2015

jan 8 | feb 17 | mar 14 | apr 24

may 12 | jun 20 | jul 13 | aug 21

sep 5

All news
Dr.Web products
Dr.Web AV-Desk
Dr.Web beta versions news
Updates of virus database
Virus alerts
Mobile threats
Virus reviews
Real-time threat news
Promotions
Corporate news

Sign up

RSS-feeds

Information
Myths about Dr.Web
About viruses

Resources
Press center
For website owners

Buy
Buy from partners
Anti-virus As a Service
Buy online
License center
Contact sales

Trojan.MWZLesson—a Trojan for POS terminals

September 16, 2015

For many years POS terminals remain one the most favorite targets for virus makers. Due to the fact that this technology is used by a large number of sales organizations around the world to process payments made using bank cards, cybercriminals just cannot leave it "unattended". Recently, Doctor Web security researchers have analyzed yet another Trojan that can infect terminals—this Trojan turned out to be a modification of another malicious program well known to our virus analysts.

Once launched, this Trojan, designed to infect POS terminals and dubbed **Trojan.MWZLesson**, modifies the registry branch responsible for autorun. Moreover, the malicious program encompasses a module that checks the infected device's RAM for bank card data. This code was borrowed from another Trojan designed for POS terminals and named Trojan.PWS.Dexter. The malware sends all acquired bank card data and other intercepted information to the command and control server.

Trojan.MWZLesson can intercept GET and POST requests sent from the infected machine's browsers (Firefox, Chrome or Internet Explorer). Such requests are forwarded to the command and control server run by cybercriminals. Moreover, this malicious program can execute the following commands:

- CMD—forward the command to the command interpreter (cmd.exe)
- LOADER—download and run a file (dll—using the regsrv tool, vbs—using the wscript tool, exe—run directly)
- UPDATE—update itself
- rate—set a time interval for communication sessions with the command and control server
- FIND—search documents using a mask
- DDOS—mount an HTTP Flood attack

Trojan.MWZLesson communicates with the server over the HTTP protocol; at that, all packages sent by the Trojan are not encrypted. However, if a special cookie parameter is missing from a package, the server ignores it.

While analyzing the architecture of **Trojan.MWZLesson**, Doctor Web security researchers made a conclusion that this Trojan is, in fact, a "crippled" version of a malicious program named **BackDoor.Neutrino.50** whose code was partly used for the creation of this new modification.

BackDoor.Neutrino.50 is a multicomponent backdoor that exploits the CVE-2012-0158 vulnerability. There have been some cases, when this malicious program was downloaded from websites hacked by cybercriminals. Once launched, **BackDoor.Neutrino.50** checks its environment for the presence of virtual machines. If the scan returns positive results, the Trojan displays the following error message: "An unknown error occurred. Error - (0x[random number])". After that, **BackDoor.Neutrino.50** initiates a self-removal process.

Aside from being able to operate on POS terminals, this Trojan can steal information stored by the Microsoft Mail client and account details used to get access to resources from a number of well-known FTP clients over the FTP protocol. Unlike **Trojan.MWZLesson**, **BackDoor.Neutrino.50** can execute more commands—in particular, it can launch several types of DDoS attacks, remove some malicious programs found in the system, and can even attempt to infect computers on a LAN.

Signatures of these Trojans have been added to Dr.Web virus databases. Therefore, these malicious programs pose no threat to our users.

Back to news

Company | News&Events | Send a virus | Online scanner | Privacy policy | Site map

Doctor Web is the Russian developer of Dr.Web anti-virus software. We have been developing our products since 1992. The company is a key player on the Russian market for software that meets the fundamental need of any business — information security. Doctor Web is one of the few anti-virus vendors in the world to have its own technologies to detect and cure malware. Our anti-virus protection system allows the information systems of our customers to be protected from any threats, even those still unknown. Doctor Web was the first company to offer an anti-virus as a service and, to this day, is still the undisputed Russian market leader in Internet security services for service providers. Doctor Web has received state certificates and awards; our satisfied customers spanning the globe are clear evidence of the high quality of the products created by our talented Russian programmers.

Search...

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

Dr.Web AV-Desk 10.0 updated