Cyber attack trends: A real-world view

The Attacker Behavior Industry Report from Vectra® provides a first-hand analysis of active and persistent attacker behaviors inside enterprise networks from January-March 2017.

Vectra cyber attack detections by the numbers

2,145,708
hosts observed in **90** days

1,805,188
different network behaviors flagged

140,341
detections

Triaged down to
62,119
hosts

3,720 hosts were tagged as **critical** and **6,987** were tagged as **high**, enabling security analysts to quickly mitigate the highest-risk threats.

Automation efficiency boost:
29x
Vectra automatically identifies suspicious hosts so you can quickly respond and mitigate threats.

Industries under siege

Healthcare and education had the most attack behaviors, pointing to openness and exposure.

Entertainment and healthcare had the widest range of cyber attacker behaviors.

Finance and technology had below-median detection rates due to strong policies and maturity.

Four real-world scenarios

Ransomware
Ransomware extorted millions of dollars from people and enterprise organizations.

Unsecure web apps
Exploiting web application vulnerabilities can be a prelude to a targeted attack.

IoT botnets IoT devices make a ripe attack surface. They can't run endpoint security and are rarely patched.

Unintentional insider threat
Accidental loss of intellectual property carries the same risk as a targeted attack.

Get more insight into the attack lifecycle and trends.
Download the Attacker Behavior Industry Report.

VECTRA®
Security that thinks®
vectra.ai