Linux.Encoder.1

Added to Dr.Web virus database: 2015-11-05
Virus description was added: 2015-11-06

SHA1:

- a5054babc853ec280f70a06cb090e05259ca1aa7 (x64, UPX)
- 98e057a4755e89fbfda043eaca1ab072674a3154 (x64, unpacked)
- 810806c3967e03f2fa2b9223d24ee0e3d42209d3 (x64, FreeBSD)
- 12df5d886d43236582b57d036f84f078c15a14b0 (x86, UPX)
- 5bd6b41aa29bd5ea1424a31dadd7c1cfb3e09616 (x86, unpacked)

Encryption ransomware for Linux written in C using the PolarSSL library.

Once launched with administrator privileges, the Trojan loads into the memory of its process files containing cybercriminals' demands:

- ./readme.crypto—file with demands,
- ./index.crypto—HTML file with demands.

As an argument, the Trojan receives the path to the file containing a public RSA key.

Once the files are read, the malicious program starts as a daemon and deletes its original files.

First, the Trojan encrypts files in the following directories:

```
/home
/root
/var/lib/mysql
/var/www
/etc/nginx
/etc/apache2
/var/log
```

After that, Linux.Encoder.1 encrypts all files in home directories. 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 from directories whose names start with one of the following strings:

```
public_html
www
webapp
backup
.git
.svn
```

At that, the Trojan encrypts only files with the following extensions:

".php", ".html", ".tar", ".gz", ".sql", ".js", ".css", ".txt" ".pdf", ".tgz", ".war", ".jar", ".java", ".class", ".ruby", ".rar" ".zip", ".db", ".7z", ".doc", ".pdf", ".xls", ".properties", ".xml" ".jpg", ".jpeg", ".png", ".gif", ".mov", ".avi", ".wmv", ".mp3" ".mp4", ".wma", ".aac", ".wav", ".pem", ".pub", ".docx", ".apk" ".exe", ".dll", ".tpl", ".psd", ".asp", ".phtml", ".aspx", ".csv"

The Trojan does not encrypt files in the following directories:

```
/
/root/.ssh
/usr/bin
/bin
/etc/ssh
```

To encrypt each file, the Trojan generates an AES key. After files are encrypted using AES-CBC-128, they are appended with the .encrypted extension. Into every directory that contains encrypted files, the Trojan plants a README_FOR_DECRYPT.txt file with a ransom demand.

If decryption is initiated, Linux.Encoder.1 will use a private RSA key to retrieve AES keys from encrypted files, traverse directories in the same order as when they were encrypted, and delete README_FOR_DECRYPT.txt files trying to decrypt all files with the .ecnrypted extension.

Doctor Web security researchers have developed a decryption technique that may help restore files encrypted by this malicious program.

Curing recommendations

For Microsoft Windows OS:

1. If the operating system (OS) can be loaded (either normally or in safe mode), download the curing utility Dr.Web CureIt! and run a full scan of your computer and the removable media you use.
2. If you can't load the OS, change the BIOS settings to load your system from a CD or USB drive. Download the image of the emergency system repair disk Dr.Web® LiveDisk or the Dr.Web® LiveDisk recording utility onto a USB drive and prepare the relevant media. After booting up with this media, run a full scan and cure whatever threats have been detected.
3. If your OS has been locked by malware from the Trojan.Winlock family, use our unlocking service. If you failed to find the unlock code, follow the instructions provided in Section 2.

For Linux:

1. On the loaded OS, run a full scan of all disk partitions using the Dr.Web Anti-virus for Linux.

For Mac OS X:

Run a full system scan using the free Dr.Web Light Scanner for Mac OS X. You can download it from the Apple App Store.

For Android:

1. If the mobile device is operating normally, download and install the free anti-virus Dr.Web for Android *Light*. Perform a full system scan and carry out the recommendations for removing any detected threats.
2. If the mobile device has been locked by Android.Locker ransomware (the screen will be telling you that you have broken some law or demanding a set ransom amount; or you will see some other announcement that prevents you from using the handheld normally), do the following:
   - Start your smart phone or tablet in the safe mode (depending on the operating system version and specifications of the particular mobile device involved, this procedure can be performed in various ways; seek clarification from the user guide that was shipped with the device or contact its manufacturer);
   - Once you have activated safe mode, install the free anti-virus Dr.Web for Android *Light* onto the infected handheld and perform a full scan of the system; follow the steps recommended for neutralising the threats that have been detected;
   - Switch off your device and turn it on as normal.

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