Subscribe for free

Browse archive

Featured news

- New Linux Trojan performs system reconnaissance
- Industrialized attackers systematically destroy defender confidence
- Rise of automation: Battle of the bots
- Intel patches MiTM flaw in its Driver Update Utility
- Businesses fail to take full advantage of encryption technology
- Malicious Crome extensions ransack Steam users' inventory
- Netflix confirms it will start blocking proxies and unblockers
- OpenWPM: An automated, open source framework for measuring web privacy
- Review: Google Hacking for Penetration Testers, Third Edition
- Good practice guide on disclosing vulnerabilities
- Cybersecurity recommendations for medical device manufacturers
- LostPass: A worryingly simple phishing attack aimed at LastPass users
- Casino operator sues Trustwave for failing to spot and stop hackers
- How email in transit can be intercepted using DNS hijacking
- Cheap web cams can open permanent, difficult-to-spot backdoors into networks
- Have I been hacked? The indicators that suggest you have

New Linux Trojan performs system reconnaissance

Posted on 20.01.2016

A new Linux threat has been identified by Dr. Web researchers. Dubbed Linux.Ekocms.1, this Trojan's apparent function is to discover details about the system it has infected and what the user does on it.

The Trojan's main capability is to take screenshots of the machine's desktop every 30 seconds. It saves them to a temporal folder in the JPEG or BMP format with a name in the ss%d-%s.sst format, where %s is a timestamp.

The screenshots are later sent tto a server controlled by the attacker (the server's addresses are hard-coded in the malware).

"All information transmitted between the server and Linux.Ekoms.1 is encrypted. The encryption is initially performed using the public key; and the decryption is executed by implementing the RSA_public_decrypt function to the received data," the researchers found.

The malware is also capable of audio recording, although the current variant of the Trojan does not use it.

The malware can download various additional files if the cybercriminals command it.

The researchers did not mention how the malware gets delivered to the victims.

Author: Zeljka Zorz, HNS Managing Editor

Follow @zeljkazorz

Linux | malware | trojan horses

Spotlight

1 2 3 4 5

Review: Google Hacking for Penetration Testers, Third Edition

Learning to use Google search effectively boils down to learning the basic query synax and effective narrowing techniques.

DON'T MISS
Wed, Jan 20th

Industrialized attackers destroy defender confidence | Rise of automation: Battle of the bots | OpenWPM: An open source framework for measuring web privacy | How email in transit can be intercepted using DNS hijacking | Cheap web cams can open permanent, difficult-to-spot backdoors