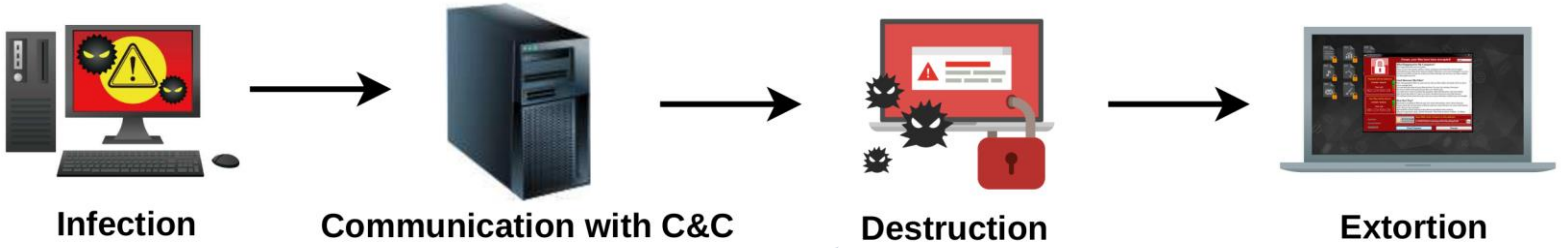
Limits of I/O Based Ransomware Detection: An Imitation Based Attack

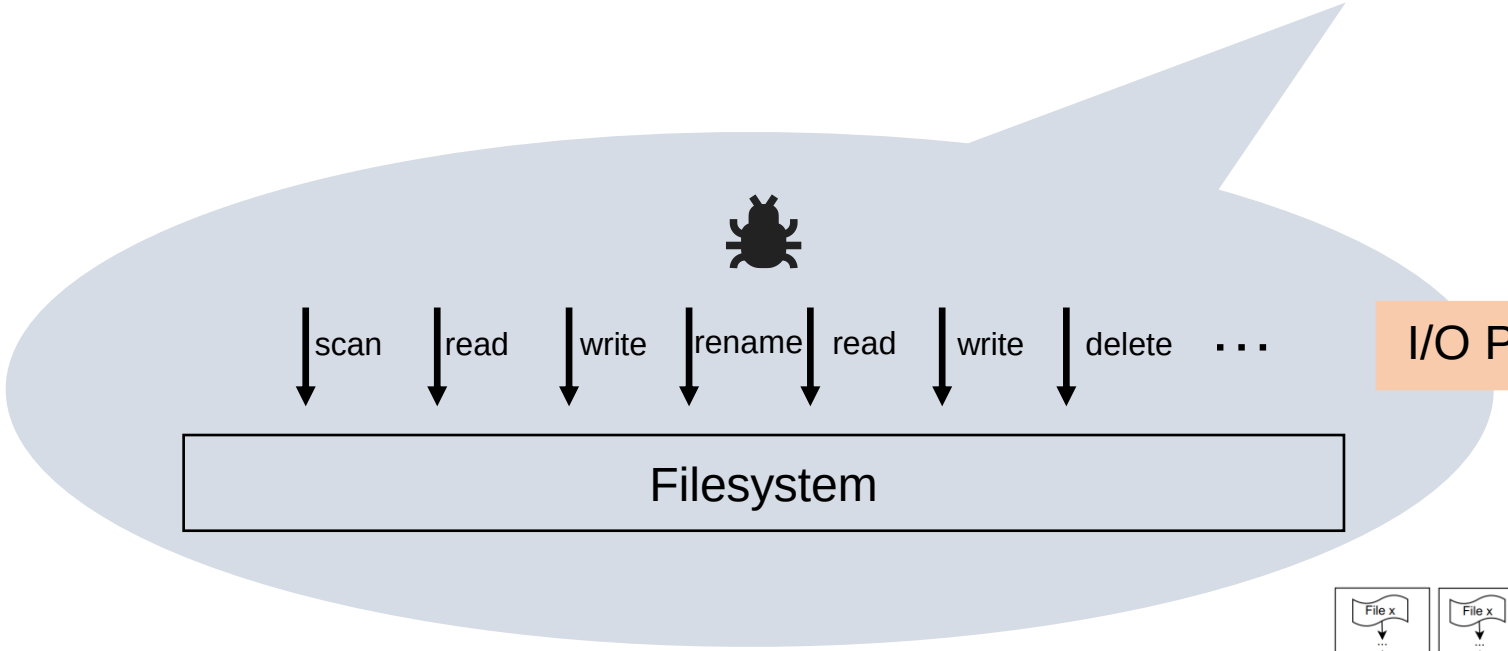
Chijin Zhou[1], Lihua Guo[1], Yiwei Hou[1], Zhenya Ma[1],
Quan Zhang[1], Mingzhe Wang[1], Zhe Liu[2], and Yu Jiang[1]

