C

Cobalt Strike Beacon: Legitimate Use, Detection, and Response

Learn what Cobalt Strike Beacon does in authorized red-team work, how attackers abuse leaked versions, and which endpoint and network behaviors aid detection.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What is Cobalt Strike Beacon?
02 What Beacon can do
03 How attackers obtain and use it
04 Endpoint detection opportunities
05 Network detection opportunities
06 False positives and authorized tests
07 Incident-response steps
08 Why deleting Beacon is insufficient

Cobalt Strike Beacon is the post-exploitation payload associated with the commercial Cobalt Strike adversary-simulation platform. Authorized red teams use it to model attacker behavior and test defenses. Threat actors also abuse cracked, leaked, or unauthorized versions after gaining access to a network.

Finding Beacon-like activity is serious, but a product name alone does not explain the initial entry point or the full scope. Defenders need to investigate the surrounding process, identity, and network behavior.

01 What is Cobalt Strike Beacon?

Beacon is Cobalt Strike's command-and-control payload for actions performed after initial access. It periodically contacts a Cobalt Strike team server, receives tasks, returns results, and can be configured to use different timing and network profiles. Cobalt Strike is a legitimate commercial red-team platform; an unexpected Beacon on a production system should nevertheless be handled as a potential intrusion until authorization is confirmed.

02 What Beacon can do

Depending on configuration and access, Beacon can run commands, execute payloads, move files, collect system information, proxy traffic, and support credential or lateral-movement operations. It communicates with team-server infrastructure using configurable profiles and sleep intervals designed for adversary simulation.

These capabilities can be legitimate only within an explicitly authorized test scope.

03 How attackers obtain and use it

Attackers may deploy Beacon after phishing, stolen credentials, exploitation, or another malware loader. It is usually a post-compromise tool rather than proof of how the intrusion began. Criminal and state-linked operations have used it because its flexible communications and mature features reduce development effort.

04 Endpoint detection opportunities

- An Office application, browser, or public-facing service spawning an unexpected shell or script interpreter.
- Suspicious memory allocation, injection, or execution inside another process.
- Unusual named pipes, token manipulation, or credential-access behavior.
- System discovery followed by remote-service or lateral-movement activity.
- Unsigned or unexpected binaries and scripts in user-writable locations.

No single artifact identifies every Beacon configuration. Detect technique chains and deviations from the normal behavior of the host.

05 Network detection opportunities

Look for regular or jittered beaconing, rare destinations, unusual HTTP headers, small repeated requests, abnormal TLS characteristics, or DNS patterns inconsistent with the initiating process. Custom malleable profiles can change observable details, and legitimate web traffic can resemble individual signals. Correlate network observations with endpoint and identity telemetry.

06 False positives and authorized tests

Maintain a controlled record of approved red-team infrastructure, time windows, users, and objectives, but do not broadly suppress matching alerts. The defensive team may need realistic validation while still distinguishing an external intrusion. An expired test window or activity outside scope should be investigated normally.

07 Incident-response steps

1. Isolate affected hosts while preserving memory, process, and network evidence.
2. Identify the parent process, user, privilege level, and first observed activity.

3. Block confirmed command infrastructure and search across all telemetry.
4. Determine the initial access path and any credential exposure.
5. Remove persistence, rotate affected secrets, and rebuild when integrity is uncertain.
6. Map observed behavior to ATT&CK techniques to guide the hunt, not as proof of attribution.

08 Why deleting Beacon is insufficient

An operator may have created accounts, stolen tokens, installed other backdoors, changed cloud permissions, or moved to systems without endpoint agents. Eradication must address access and persistence throughout the environment. Review the related command-and-control and incident timeline, not only one executable.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com