UMBC

Ransomware in Active Directory: A Dataset and Analysis of Early-Stage Behavior

Prajna Bhandary, Charles Nicholas, RJ Joyce, Bojing Li

December 8, 2025

Presented at Cyber Security Experimentation and Test Workshop (CSET'25)

*https://umbc-dream-lab.github.io/

Outline

- Significant Findings
- Motivation
- Related Work
- Methodology
- Results
- Conclusion
- Future Work

Significant Findings

- Early-Stage behaviors are distinctive across ransomware families
- Early-Stage orderings are stable across runs
- Family templates separate behaviors
- A reproducible AD-centric dataset created

Motivation

- **Ransomware:** still violating SLAs and peace of mind since the early 2000s
- Limited or close to **“no”** publicly available ransomware datasets
- **“minutes”** rather than **“hours”** are important
  - Responders must know where to look

➢ What happens in the **first few minutes**, and how do these early minutes **differ across** families and host roles?

Related Work

Ransomware and AD Focused

- ❑ Keyogeg et al. – ML detection using AD Domain Services logs
- ❑ McDonald et al. – ransomware disrupting Windows Server services
- ❑ Hampton et al. – API-level behavioral signatures
- ❑ Herrera-Silva et al. – dynamic traces + ML detection

Key Limitation Across These Works

- ❑ Almost all studies analyze single machines, post-infection behavior, or non-AD telemetry.

Related Work, contd.

Machine Learning Approaches

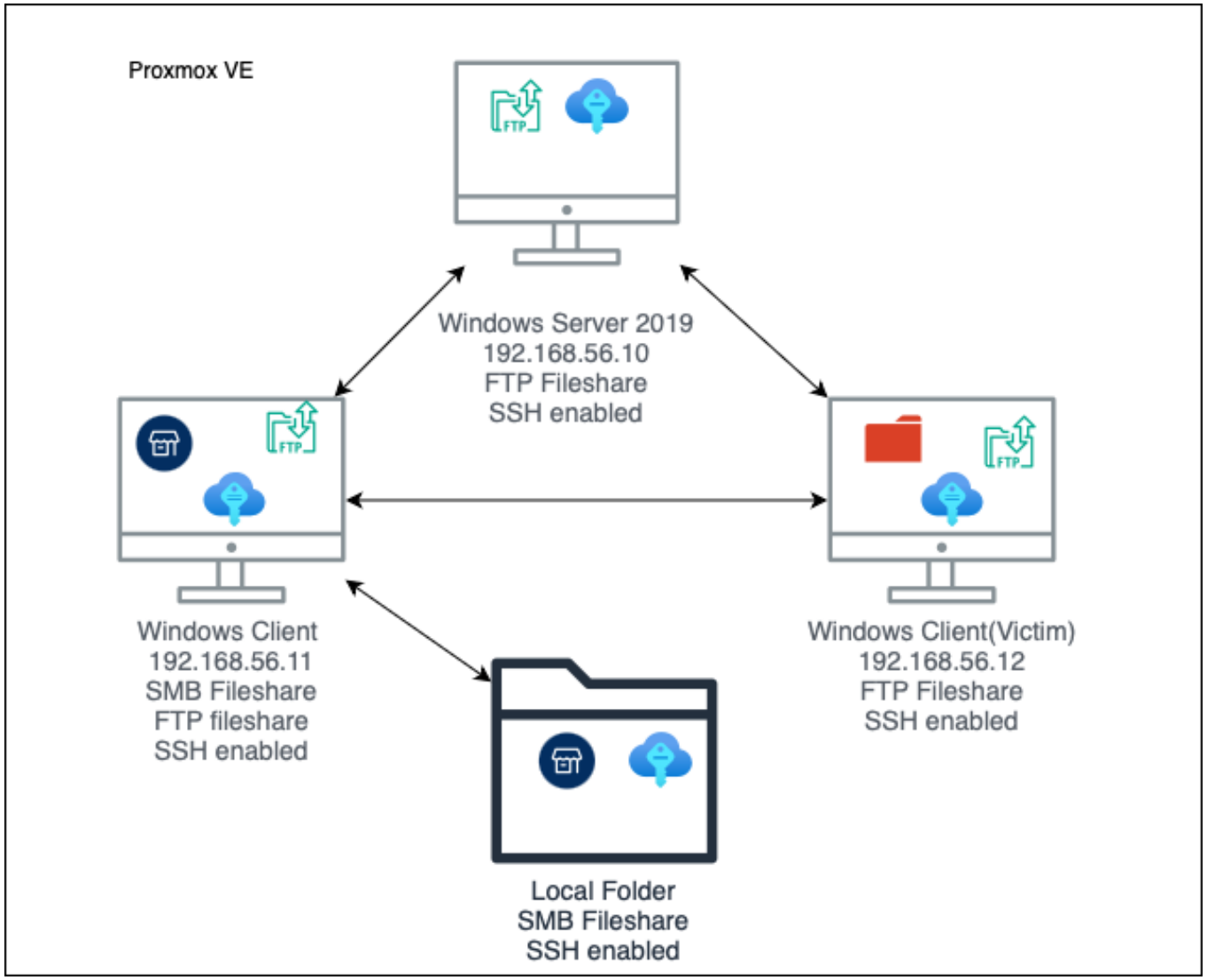
- ❑ Many related work
- ❑ Reveals family patterns but only for single-host traces.

