Necurs botnet

By Contributors to Wikimedia projects

Published: 2016-06-27 · Archived: 2026-04-05 19:01:33 UTC

From Wikipedia, the free encyclopedia

The **Necurs botnet** is a distributor of many pieces of malware, most notably Locky.

Around June 1, 2016, the botnet went offline, perhaps due to a glitch in the command and control server running Necurs. However, three weeks later, Jon French from AppRiver discovered a spike in spam emails, signifying either a temporary spike in the botnet's activity or return to its normal pre-June 1 state.[1][2]

In a 2020 report, it was noted to have particularly targeted India, Southeast Asia, Turkey and Mexico.[3]

Distributed malware

[edit]

Source:[4]

- Bart
- Dridex
- Locky
- RockLoader
- Globeimposter

- Conficker
- Command and control (malware)
- Gameover ZeuS
- Operation Tovar
- Timeline of computer viruses and worms
- Tiny Banker Trojan
- Torpig
- Zeus (malware)
- Zombie (computer science)

1. ^ *French, Jon (27 June 2016). "Necurs BotNet Back With A Vengeance Warns AppRiver". Retrieved 27 June 2016.*
2. ^ *"Pump and dump spam: Incapta Inc (INCT)". Retrieved 22 Mar 2017.*
3. ^ *"Microsoft Hijacks Necurs Botnet that Infected 9 Million PCs Worldwide". The Hacker News.*
4. ^ *"Hackers behind Locky and Dridex start spreading new ransomware". Retrieved 27 June 2016.*