# Ebury (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:42:19 UTC

elf.ebury (Back to overview)

## Ebury

---

This payload has been used to compromise kernel.org back in August of 2011 and has hit cPanel Support which in turn, has infected quite a few cPanel servers. It is a credential stealing payload which steals SSH keys, passwords, and potentially other credentials.

This family is part of a wider range of tools which are described in detail in the operation windigo whitepaper by ESET.

#### References


2024-05-14 · ESET Research · Marc-Etienne M.Léveillé
Ebury is alive but unseen: 400k Linux servers compromised for cryptocurrency theft and financial gain
Ebury

2024-05-13 · ESET Research · Marc-Etienne M.Léveillé
Ebury is alive but unseen: 400k Linux servers compromised for cryptocurrency theft and financial gain
Ebury

2021-04-21 · CSIRT Italia · CSIRT Italia
Windigo footprints: an Ebury variant
Ebury

2019-06-04 · CERN · CERN Computer Security
Advisory: Windigo attacks
Ebury

2018-12-05 · ESET Research · Marc-Etienne M.Léveillé
The Dark Side of the ForSSHe
Ebury

2018-12-01 · ESET Research · Hugo Porcher, Marc-Etienne M.Léveillé, Romain Dumont
THE DARK SIDE OF THE FORSSHE: A landscape of OpenSSH backdoors
Ebury

2017-10-30 · ESET Research · Frédéric Vachon
Windigo Still not Windigone: An Ebury Update
Ebury

2017-03-28 · Department of Justice · Office of Public Affairs
Russian Citizen Pleads Guilty for Involvement in Global Botnet Conspiracy
Ebury

2014-10-15 · ESET Research · Olivier Bilodeau
Operation Windigo: “Good job, ESET!” says malware author
Ebury

2014-03-01 · ESET Research · Alexis Dorais-Joncas, Benjamin Vanheuverzwijn, Joan Calvet, Marc-Etienne M.Léveillé, Olivier Bilodeau, Pierre-Marc Bureau
OPERATION WINDIGO
Ebury

2014-02-21 · ESET Research · Marc-Etienne M.Léveillé
An In-depth Analysis of Linux/Ebury
Ebury

There is no Yara-Signature yet.

---