Key Limitation Across These Works

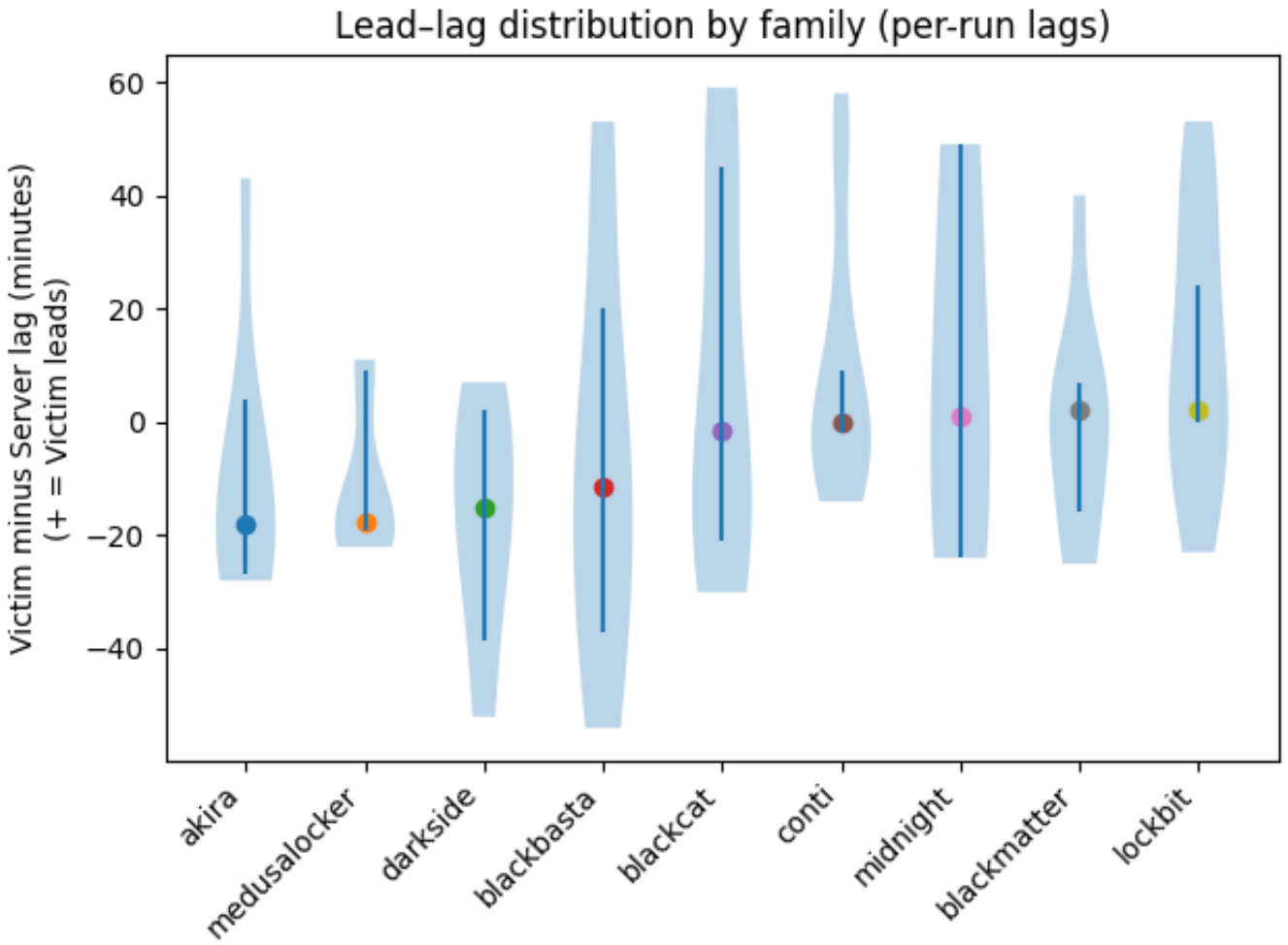
- ❑ No analysis of lead–lag, stage ordering, or family templates in AD logs.
- ❑ No reproducible AD-centric ransomware dataset.

