halcyon

Deconstructing Ransomware Operations

From Initial Access to Triple Extortion, What to Expect in 2026

halcyon.ai

The **Halcyon Ransomware Research Center** unites experts, drives smart policies, and delivers actionable intelligence to detect, disrupt, and defeat ransomware.

Unite Experts and Defenders

We bring together cybersecurity experts, government officials, and international partners to share knowledge, close critical gaps, and take decisive action against ransomware.

Drive Public Policy

We identify policy challenges and deliver data-driven options to solve ransomware challenges through smart sources, quality research, and trust-based consensus building with our public and private industry partners.

Advance Understanding

From in-depth ransomware analysis to practical threat intelligence, we deliver insights designed to be clear, actionable, and impactful at every stage of defense.

halcyon | Ransomware Research Center

halcyon.ai/ransomware-research

The Ransomware Reality

8000+ Ransomware Attacks

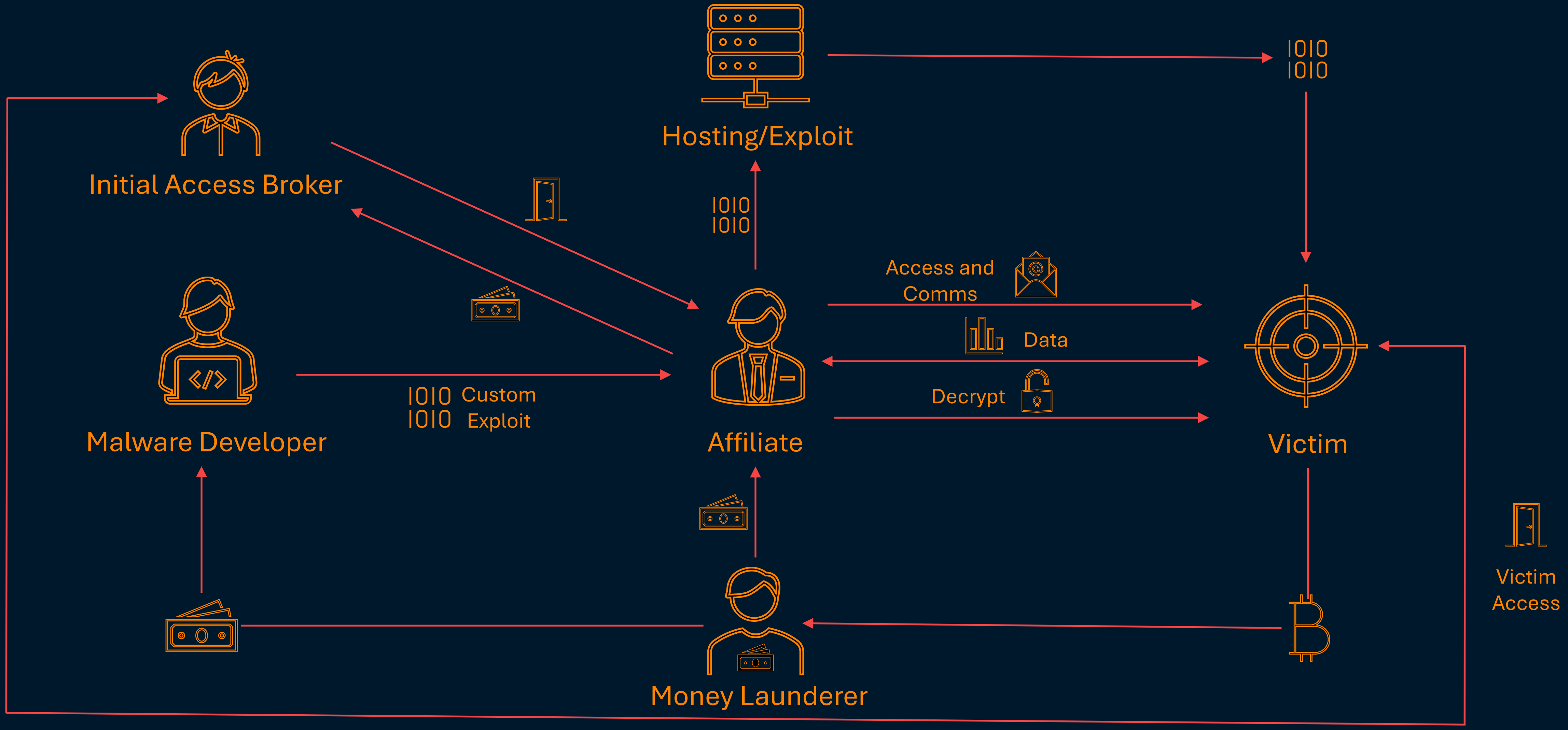
Reported or claimed by threat actors globally in 2025

