

# Botnet C&C | FortiGuard Labs

Archived: 2026-04-05 16:28:34 UTC

## EmpireMonkey malware distribution



### Description

This botnet is a type of malware bot that may perform many malicious tasks, such as downloading and executing additional malware, receiving commands from a control server and relaying specific information and telemetry back to the control server, updating or deleting itself, stealing login and password information, logging keystrokes, participating in a Distributed Denial of Service (DDoS) attack, or locking and encrypting the contents of your computer and demanding payment for its safe return.

### Symptoms

Some possible symptoms include, but are not limited to:

- Inability to restart the computer in safe mode
- Inability to open the Windows registry editor
- Inability to open the Windows task manager
- Modification or deletion of certain registry entries
- Significant increase in disk activity
- Significant increase in network traffic
- Connection attempts to known malicious IP addresses
- Creation of new files and directories with obfuscated or random names

### Analysis

A detailed analysis of this specific malware bot is not currently available. Fortinet's team of AV and bot analysts will update this page when a complete analysis is available.



### Instructions

It is not recommended that any attempts to remove this malware be performed manually. Fortinet recommends that you remove this threat by running a complete scan of your system using FortiClient Endpoint Protection.