Methodology

- **Setup & Log collection**
  - Executed in a controlled Proxmox environment
  - One AD Domain Controller (Windows Server)
  - Two Windows 10 clients
- Logs collected**: Security, System, and Application** logs



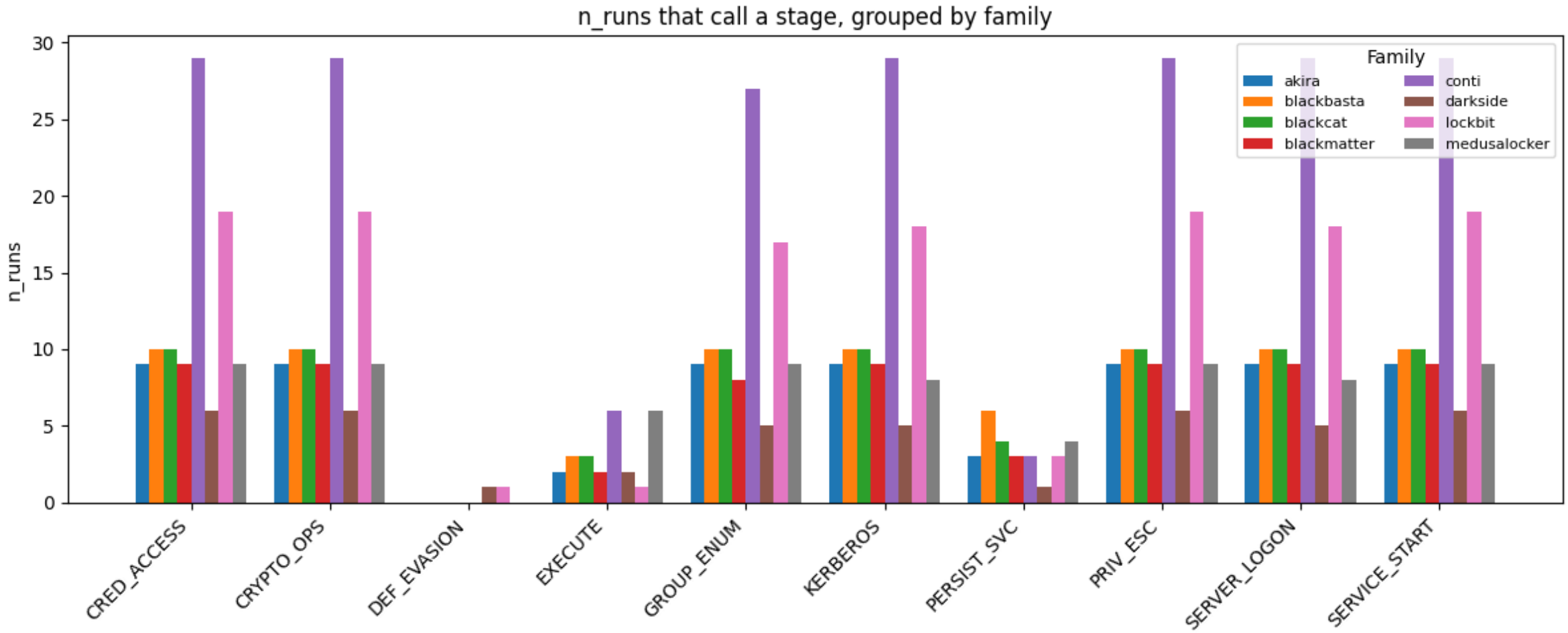
Lead-lag



- Positive median – Victim activity first
- Negative median – Server activity first

Family	Count	Median	Mean
Akira	9	-18.0	-9.78
MedusaLocker	8	-17.5	-11.38
DarkSide	6	-15.0	-17.17
Black Basta	10	-11.5	-7.70
BlackCat	10	-1.5	7.10
Conti	29	0.0	9.24
BlackMatter	9	2.0	-0.67
Lockbit	19	2.0	12.74

Counts of Runs that exhibited in each stage



Stage Ordering Consistency across Families

- Cred_Access before crypto_ops
  - All of them
- Priv_esc before persist_svc
  - Black Basta, Akira, BlackCat, MedusaLocker

Family	Runs (PRIV_ESC -> PERSIST_SVC)	Runs (CRED_ACCESS -> CRYPTO_OPS)
Akira	3	9
Black Basta	6	10
BlackCat	4	10
BlackMatter	3	9
Conti	3	29
DarkSide	1	6
LockBit	3	19
MedusaLocker	4	9

Family Template Scoring

- Families behave differently – can build a template
- More diverse on Victim Side

	Victim	Server
Family	AUC (one-vs-rest)	AUC (one-vs-rest)
Akira	0.697	0.702
Black Basta	0.735	0.670
BlackCat	0.739	0.639
BlackMatter	0.773	0.509
Conti	0.520	0.569
DarkSide	0.818	0.632
Lockbit	0.557	0.452
MedusaLocker	0.810	0.751
Macro AUC	**0.706**	**0.616**

Top True Matches (Victim role)

