You don’t have a malware problem

You have an adversary problem

https://cyberyog.com/partners/crowdstrike/

Global Adversaries: The growing threat actor landscape

257

Total Tracked

140

Malicious Activity Clusters

26

New Adversaries

https://cyberyog.com/partners/crowdstrike/

DECRYPTING THE THREAT MATRIX: CROWDSTRIKE NAMING CONVENTIONS

NATION-STATE (CHINA)	PANDA	e.g., MUSTANG PANDA, WICKED PANDA
NATION-STATE (RUSSIA)	BEAR	e.g., FANCY BEAR, COZY BEAR
NATION-STATE (IRAN)	KITTEN	e.g., CHARMING KITTEN, NEMESIS KITTEN
NATION-STATE (NORTH KOREA)	CHOLLIMA	e.g., FAMOUS CHOLLIMA, LABYRINTH CHOLLIMA
eCRIME / CRIMINAL	SPIDER	e.g., ALCHEMIST SPIDER, SCATTERED SPIDER
HACKTIVIST	JACKAL	e.g., BOUNTY JACKAL, RENEGADE JACKAL

EMERGING VECTORS

Other active origin clusters:

India → TIGER

Pakistan → LEOPARD

Turkey → WOLF

https://cyberyog.com/partners/crowdstrike/

Insider Threats Lead to Breaches and Financial Losses

50%

of organizations experienced insider incidents in 2023.

$16.2M

Average annual cost of insider threats.

71%

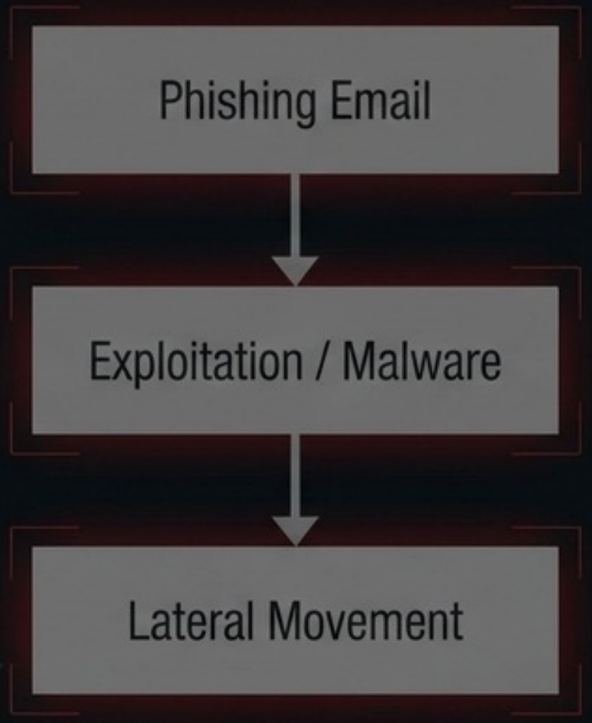
of insider incidents resulted in data exfiltration.

https://cyberyog.com/partners/crowdstrike/

https://cyberyog.com/partners/crowdstrike/

The Perimeter is Obsolete: Bypassing the Kill Chain

Traditional Cyber Kill Chain



Modern Insider Infiltration

https://cyberyog.com/partners/crowdstrike/

Adversary Deep Dive

FAMOUS CHOLLIMA

Origin Classification

North Korea

Operating Method

Legitimate internal employment leveraging synthetic or stolen identities to infiltrate corporate environments.

CROWDSTRIKE

https://cyberyog.com/partners/crowdstrike/

DECLASSIFIED INTELLIGENCE DOSSIER

The Threat Identity Web: Consolidating the Intelligence

Disparate industry names track back to a single, highly coordinated CrowdStrike-tracked adversary.

https://cyberyog.com/partners/crowdstrike/

DECLASSIFIED INTELLIGENCE DOSSIER

The Geographic Blast Radius

EUROPE

Austria

Estonia

France

Italy

Spain

Switzerland

https://cyberyog.com/partners/crowdstrike/

The Infiltration Equation

When the adversary logs in with valid credentials, traditional perimeter security becomes an accomplice. Security must evolve into active counter-espionage.

https://cyberyog.com/partners/crowdstrike/

CrowdStrike Solutions: The Internal Immune System

CROWDSTRIKE

https://cyberyog.com/partners/crowdstrike/