[1]Tsinghua University, Beijing, China
[2]NUAA, Nanjing, China

I/O Based Ransomware Detection

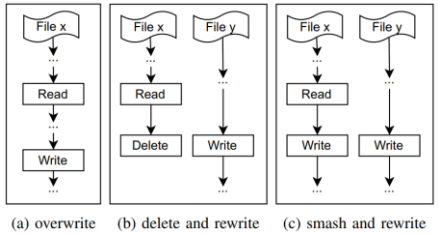
Ransomware Lifecycle





I/O Pattern

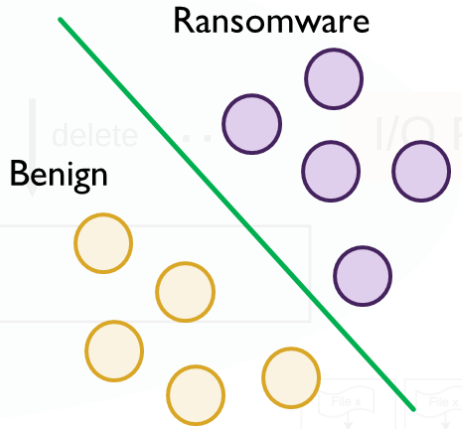
Ransomware Detection Based on Program's I/O Pattern



[e.g., Unveil (Usenix Sec'16)]

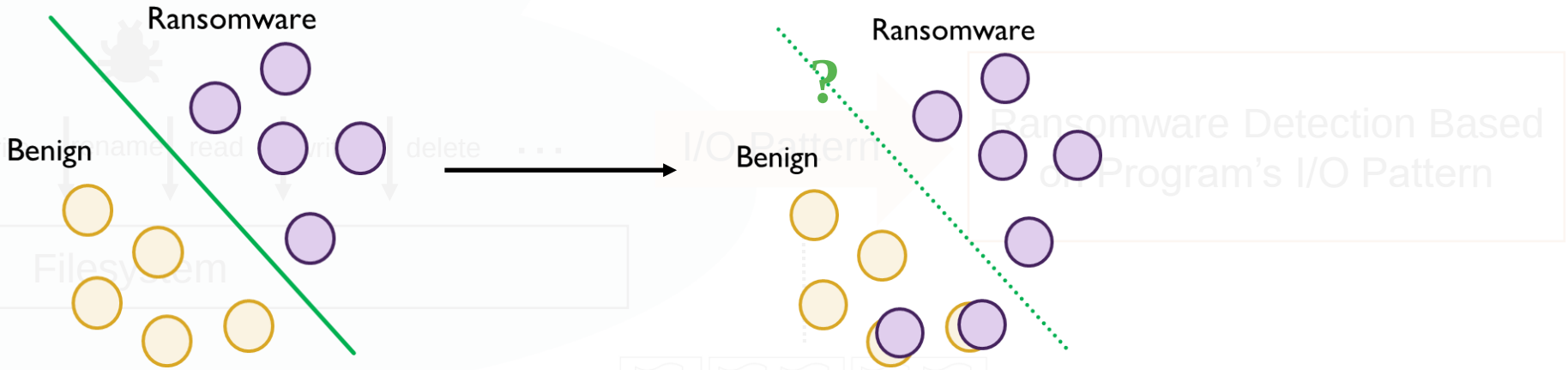
I/O Based Ransomware Detection

Assumption: ransomware behaves very differently from benign programs regarding observed I/O detection patterns.



