The Hacker News™
Security in a serious way

Linux Ransomware targeting Servers and Threatening Webmasters to Pay

Monday, November 09, 2015 Swati Khandelwal

Since past few years, **Ransomware** has emerged as one of the catastrophic malware programs that lets hacker encrypts all the contents of a victim's hard drive or/and server and demands ransom (typically to be paid in **Bitcoin**) in exchange for a key to decrypt it.

Until now cyber criminals were targeting computers, smartphones and tablets, but now it appears they are creating ransomware that makes the same impact but for **Web Sites** – specifically holding files, pages and images of the target website for Ransom.

Dubbed **Linux.Encoder.1** by Russian antivirus firm **Dr.Web**, the new strain of ransomware targets Linux-powered websites and servers by encrypting MySQL, Apache, and home/root folders associated with the target site and asking for 1 **Bitcoin** (~ *$300*) to decrypt the files.

The ransomware threat is delivered to the target website through known vulnerabilities in website plugins or third-party software.

Must Read: FBI Suggests Ransomware Victims — 'Just Pay the Ransom Money'.

Once infected, the Linux.Encoder.1 malware encrypts all files in the **Home** directories on the system as well as **Backup** directories and the **System Folders** associated with Web site files, pages, images, code libraries and scripts.

Ransomware Uses AES Encryption

According to the security researchers, the ransomware in question needs root privileges to work. Additionally, when it launches, the malware starts downloading:

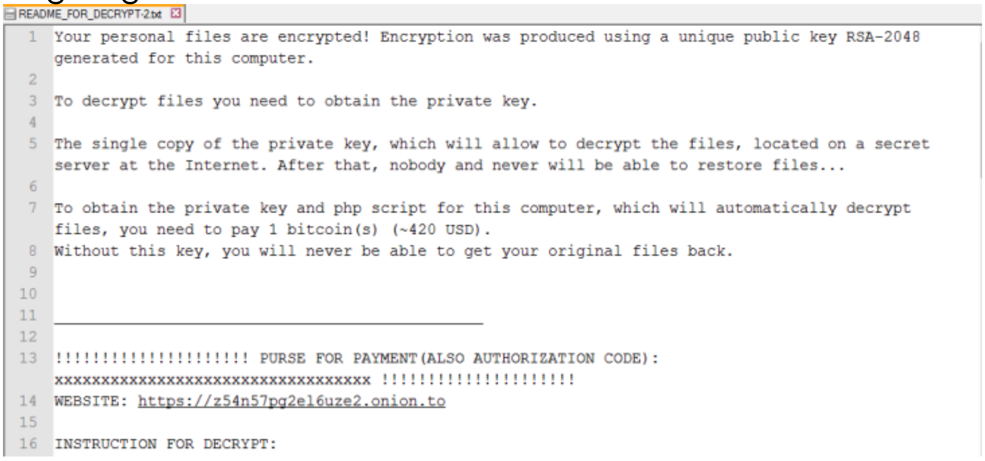
- The **Ransom Message** containing the demands of fraudsters
- A file containing the public **RSA key**

After that, the Ransomware starts as a daemon and deletes all of the original files. The RSA key is then used to store AES keys that are used by the ransomware to encrypt the local files on the infected computer.

The ransomware also adds the **.encrypt** extension to each file it encrypts and writes a ransom text message in every folder.

Also Read: FBI Offers $3 Million Reward For Arrest Of Russian Hacker behind CryptoLocker Ransomware.

Targeting Linux-Powered Websites and Servers



```
Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to decrypt the files, located on a secret
server at the Internet. After that, nobody and never will be able to restore files...

To obtain the private key and php script for this computer, which will automatically decrypt
files, you need to pay 1 bitcoin(s) (~420 USD).
Without this key, you will never be able to get your original files back.



_____________________________________________

!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!
WEBSITE: https://z54n57pg2el6uze2.onion.to

INSTRUCTION FOR DECRYPT:
```

The malware specifically encrypts files in folders that are typically found in Linux Web server setups, including directories like home, root, MySQL, Apache, and any directory that includes terms such as git, svn, webapp, www, public_html, or backup.

