Dr.WEB®
since 1992

Anti-virus protection for cash registers and POS terminals

Dr.WEB®
since 1992

Defend what you create

Anti-virus protection for cash registers and POS terminals

An underestimated danger and how to avert it with Dr.Web's help

The POS terminals of several hundred Wendy's fast food restaurants were infected with a Trojan that steals credit card data.
https://xakep.ru/2016/05/12/wendys/

This is only one of the officially acknowledged infection incidents involving a retailer's network. But a huge number of infections go unreported in the mass media. What is the real situation with regards to the security of devices located within the local networks of businesses?

Here you can see the result of the NePetya outbreak (a type of encryption ransomware) — a paralysed sales process. This malicious program did not specifically target the in-store equipment, but ended up infecting it too. The infection of the in-store equipment led to monetary losses: the money that the customers would have spent in the store if they could have...

In-store equipment (cash registers and POS terminals) must be protected by the same type of anti-virus that protects ordinary PCs.

Defend what you create

What is it about cash registers and POS terminals that attracts cybercriminals?

Trojan.MWZLesson — a Trojan designed to infect POS terminals with a module that checks the infected device's RAM for bank card data.

By infecting computerised cash registers, cyber-criminals can acquire credit card information, and the passwords and logins of network administrators who have access to those devices.

Very often administrators use the same password to access different resources — this means that a hacker can use a network server to disable the anti-virus protection.

In-store equipment can also be infected by specially designed malware to collect sales statistics that will benefit competitors or to "adjust" the parameters of the goods and services sold in stores.

How can malware infiltrate business networks?

- By exploiting software vulnerabilities
- Using social-engineering techniques
- Via removable media
- Via the local network
- Via a fake POS terminal

For example, BackDoor.Neutrino.50 is a multicomponent backdoor that exploits the CVE-2012-0158 vulnerability.

! As a rule, in-store equipment is not updated; therefore, it contains many vulnerabilities.

! Malware can be planted in a device before it is purchased and delivered, or it can be «delivered» by the employees of companies that maintain a business's devices. Modern devices, including POS terminals, have USB connectors to which infected media can be connected.

Defend what you create

Why can cash registers and POS terminals be infected so easily?

POS devices (Point Of Sale), such as cash registers, terminals, and electronic scales, are computers. Many of them incorporate Intel CPUs and run Windows or Linux.

https://habrastorage.org/files/6b5/663/2e4/6b56632e4a9b4c51bed81246b5c2a8f7.JPG

POS computers are very powerful. Their configuration, based on Quad-Core J1900 2.4 GHz or more and RAM starting at 2-4 GB, is perfect for most office tasks.

Since POS devices incorporate standard hardware and software components, virus writers can easily design malicious programs for them. Moreover, cash registers and POS terminals can also easily be infected by «common» malware that has not specifically been designed for POS devices. For example, by encryption ransomware.

What anti-viruses can be used to protect a POS device?

If the device software permits the installation of an anti-virus, we recommend that you install Dr.Web anti-virus and activate the following components:

- Dr.Web SpIDer Guard file monitor
- Dr.Web SpIDer Gate HTTP monitor
- Dr.Web Preventive Protection
- Device access control in the Office Control component

Dr.Web is a protection system that protects against malware programs of any complexity and purpose.

- The presence of a self-protection driver ensures that the anti-virus won't be disabled by cybercriminals.
- The protected update system ensures "cures" are received.
- Its modern technologies can find a Trojan no matter where it is hiding.

Dr.Web lets users protect their POS devices from malicious programs, network scanning for the purpose of finding vulnerable objects, and the launch of previously unknown threats.

The device control access system and preventive protection restrict the use of removable media and prevent computer resources from being accessed.

! In addition to POS devices, the servers and workstations that have access to them also require protection. We recommend that you create a subnet of those devices on which an anti-virus cannot be installed by separating them from the remaining computers and servers and that you install a traffic control system for inbound subnet data.

Recommended products

The Dr.Web Control Center is provided free of chargeo.

Dr.Web Desktop Security Suite, Comprehensive protection

Dr.Web Server Security Suite

Dr.Web Gateway Security Suite

GET 25% OFF

when purchasing a license for three Dr.Web products.

Only by protecting your retail business's network with a centrally managed anti-virus can you minimise your losses during a hacker attack or an accidental infection!

Defend what you create

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040
Tel.: +7 495 789–45–87 Fax: +7 495 789–45–97

www.drweb.com
www.drweb-curenet.com
www.av-desk.com
www.free.drweb.com