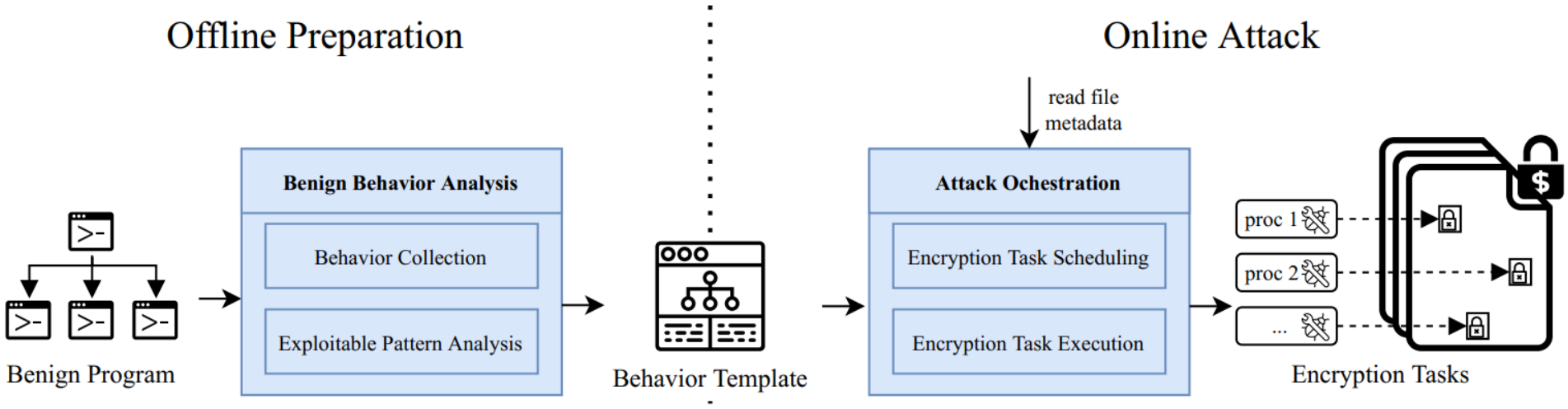
Imitation Based Ransomware Attack

Research question: Can a ransomware program evade the existing detection techniques by imitating the behaviors of benign programs?



Imitation Based Ransomware Attack

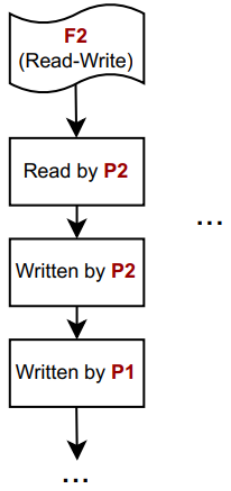
- Imitation based attack
  - Goal: help existing detectors realize the limits of their feature engineering
  - Idea: imitate behaviors of benign programs to disguise its encryption tasks
  - Approach
    1. Learn behavior patterns from a benign program
    2. Orchestrate child processes to perform encryption tasks