- Similarities between **inter-families**
  - significantly similar behavior

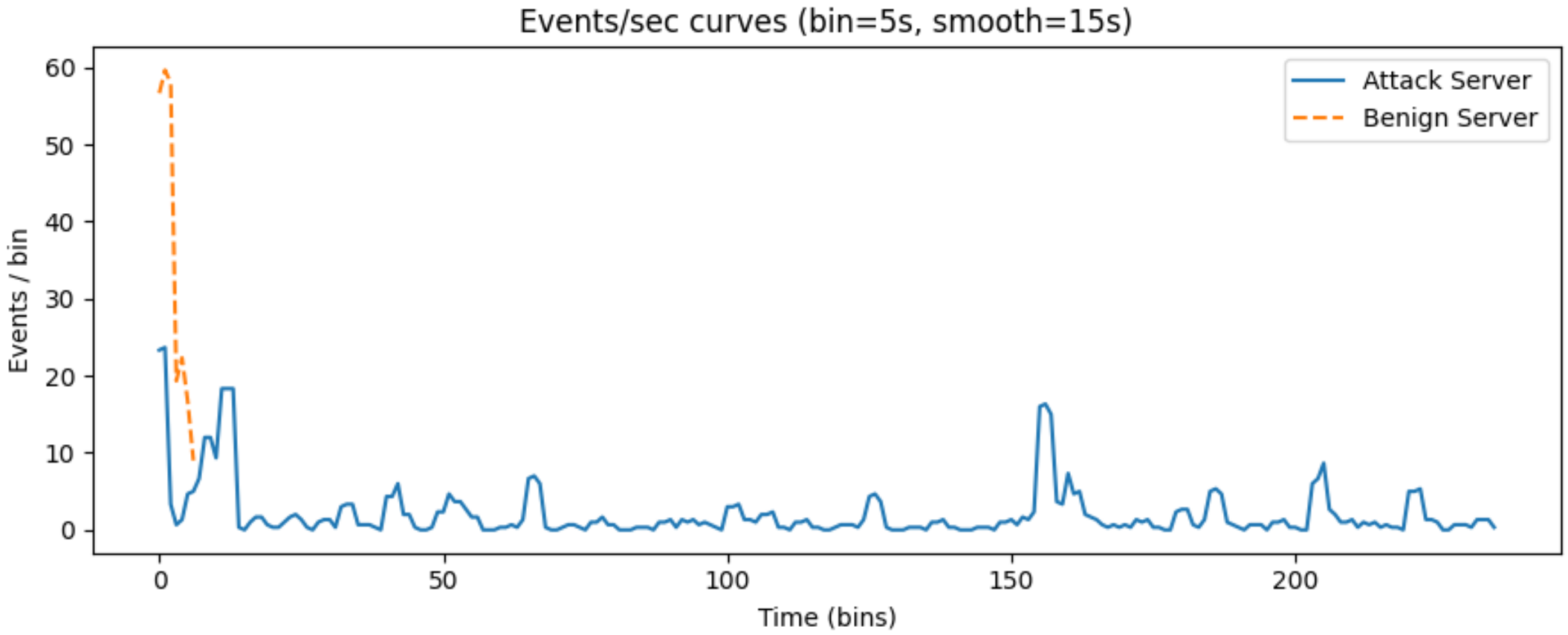
Run_hash (trunc.)	Run_family	Target_family	score
9bd6d6d9....	DarkSide	DarkSide	0.737815
03a52225....	DarkSide	DarkSide	0.737815
acb60f0d.....	Black Basta	Black Basta	0.688659
db22c29a....	Black Basta	Black Basta	0.684871
6f934eb7....	Akira	Akira	0.676486
1638132d.....	DarkSide	DarkSide	0.667585
b28fd564.....	Black Basta	Black Basta	0.651912
fc4c8e5b.....	MedusaLocker	MedusaLocker	0.650620
b713af09.....	BlackCat	BlackCat	0.650571
1b5164f0.....	Lockbit	Lockbit	0.648343

Top False Matches (Victim role)

- Similarities between **intra-families**
  - Akira – DarkSide
  - BlackCat –DarkSide
  - Black Basta – DarkSide

Run_hash (trunc.)	Run_family	Target_family	score
5ca9991f....	Akira	DarkSide	0.729441
6f934eb7....	Akira	DarkSide	0.728278
03ba73be.....	BlackCat	DarkSide	0.727966
c98ef747....	BlackCat	DarkSide	0.727450
db22c29a....	Black Basta	DarkSide	0.727337
1bad2b6e.....	MedusaLocker	DarkSide	0.726206
1b5164f0.....	Lockbit	DarkSide	0.718886
acb60f0d.....	Black Basta	DarkSide	0.715702
03a52225	DarkSide	Black Basta	0.700240

Benign v/s Ransomware



Conclusion

- Early-stage ransomware behavior is distinct and measurable
- Timing + stage patterns are consistent across runs and families
- Victim logs provide strongest early detection signal
- Benign activity looks fundamentally different
- We release a reproducible AD early-stage dataset

Future Work

- Scale the Dataset Automate execution
- Strengthen Feature Engineering
- Build Detection Models
- Integrate AD Semantics
- Broaden the Framework

Thank You!

- Contact:
  - prajnab1@umbc.edu

- GitHub Link
  - https://github.com/UMBC-DREAM-Lab/Ransomware_in_AD_Early-Satge-Analysis