purchase a botnet segment for criminal use, located in multiple countries.

The program is constantly upgraded by its creators, and new Trojan versions are churned out. Every day dozens of entries of Trojan.Carberp are added into Doctor Web virus databases. And that's only one Trojan modification...

Facts

- Every day Doctor Web's anti-virus laboratory receives on average about 60,000 malware samples.
- A record was set on November 28, 2012, when the Doctor Web anti-virus laboratory received more than 300,000 samples. At the beginning of December, we saw another record! And that number does not include every virus created that day.

Virus analysts are not magicians and are unable to instantly process the thousands and thousands of suspicious files that are received daily. The risk of infection with an unknown virus is always present.

Did a Trojan sneak up on your computer?

No! You invited it in!

Carberp family Trojans penetrate computers while **victims browse compromised sites**. No action needs to be taken to get a system infected. **It occurs automatically**.

The most dangerous websites for PCs are:

1. Sites related to technologies and telecommunications.
2. News portals, business outlets, accounting-related sites and forums, online courses/lectures, etc.
3. Women's sites (health, cooking).

There is another way of transferring an infection: via removable media.

Important!

Removable media includes not only flash drives but also any **USB device**! A virus can be transmitted from one PC to another even with a camera or a portable media player.

Trojans are designed to be spread by users, because unlike viruses, they cannot replicate themselves without user intervention. People contribute to their propagation. That's how a computer can get infected — even when no Internet or network connection is present.

Office computers are no longer the only targets of cyber attacks—personal devices (including mobile phones) are at risk too.

A banking Trojan for the Android OS already exists: Android.SpyEye.1.

Are Trojans undetectable?

There exists a dangerous delusion that a virus's actions are usually visible and that a computer infection will be discovered instantaneously. But it's not true!

- Modern virus writers aim at creating malicious software that should remain undetected in a system for as long as possible — both by the user and special programs (anti-viruses).
- For example, Trojan.Carberp, when launched on an infected machine, undertakes several steps to avoid being detected by control and monitoring systems. After launching successfully, the Trojan injects itself into running applications.

Why does this happen?

1. Technologically sophisticated and dangerous viruses are created for commercial purposes. Virus writers scan them with all available anti-viruses. That's why many malware samples cannot be detected by anti-viruses before entering an anti-virus lab.
2. Trojans designed to steal money from a certain company may remain undetected by an anti-virus if fraudsters know what anti-virus is used by that company.
3. The Trojan penetrated the accountant's computer exploiting several vulnerabilities in the installed software. When she clicked the button in the pop-up window, she activated the Trojan. From that moment on, the Trojan started stealing information from the victim's computer.

4. Users, ignorant of computer security basics or simply tired or careless, unintentionally facilitate malware's penetration of a network (by using USB devices without scanning them with an anti-virus, opening e-mails from unknown senders, and surfing the Web during working hours).

In an effort to teach users security basics, Doctor Web creates training courses, designed for a wide range of PC users, and offers free on-line tests on computer basics. Knowledge acquired while studying such courses makes it easier to cope with computer threats and to not fall for criminals' tricks.

Doctor Web education portal:

http://training.drweb.com

Important!

Today, only an anti-virus can cure malware-infected systems.

What should I do?

Unfortunately the victim discovers the theft after the fact. But that's no excuse for inaction! In this case, how you respond is critical.

Important!

- Do not attempt to update the anti-virus or run a scan—you may destroy the traces of intruders in the system!
- Do not attempt to reinstall the operating system!
- Do not attempt to remove any files or programs from the disk!
- Never use a computer from which e-banking system authentication credentials have allegedly leaked, even if there is an urgent need to do so!

There are no statistics showing the amount of money stolen from online banking systems using malicious software. Quite often victims do not notify law enforcement authorities, believing that they won't get their money back. They do not know how to act in this situation or how to initiate an investigation. They end up spinning their wheels.

Money theft using malware is a crime. Law enforcement authorities need your formal complaint (i.e., a legal reason) to initiate a criminal case against intruders. Remember: There may be many victims, but you may be the first one to notice the criminal activity and contact the authorities, in which case, your complaint may lead to the curtailment of the intruders' activities.

Every criminal leaves traces. Computer criminals are no exception—i.e., we can and must fight them.

125124, Russia, Moscow, 3d street Yamskogo polya 2-12A
Phone: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97

www.drweb.com | estore.drweb.com | www.drweb-curenet.com
www.av-desk.com | www.freedrweb.com | mobi.drweb.com