Imitation Based Ransomware Attack

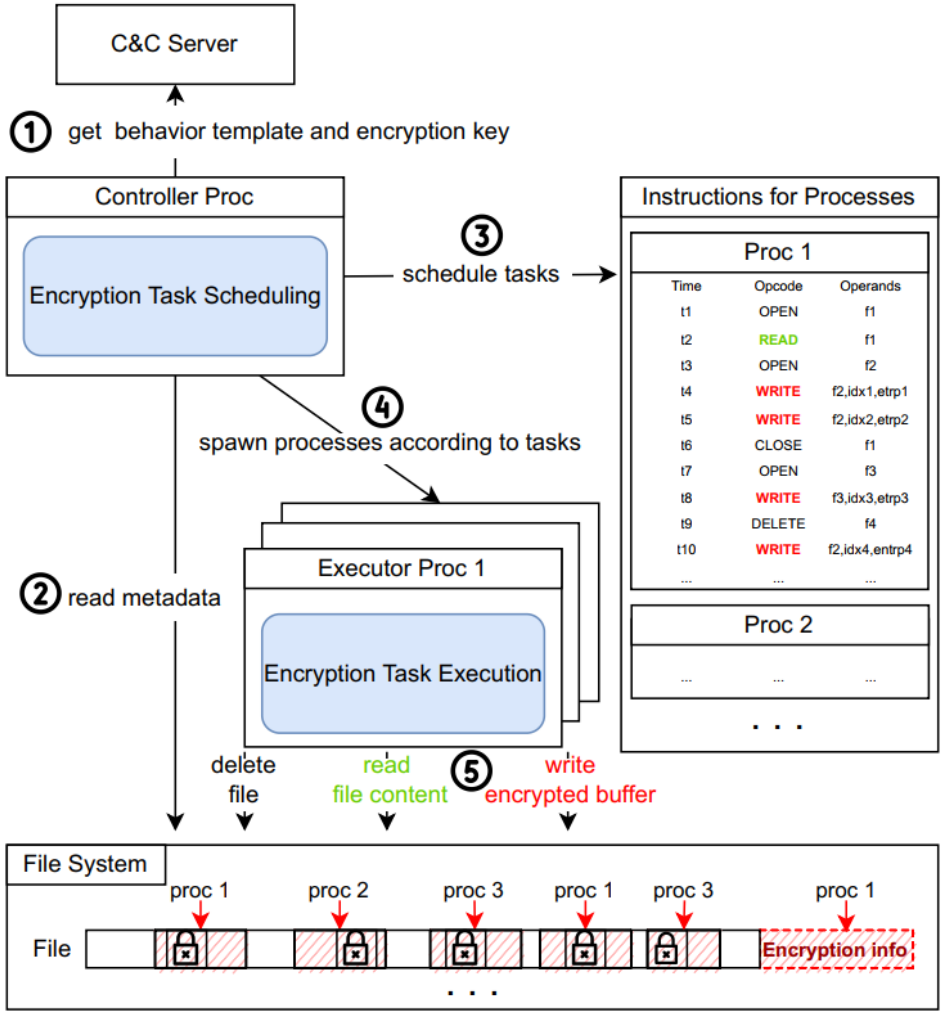
- Offline Preparation Phase
  - Running benign programs to collect behavior logs
  - Extracting behavior template from the logs

Time	Proc	Operation	File	Extra Info
T_0 + 0	P1	QUERY INFO	F1	Null
T_0 + 12	P1	QUERY INFO	F2	Null
T_0 + 14	P2	QUERY INFO	F2	Null
T_0 + 20	P2	OPEN	F2	mode: ALL_ACCESS
T_0 + 25	P2	READ	F2	buff len: 4096
T_0 + 30	P2	WRITE	F2	buff len: 1024 entropy: 5.67
. . .				



