



HELP NET SECURITY

[NEWS](#)
[MALWARE](#)
[ARTICLES](#)
[REVIEWS](#)
[Q&As](#)
[EVENTS](#)
[SOFTWARE](#)
[NEWSLETTER](#)

[Subscribe for free](#)
[Browse archive](#)

HITBSECCONF2016 AMSTERDAM

23-27 MAY 2016



7TH ANNUAL HITBSECCONF
IN EUROPE, NH KRASNAPOLSKY

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

10 key questions to ask when selecting a cloud services vendor

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 to a server controlled by the attacker (the server's addresses are hard-coded in the malware).

"All information transmitted between the server and Linux.Ekocms.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](#)

Subscribe to the HNS newsletter and win one of these books.
If you win, we'll e-mail you on February 8.



Email Address

What you need to know to [earn more](#) in
system administration and [security](#)

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 syntax and effective narrowing techniques.



Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.



Daily digest

Receive a daily digest of the latest security news.

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



The banner features a dark background with a circuit board pattern on the left. A red arrow points to a book titled 'INSECURE' and another red arrow points to a book titled 'MAINFRAME SECURITY'. Below these are two blue buttons: 'Subscribe for free' and 'Browse archive'. The main title 'HELP NET SECURITY' is in large, bold, white letters. To the right is a search bar with the text 'Search Help Net Security' and a magnifying glass icon. Further right are icons for RSS, email, and Twitter. Below the main title is a horizontal strip with three circular icons: a question mark, a lightbulb, and an exclamation mark. To the left of this strip is the text 'STAY INFORMED' in yellow and white. To the right is the text 'GET OUR NEWSLETTER' in white. At the bottom of the banner is a dark gray bar with the text 'COPYRIGHT 1998-2016 BY HELP NET SECURITY. // READ OUR PRIVACY POLICY // ABOUT US // ADVERTISE //