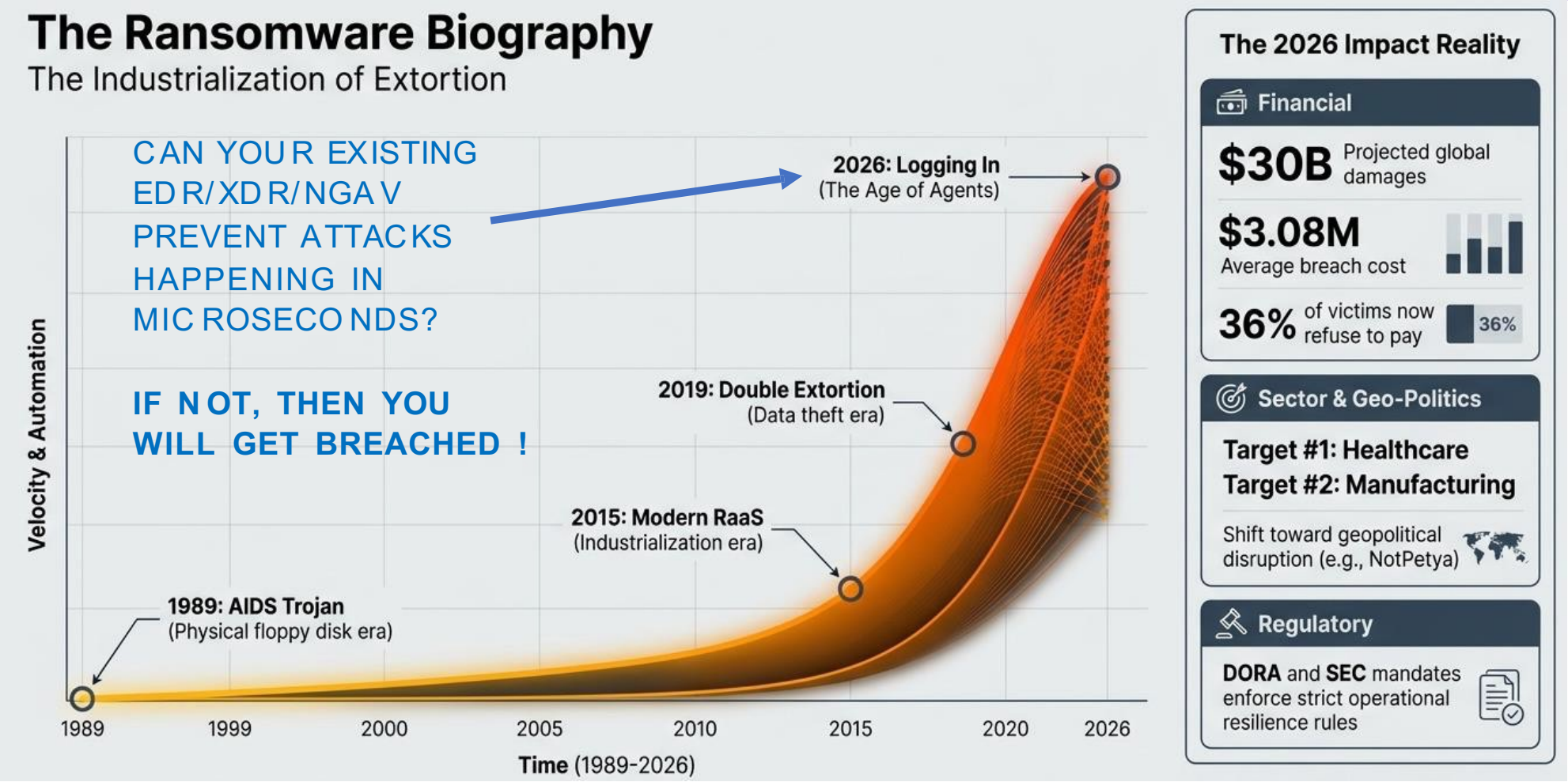
A Decade of Threat Evolution

ArmorxAI

INFLECTION POINT — EXPONENTIAL THREAT MODEL ACCELERATION



"Detection-and-response was built for an attacker that gives you seconds to react. AI-orchestrated kill chains give you microseconds."

Why the Existing Stack Breaks

ArmorxAI

MYTHOS JUST INVALIDATED EVERY EXISTING CATEGORY ASSUMPTION.

EDR

01. EDR / XDR

CrowdStrike · SentinelOne · Palo Alto

Assumption: Behavioral anomaly detection catches novel threats post-execution.