Imitation Based Ransomware Attack

- Online Attack Phase
  - Scheduling based on behavior template
  - Execution based on scheduling results



Evaluation – Attack Effectiveness

Three Industrial Tools | Three Academic Tools

Imitation-Based Attack →

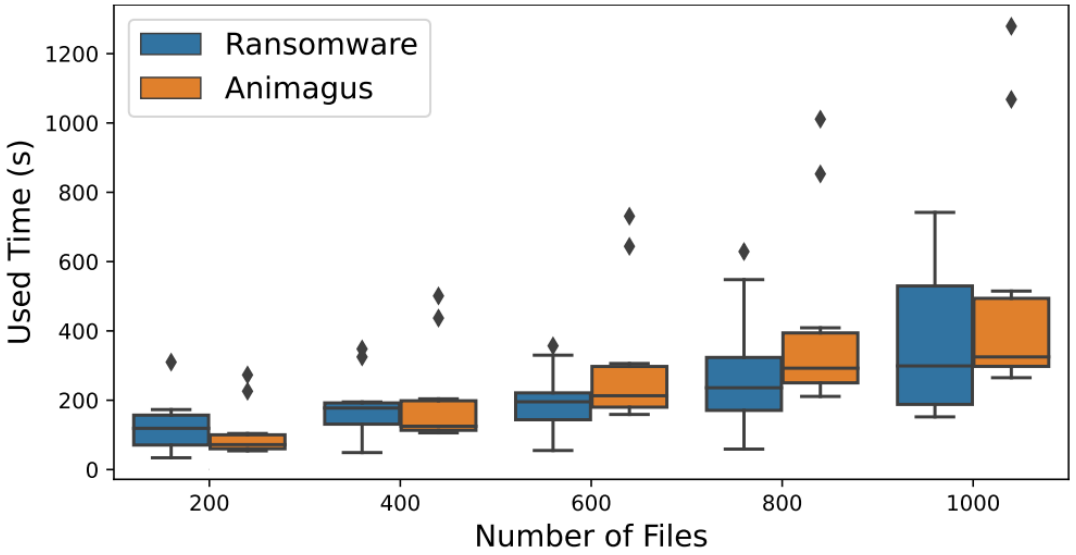
Ten Ransomware Families

Program	v.s. Detection Tools					
	Kaspersky	360	Defender	Unveil	Redemption	ShieldFS
ANIMAGUS	✓	✓	✓	✓	✓	✓
ANIMAGUS⁻	✗	✗	✗	✓	✗	✗
WannaCry	✗*	✗*	✗*	✗	✗	✗
Avoslocker	✗*	✗*	✓	✓	✓	✗
XData	✗*	✗*	✗*	✓	✓	✗
TeslaCrypt	✗*	✗*	✗*	✗	✗	✗
Bitman	✗*	✗*	✗*	✗	✗	✗
Vobfus	✗*	✗*	✗*	✓	✓	✗
Dalexis	✗*	✗*	✗*	✗	✓	✗
Yakes	✗*	✗*	✗*	✗	✗	✗
Koxic	✗*	✗*	✗	✓	✓	✗
phobos	✗*	✗*	✗*	✓	✗	✗

✓: attack successfully; ✗: be detected; ∗: be detected as soon as it started.

Despite the effectiveness of these detection tools in identifying most forms of ransomware, Animagus still evades these tools.

