2024 Threat Detection Report & Midyear Update

This in-depth look at the most prevalent trends, threats, and ATT&CK® techniques is designed to help you and your team focus on what matters most.

READ UPDATE ›

SEE 2024 PDF ›

START HERE

GETTING STARTED

based on in-depth analysis of nearly 60,000 threats detected across our 1,000+ customers’ **endpoints, networks, cloud infrastructure, identities, and SaaS applications** over the past year.

This report provides you with a comprehensive view of this threat landscape, including new twists on existing adversary techniques, and the trends that our team has observed as adversaries continue to organize, commoditize, and ratchet up their cybercrime operations.

some of our key findings:

- **Everyone is migrating to the cloud, including bad guys: Cloud Accounts was the fourth most prevalent ATT&CK technique we detected this year, increasing 16-fold in detection volume and affecting three times as many customers as last year.**

- **Despite a spate of new CVEs, humans remained the primary vulnerability that adversaries took advantage of in 2023. Adversaries used compromised identities to access cloud service APIs, execute payroll fraud with email forwarding rules, launch ransomware attacks, and more.**

- **While both defenders and cybercriminals have discovered use cases for generative artificial intelligence (GenAI), we see defenders as having the edge.**

- **Container technology is omnipresent, and it's as important as ever to secure your Linux systems to prevent adversaries from escaping to host systems.**

along with instances of reflective code loading and AppleScript abuse.

- **Often dismissed, malvertising threats delivered payloads far more serious than adware, as exemplified by the Red Canary-named Charcoal Stork, our most prevalent threat of the year, and related malware ChromeLoader and SmashJacker.**
- **Our new industry analysis showcases how adversaries reliably leverage the same small set of 10-20 techniques against organizations, regardless of their sector or industry.**

We also check back on the timeless **threats** and **techniques** that are prevalent year-after-year, explore emerging ones that are worth keeping an eye on, and introduce two new **free tools** that security teams can start using immediately.

Use this report to:

- Explore the most prevalent and impactful **threats**, **techniques**, and **trends** that we've observed.

infrastructure, and applications.

- Learn how to emulate, mitigate, and detect specific threats and techniques.
- Shape and inform your readiness, detection, and response to critical threats.

BEHIND THE DATA

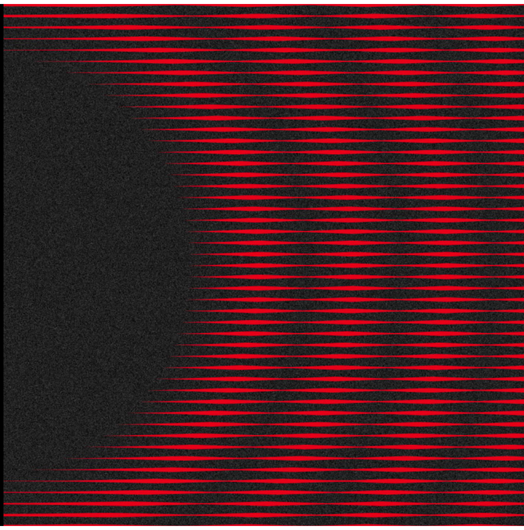
Methodology

The Threat Detection Report sets itself apart from other annual reports with its unique data and insights derived from a combination of expansive detection coverage and expert, human-led investigation and confirmation of threats. The data that powers Red Canary and this report are not mere software signals—this data set is the result of hundreds of thousands of expert investigations across millions of protected systems. Each of the nearly 60,000 threats that we responded to have one thing in common: These threats weren't prevented by our customers' expansive security controls—they are the product of a breadth and depth of analytics that we use to detect the threats that would otherwise go undetected.

READ MORE ABOUT HOW WE COUNT ›

ACKNOWLEDGMENTS

Thanks to the dozens of security experts, writers, editors, designers, developers, and project managers who invested countless hours to produce this report. And a huge thanks to the **MITRE ATT&CK®** team, whose framework has helped the community take a giant leap forward in understanding and tracking adversary behaviors. Also a huge thanks to all the Canaries—past and present—who have worked on past **Threat Detection Reports** over the last six years. The Threat Detection Report is iterative, and parts of the 2024 report are derived from previous years. This report wouldn't be possible without all of you!



Search ›

- Managed Detection and Response (MDR)
- Readiness Exercises
- Linux EDR
- Atomic Red Team™
- Mac Monitor
- What's New?
- Plans

- Deliver Enterprise Security Across Your IT Environment
- Get a 24×7 SOC Instantly
- Protect Your Corporate Endpoints and Network
- Protect Your Users' Email, Identities, and SaaS Apps
- Protect Your Cloud
- Protect Critical Production Linux and Kubernetes
- Stop Business Email Compromise
- Replace Your MSSP or MDR
- Run More Effective Tabletops
- Train Continuously for Real-World Scenarios
- Operationalize Your Microsoft Security Stack
- Minimize Downtime with After-Hours Support

RESOURCES

- View all Resources
- Blog
- Integrations
- Guides & Overviews
- Cybersecurity 101
- Case Studies
- Videos
- Webinars
- Events
- Customer Help Center
- Newsletter

PARTNERS

- Overview
- Incident Response
- Insurance & Risk
- Managed Service Providers
- Solution Providers
- Technology Partners
- Apply to Become a Partner

COMPANY

- About Us
- The Red Canary Difference
- News & Press
- Careers – We're Hiring!

info@redcanary.com
+1 855-977-0686 Privacy Policy Trust Center and Security Cookie Settings