DARKTRACE

■ Executive summary

Annual Threat Report 2025

At Darktrace, the incidents detected by our AI across the customer fleet mark the beginning of a deeper investigation. Our analysts and researchers aim to connect mitigated threats to wider trends from across the threat landscape. Through hindsight analysis, we have highlighted numerous threats, showcasing the evolving nature of cyber-attacks and Darktrace's ability to identify them.

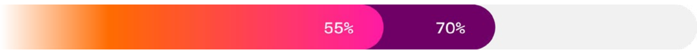
Multiple campaigns target vulnerabilities in internet-facing systems

The most significant campaigns involved the exploitation of zero-day and n-day vulnerabilities in edge and perimeter network technologies. In the first half of the year, these threats against **internet-facing devices accounted for 40% of identified campaign activity.**

- **Ivanti Connect Secure (CS) and Ivanti Policy Secure (PS)**
  CVE-2023-46805 and CVE-2024-21887
- **Palo Alto Network (PAN-OS) firewall devices**
  CVE 2024-3400
- **Fortinet – FortiManager**
  CVE 2024-47575

Onslaught of email threats continues

Between December 21, 2023, and December 18, 2024, Darktrace / EMAIL detected over 30.4 million phishing emails across the fleet. Of these, **70%** successfully bypassed Domain-based Message Authentication, Reporting, and Conformance (DMARC) verification checks and **55%** passed through all other existing layers of customer email security **before being detected by Darktrace.**



Attackers increasingly target industrial systems

The Threat Research team investigated numerous Operational Technology (OT) attacks, **more than doubling the number of OT investigations from the previous year**. The team tracked new tailored malware for Industrial Control Systems (ICS), joint warnings from government agencies, and potential compromises from Darktrace / OT customers. This highlighted that targeting OT systems is becoming increasingly achievable, a trend that is likely to continue.

Download the full report

Discover the latest threat landscape trends and recommendations from the Darktrace Threat Research team.

DARKTRACE
Annual Threat Report 2024
Ransomware: Persistent threats and emerging strains

Persistent ransomware threats and emerging strains remain a top concern

Both novel and re-emerging strains of ransomware challenged the customer fleet. Notable attack trends included using phishing emails as an attack vector, exploiting legitimate tools to mask C2 communication, and exfiltrating data to cloud storage services.

Prominent ransomware actors:

- Akira Ransomware
- LockBit Ransomware
- Lynx Ransomware
- Fog Ransomware
- RansomHub Ransomware