jamf

Beacon by Jamf Threat Labs

Threat hunting service for macOS

Enterprise Mac adoption continues to increase, and so does interest from threat actors. Mac-specific **tactics, techniques and procedures** (TTPs), malware variants and delivery methods continue to evolve alongside macOS security frameworks. Because of its unique nature, organizations struggle to start, scale, repeat and measure effective Mac threat hunting programs.

Beacon by Jamf Threat Labs solves this challenge.

Beacon is a Mac-focused threat hunting service delivered by Jamf Threat Labs – a team of security researchers, analysts and engineers who publish Mac malware research and develop the detection engines that drive Jamf's platform.

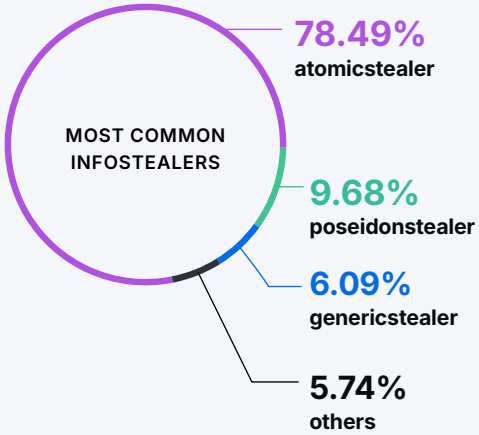
The service is designed to detect, analyze and report the macOS threats that traditional security tools and teams leave under-monitored. The team's Apple expertise gives insight into the TTPs of threat actors, the vulnerabilities they look to exploit and how to identify gaps in macOS configurations.

Key benefits

- Enhance Mac threat hunting with industry-leading Mac security knowledge
- Maintain operational control with step-by-step remediation guidance
- Stay informed with personalized monthly reports on emerging threats and Mac security posture

Examples of threats **Beacon detects** and **reports**:

- Supply chain attacks containing trojanized packages
- Malicious code execution in VSCode or Xcode projects
- ClickFix social engineering
- DPRK backdoors from fake job lures
- And more.



Threat Labs

2026 Mac Security 360

The power of Jamf Threat Labs securing your Mac environment

macOS expertise

Dedicated Mac threat hunting service

- Researchers who understand macOS threat landscape, macOS internals and attacker behaviors
- Jamf telemetry built on Apple's Endpoint Security API provides deeper visibility into macOS
- Direct access to Jamf Threat Labs for questions about your Apple security posture

Deep intelligence

Contextualized Apple threat intelligence at scale

- Telemetry sweeps for emerging Apple-specific attack techniques, Indictors of Compromise, and hidden malware
- Retro hunting searches telemetry up to one year back for previously unknown threat indicators
- Uses Jamf Threat Labs written hunting rules that improve detection alerts for novel malware, suspicious behaviors and TTPs. *Hosted in Jamf Cloud.*

Operational control

Own your environment — Beacon enhances its security

- Collaborate with Jamf Threat Labs to implement personalized remediation steps to organizational requirements
- Receive monthly security reports highlighting organizational security score, blocked Mac malware, emerging threats and more
- Maintain full control while benefiting from expert guidance

How Beacon works:

1. **Configure**

Jamf configures your telemetry, enabling Jamf Threat Labs to hunt for threats.

2. **Hunt**

Jamf Threat Labs applies intelligence to identify macOS attacks, TTPs, and IOCs.

3. **Report**

Jamf Threat Labs delivers actionable guidance (workflows, scripts) for active threat response.

Every month, Jamf Threat Labs sends reports detailing your security environment and posture.

4. **Respond**

Security team remains in charge of containment, remediation and policy changes – response backed by Jamf Threat Labs analysis and counsel.

Beacon by Jamf Threat Labs.
Measurable, repeatable threat hunting that scales with your Mac fleet.

jamf

www.jamf.com

To learn more, reach out to your preferred reseller or Jamf representative. Or contact us today.