Moreover, the ransomware looks for files that have extensions specific to Web development environments including .js, .css, .properties, .xml, .ruby, .php, .html, .gz, and .asp, as well as other file extensions like .rar, .7z, .xls, .pdf, .doc, .avi, .mov, .png, and .jpg.

Once the victim pays the ransom amount, the system receives a signal to pass over the directories again to decrypt the files.

Until security researchers create a decryption program, they recommend webmasters to backup all important data and keep all their files in place in case they are targeted.

Also Read: Anyone can Now Create their Own Ransomware using This Hacking ToolKit.

Bitcoin, Hacking Linux Servers, Linux Malware, Linux Ransomware, Linux Security, Linux Server, Malware, Ransomware, Ransomware Malware, Website Security

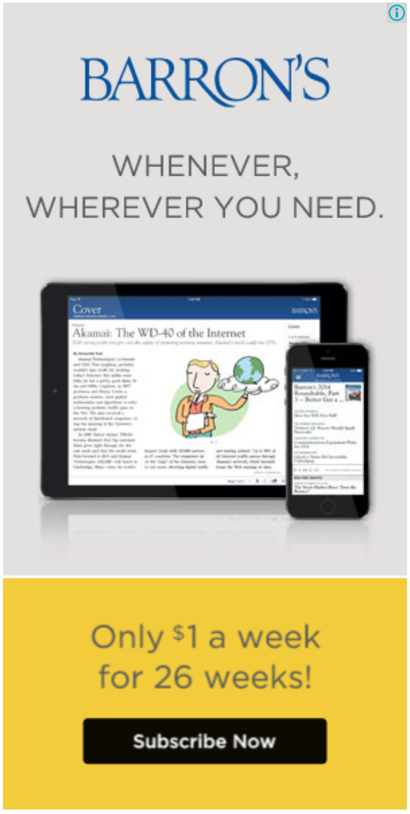
ABOUT THE AUTHOR

Swati Khandelwal

Swati Khandelwal is Senior Technical Writer and Cyber Security Analyst at The Hacker News. She is a Technology enthusiast with a keen eye on the Cyberspace and other tech related developments. She is lover of digital culture, gadgets, creative media, technology, and general interest reporting.

LATEST STORIES

COMMENTS



Popular Stories

Anonymous Group Leaks Identities of 1000 KKK Members

Researcher releases Free Hacking Tool that Can Steal all Your Secrets from

The Hacker News Password Manager

The Hacker News Hackers have Hacked into US Arrest Records Database

The Hacker News Hackers WIN $1 Million Bounty for Remotely Hacking latest iOS 9 iPhone

The Hacker News Kim Dotcom's Decentralized Internet — For You, Powered By You

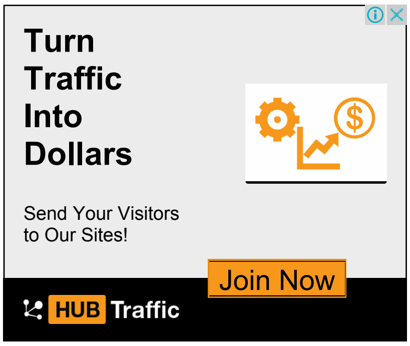
The Hacker News Anonymous Hackers to Leak 1000 of KKK Members Details on Million Mask March (Nov 5, 2015)

The Hacker News FBI Deputy Director's Email Hacked by Teenager Who Hacked CIA Chief

The Hacker News ISIS Supporter Hacks 54,000 Twitter Accounts and Posts Details of Heads of the CIA and FBI

The Hacker News Fourth, a 16-year-old Hacker, Arrested over TalkTalk Hack

The Hacker News Meet The World's First Person Who Hacked His Body to Implant a Bitcoin Payment CHIP



About | THN Magazine | The Hackers Conference | Sitemap | Advertise on THN | Submit News | Privacy Policy | Contact