19 Attack Attempts
Every Second in 2024

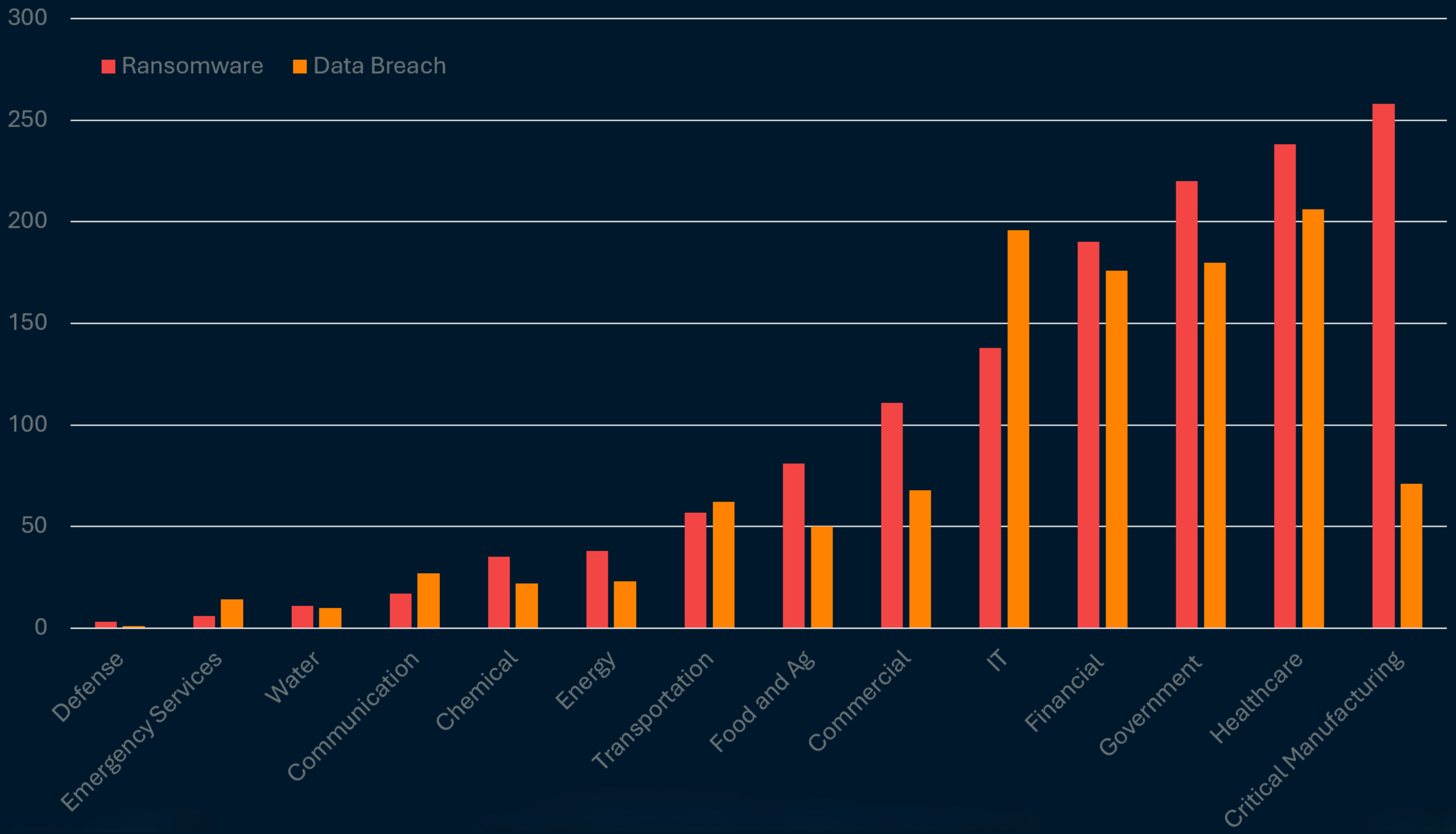
$5,130,000
Average Recovery Cost

22 Days of Downtime
Average Time for Recovery

Ransomware-as-a-Service

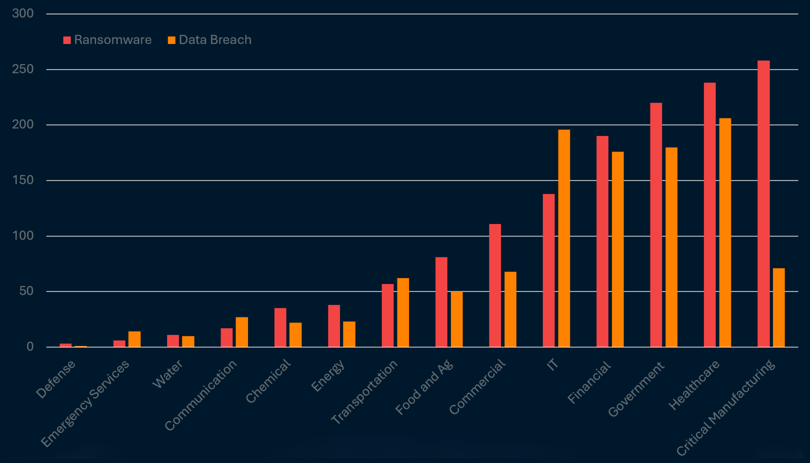


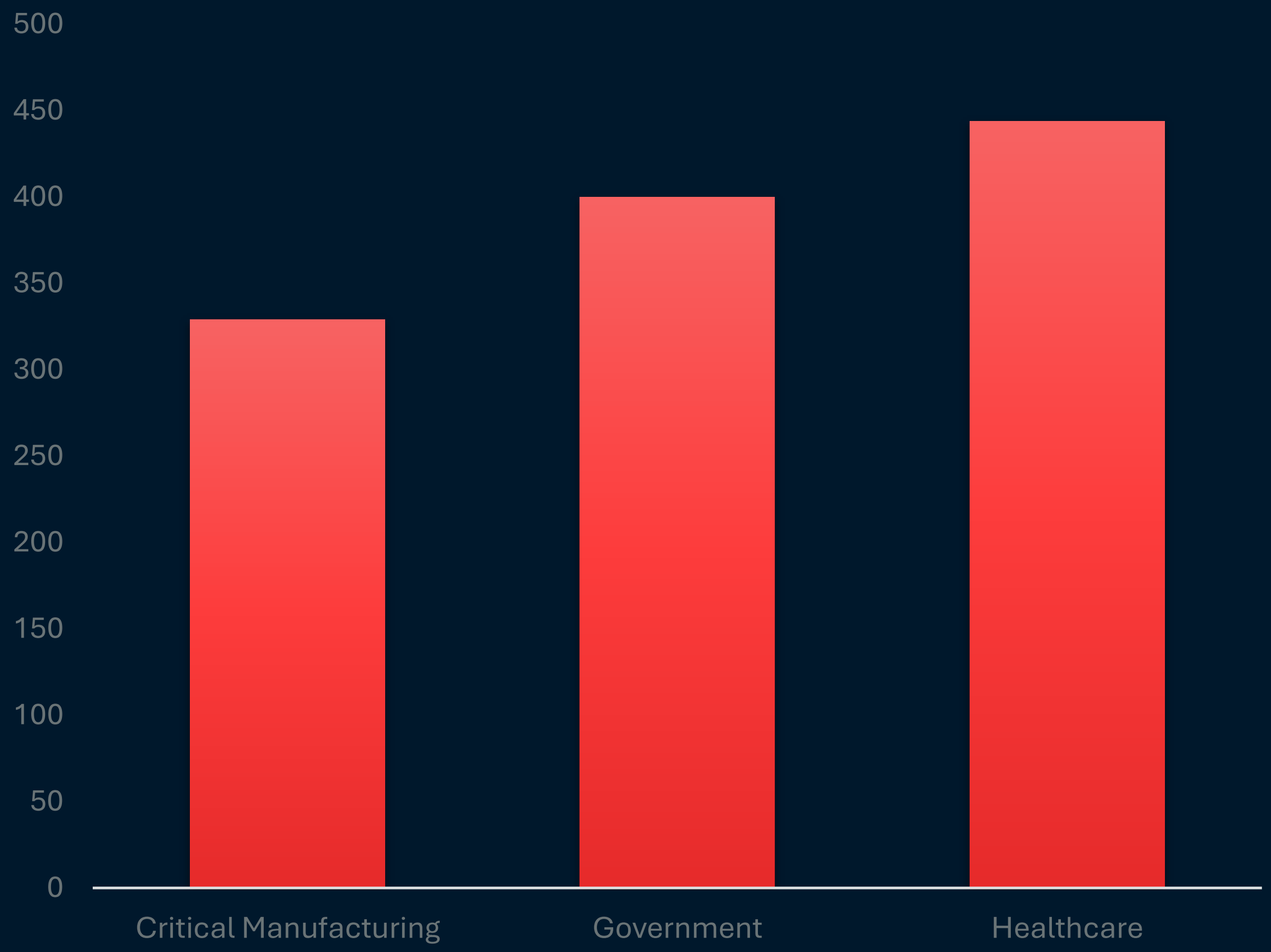
Ransomware and Data Breach By Sector



Source: FBI Internet Crime Complaint Center

Ransomware and Data Breach By Sector





Source: FBI Internet Crime Complaint Center

No Guarantees

Not All Data is Recovered

On average, 65% of data recovered after paying ransom.

For one in five cases, decryptors fail entirely or corrupt files.

Repeat Attacks Are Common

78% of organizations that paid were attacked again.

