Sign in | Register ▼         BUY from our partners | online | with mobile

## Dr.WEB®
Anti-virus

**Home   Business   Download   eStore   Support   Training   Partners**

EN

<< **2015**

| jan 8 | feb 17 | mar 14 | apr 24 |
| may 12 | jun 20 | jul 13 | aug 21 |
| sep 12 | oct 23 | nov 7 | |

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

# Encryption ransomware threatens Linux users

**November 6, 2015**

**Doctor Web warns users about new encryption ransomware targeting Linux operating systems. Judging from the directories in which the Trojan encrypts files, one can draw a conclusion that the main target of cybercriminals is website administrators whose machines have web servers deployed on. There have been some cases, when virus makers exploited the CMS Magento vulnerability to launch attacks on web servers. Doctor Web security researchers presume that at least tens of users have already fallen victim to this Trojan.**

Once launched with administrator privileges, the Trojan dubbed **Linux.Encoder.1** downloads files containing cybercriminals' demands and a file with the path to a public RSA key. After that, the malicious program starts as a daemon and deletes the original files. Subsequently, the RSA key is used to store AES keys which will be employed by the Trojan to encrypt files on the infected computer.

First, **Linux.Encoder.1** encrypts all files in home directories and directories related to website administration. Then the Trojan recursively traverses the whole file system starting with the directory from which it is launched; next time, starting with a root directory ("/"). At that, the Trojan encrypts only files with specified extensions and only if a directory name starts with one of the strings indicated by cybercriminals.

Compromised files are appended by the malware with the .encrypted extension. Into every directory that contains encrypted files, the Trojan plants a file with a ransom demand—to have their files decrypted, the victim must pay a ransom in the Bitcoin electronic currency.



Doctor Web recommends users whose files have been encrypted to contact technical support providing detailed information on the incident and sending several samples of encrypted files. To decrypt files, it is very important that the user does not modify or delete them—otherwise, encrypted data may be permanently lost.

More about this Trojan

**Share this news** with your friends in social networks and invite them to read it!

F  T  G+  +  1

Back to news

---

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

Search...   »

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

Configure Dr.Web 11.0 components!

Dr.Web for IBM Lotus Domino updated to version 10.0.1