HADRIAN

Infostealer Infection Detection

Infostealers are surging—16 times more infections occurred in 2025 than in 2020. This insidious malware extracts sensitive data and session tokens from unmanaged devices, giving attackers full access to accounts and systems, even bypassing MFA. Hadrian's partner Passguard ethically infiltrates criminal marketplaces to monitor infostealer data that could be used to compromise your organization.

- Hadrian's partnership with Passguard allows for the ethical infiltration of criminal marketplaces where infostealer logs are traded. This gives you visibility over ongoing infections—revealing compromised devices, session details, malware type, and more. You can assess exposure, target response where it matters, and act before attackers do.
- No set-up is required and you never have to share your sensitive data in order to start with Infostealer Infection Detection. A full scan of criminal marketplaces on the dark web identifies all current infections with access to your system, contextualizes them, then sends you a prioritized list of potential threats with remediation advice.
- This approach doesn't merely alert you to infostealers—it allows you to be proactive when it comes to eliminating risks from infostealers infections.

Key Benefits

- **Early detection of compromises**

  Stay ahead of potential breaches by receiving real-time insights into infostealer activity from criminal marketplaces–so you can protect your data before a breach.

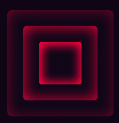
- **Straight-forward, actionable intelligence**

  Get clear information about what data has been compromised and when it happened, allowing your team to take quick and effective action.

- **Cover blindspots left by unmanaged devices**

  Proactively strengthen security posture by maintaining visibility of infected unmanaged devices with access to your network.

Key Differentiators

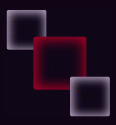


Infostealer marketplace coverage

Industry-leading breadth and depth via infiltration of infostealer marketplaces—outperforming alternative threat intelligence sources.

Comprehensive insights

Gain detailed information on infected devices, compromised credentials and session data, and malware specifications for swift action.

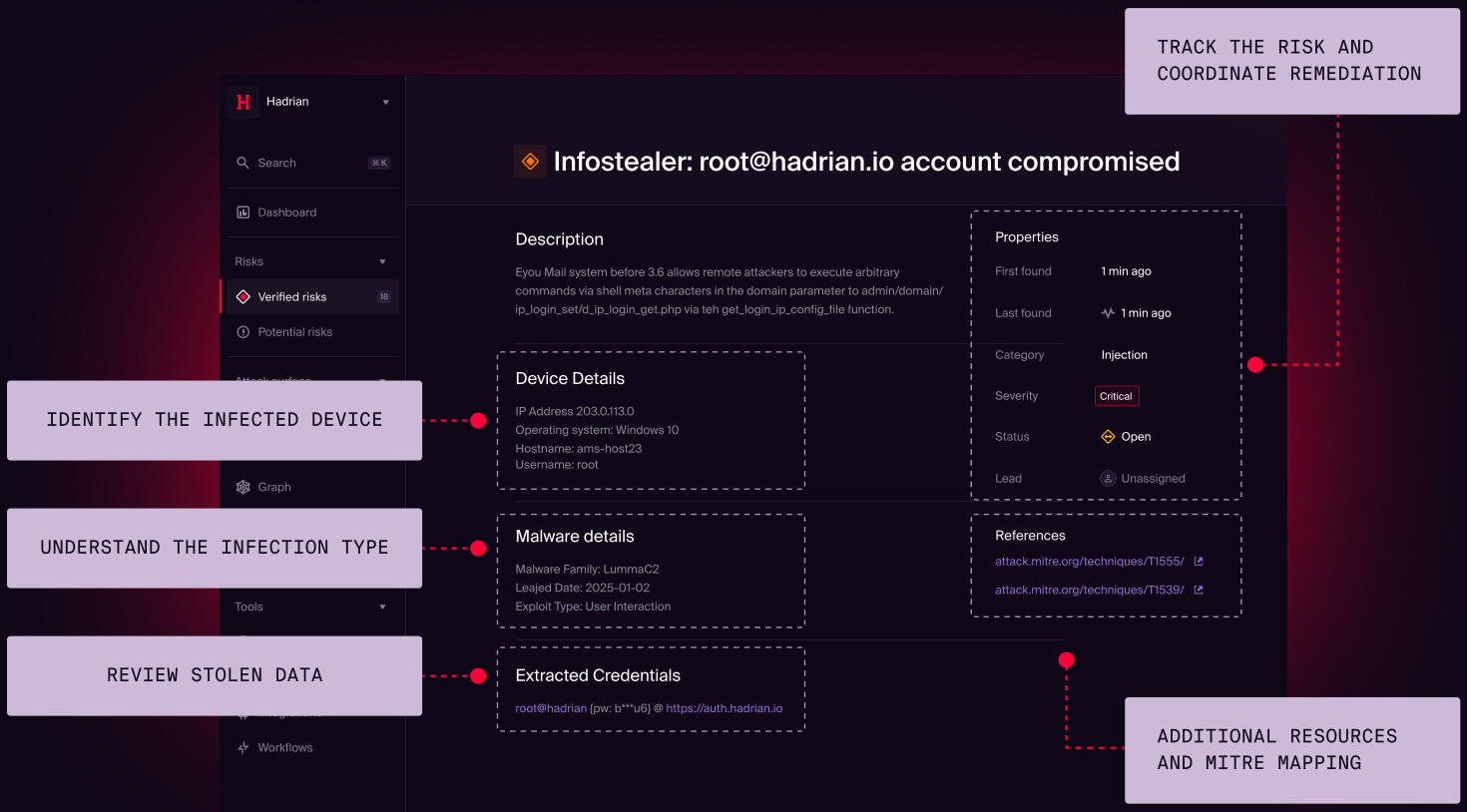


Ethical dark web infiltration

Infostealer marketplaces are ethically infiltrated using techniques that avoid direct interaction with threat actors or illegal data acquisition.

HADRIAN

Stop the infostealer threat



- **Continuous monitoring**

  Marketplaces are monitored around the clock so that you can take action the moment your data appears.

- **Zero false positives**

  To ensure accuracy, multiple signals are correlated, including domain, email, timestamps, metadata, and more.

- **Secure unmanaged devices**

  Infostealer malware targets unmanaged devices. Our monitoring provides you visibility of an infection.

- **Context-based prioritization**

  Intelligent risk scoring prioritizes the most critical stolen data based on asset importance.

- **Zero-touch deployment**

  No installation or agent setup is required, real-time visibility of infostealer infections is collected from the dark web.

- **Data breach monitoring**

  In addition to data stolen by infostealers, you can view all credential leaks from data breach dumps.

About Hadrian

Hadrian's AI-driven offensive security provides real-time visibility of how a hacker would begin an attack against your organization. The platform provides visibility of zero-day threats, OWASP issues, cloud misconfigurations and infostealer infections.. The cloud-based, agentless technology is constantly updated and improved by Hadrian's ethical hacker team, so businesses can stay several steps ahead of bad actors.