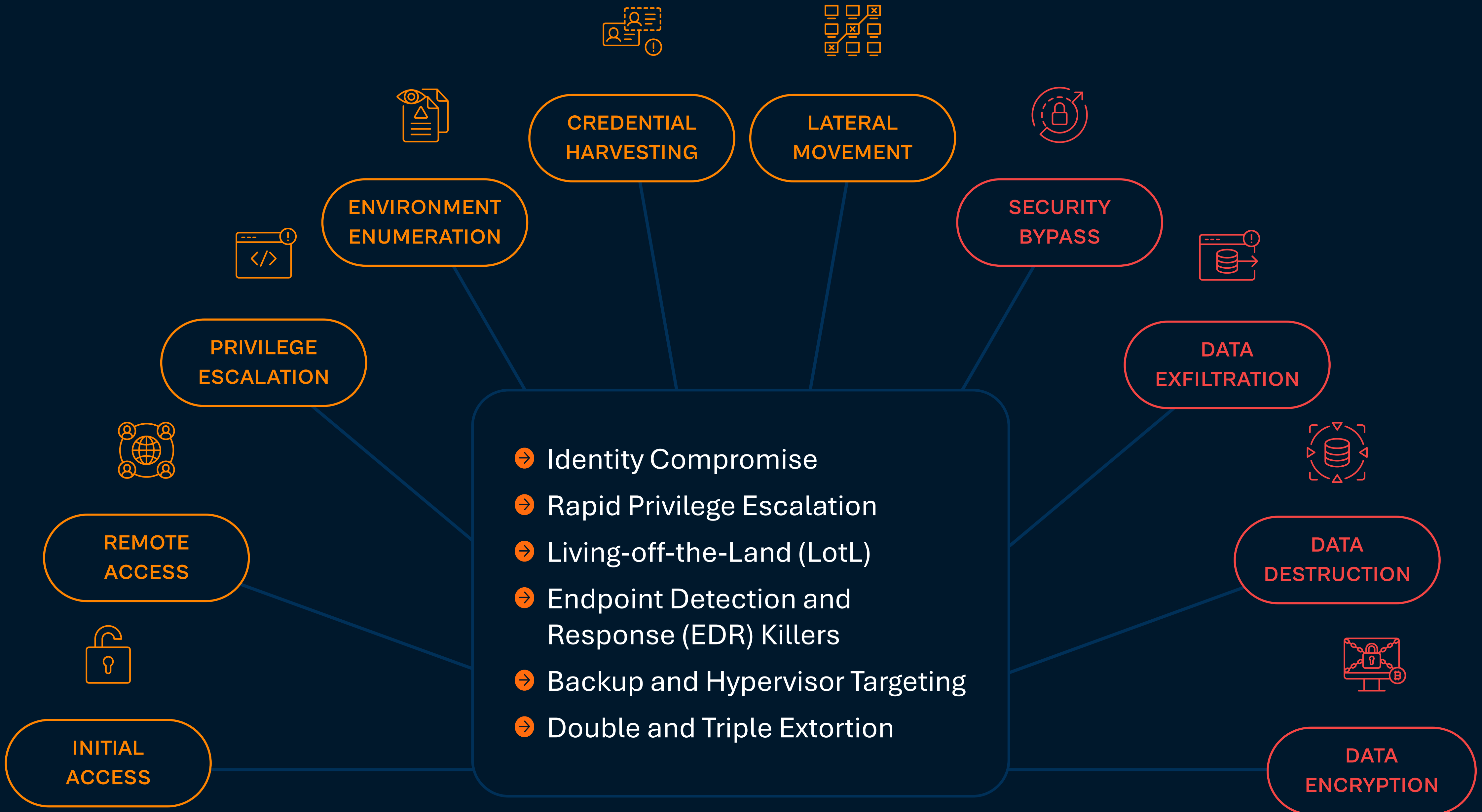
Of those, 36% were hit by the same threat actor.

The Threat Landscape is Changing

The number of ransomware groups is increasing

The fastest growing threat is speed

Targeting has shifted from opportunistic to strategic



INITIAL ACCESS

REMOTE ACCESS

PRIVILEGE ESCALATION

ENVIRONMENT ENUMERATION

CREDENTIAL HARVESTING

LATERAL MOVEMENT

SECURITY BYPASS

DATA EXFILTRATION

DATA DESTRUCTION

DATA ENCRYPTION

- Identity Compromise
- Rapid Privilege Escalation
- Living-off-the-Land (LotL)
- Endpoint Detection and Response (EDR) Killers
- Backup and Hypervisor Targeting
- Double and Triple Extortion

How Modern Ransomware Operations Work

Why Ransomware Works So Well

Identity is still too easy to abuse

Anti-virus and EDR systems are relentlessly targeted

Defenders are not optimized for speed

Nation-State Overlaps

Nation-state and criminals increasingly indistinguishable

Zero Days
Identity/Authentication Abuse
Living Off the Land
Data Theft First

Nation states masquerade as cyber criminals

Iranian attacks against Albania in 2022 deployed ransomware to hide more destructive operations

What to Expect in 2026

Prediction #1

The Number of Attacks Will Go Up (and Many Attackers Will be Amateurs)

Prediction #2

AI-Enhanced Social Engineering Will Become the #1 Initial Access Vector

Prediction #3

Faster, Fully Automated Ransomware Campaigns

Hardening Against Increasingly Advanced Ransomware Operations

Ask the Right Questions

Are we clear on our current security posture and incident readiness?

Where are we knowingly accepting risk—and why?

What workforce, funding, or policy constraints prevent improvement?

Practice Incident Response

What services stay online?

What stops?

Who decides?

Who speaks?

Prioritize Defense in Depth

Assume you will be compromised

Layer your defenses

Go Beyond Signature-Based Detection

Deployadvanced protection that includes behavior-based detection halcyon

Thank You

Questions? Contact us at Ransomware-Research-Center@halcyon.ai

Visit us at www.halcyon.ai/ransomware-research

halcyon.ai