BREAKS WHEN:

Mythos generates malware with zero known signatures. AI variants evade behavioral baselines in real time. Attacks happen in microseconds that bypass traditional defense.

NGAV

02. Anti-Malware / NGAV

Sophos · McAfee · Symantec

Assumption: Signature databases are updated fast enough to keep pace with malware evolution.

BREAKS WHEN:

AI generates polymorphic payloads faster than signature updates can ship rendering NGAV ineffective against attacks happening in microseconds.

BCK

03. Backup & Recovery

Rubrik · Cohesity · Veeam

Assumption: Immutable backups ensure business recovery within hours.

BREAKS WHEN:

24-day dwell-time assumption collapses when AI actors achieve objectives in < 1 ms.

ZT

04. Zero-Trust Resilience

Halcyon

Assumption: Micro-segmentation and least-privilege limit the blast radius of any breach.

BREAKS WHEN:

AI kill chains move laterally before segmentation policies can enforce isolation.

The Ransomware Kill Chain

ArmorxAI

01

BEACON DOWNLOAD & C2 STAGING

3 IOAs

FILELESS BEACON - *increasingly preferred*

C2 CONNECTIONS – *near universal in 90% of attacks*

TIME SHARE: 22%

02

PERSISTENCE & PRIVLIEGE ESCALATION

4 IOAs

CRDENTIAL HARVESTING – *present in nearly every attack (85%)*

REGISTRY PERSISTENCE – *increasing to 50% of attacks*

TIME SHARE: 18%

03

EXECUTION & INJECTION

7 IOAs

PROCESS HOLLOWING – *most prevalent technique (65%)*

BYOVD – *fastest growing (nearly tripled in last 3 years)*

TIME SHARE: 32%

04

LATERAL MOVEMENT & PROPOGATION

3 IOAs

BULK FILE ACCESS (pre-encryption) – *increasingly used in 75% of attacks*

SHADOW COPY DELETION – *still used in 70% of attacks*

TIME SHARE: 20%

05

POST EXPLOITATION

3 IOAs

DEFENSE DISABLING & ANTI ANALYSIS – *BYOVD is driving this up*

LIVE-OFF-THE-LAND SCRIPT ABUSE – *Risen to one in every 3 attacks*

TIME SHARE: 8%

EDR fires at Stage 5 — after encryption has begun and is 4 min to 60 min late

RansomArmor: IOA interception occurs before execution (at Stage 1) — in milliseconds

Anubis Ransomware-as-a-service (RaaS) Evidence

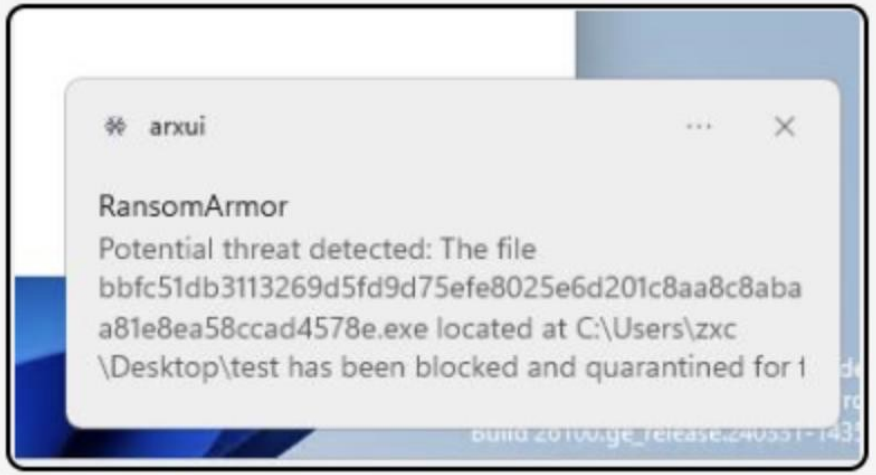
ArmorxAI

Anubis threat actors have publicly listed approximately 70 victims since inception in February 2024. Six healthcare breaches:

- Pound Road Medical Center (Australia, Nov 2024)
- Ambleside (NC, Aug 2024)
- Dermatology Associates of Concord (MA, Sept 2025)
- AllerVie Health (TX, Oct 2025)
- Mid-South Pulmonary & Sleep Specialists (TN, Nov 2025).

RansomArmor successfully blocked and killed Anubis in milliseconds: Screenshots below:

If your current anti-ransomware tool cannot stop this new attack surface, then you need RansomArmor



File icon (PE):	
dhash icon	499676ce96cc718e (1 x RedLineStealer, 1 x Anubis, 1 x Wabot)
Reporter	petikvx
Tags:	Anubis exe Ransomware