Evaluation – Attack Throughput

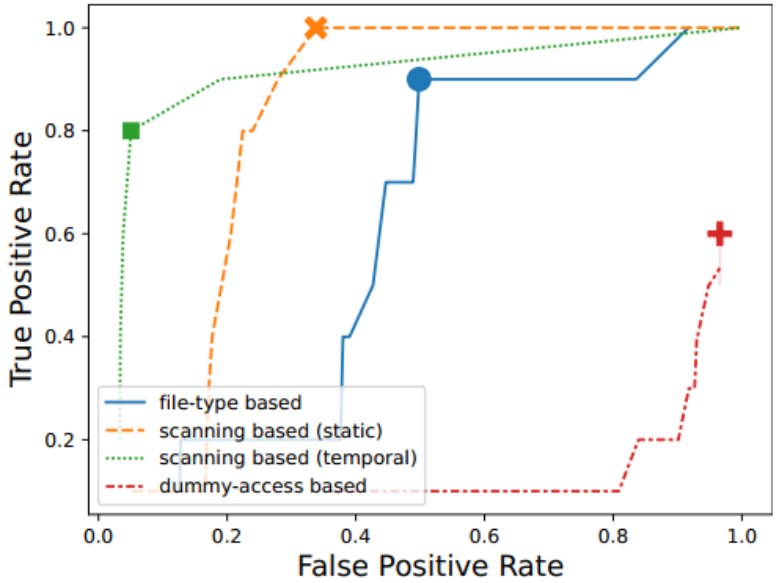


	200 files	400 files	600 files	800 files	1000 files
ANIMAGUS^{FireFox}	56s	112s	193s	254s	320s
ANIMAGUS$^{MS\ Edge}$	226s	437s	644s	853s	1068s
ANIMAGUS^{Chrome}	273s	501s	731s	1011s	1279s
ANIMAGUS$^{WPS\ Office}$	81s	110s	233s	323s	330s
ANIMAGUS$^{MS\ Office}$	134s	234s	334s	397s	512s
ANIMAGUS^{7Zip}	63s	125s	178s	262s	295s
ANIMAGUS^{WinRAR}	54s	106s	159s	211s	265s
ANIMAGUS$^{Golang-go}$	59s	117s	173s	232s	289s
ANIMAGUS^{Rustc}	63s	125s	186s	249s	306s
ANIMAGUS$^{Visual\ Studio}$	89s	182s	272s	350s	431s

The encryption time of Animagus is not much longer than that of traditional ransomware, but the attack success rate is much higher.

Evaluation – Robustness Against Defense

- Detection Strategies
  - File-type based detector
  - Scanning based detector
  - Dummy-access based detector

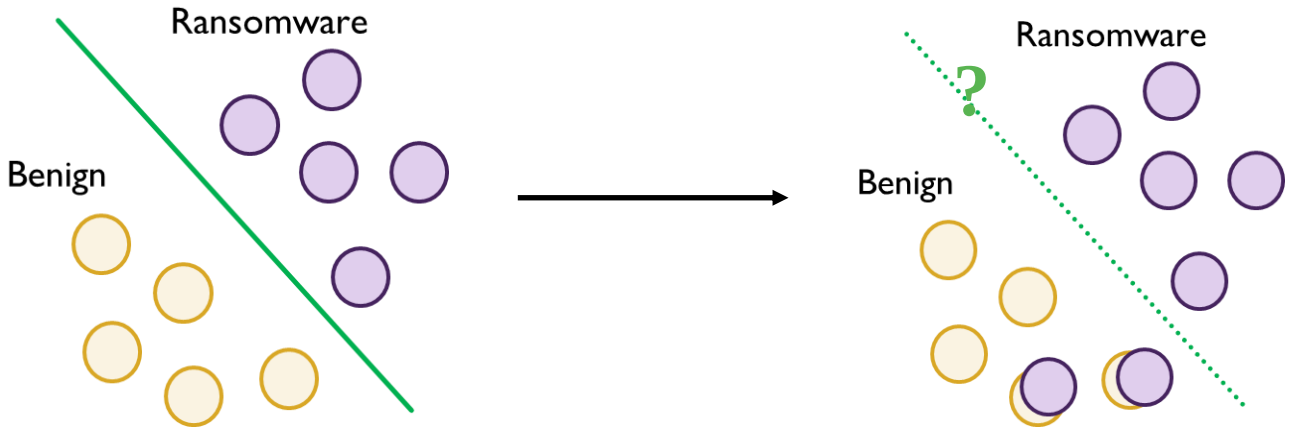


Simple detection strategies cannot effectively detect Animagus without a considerable FPR.

	TPR	FPR	F1-score
file-type based detector	0.900	0.499	0.751
static scanning based detector	1.000	0.338	0.856
temporal scanning based detector	0.800	0.051	0.865
dummy-access based detector	0.600	0.966	0.468

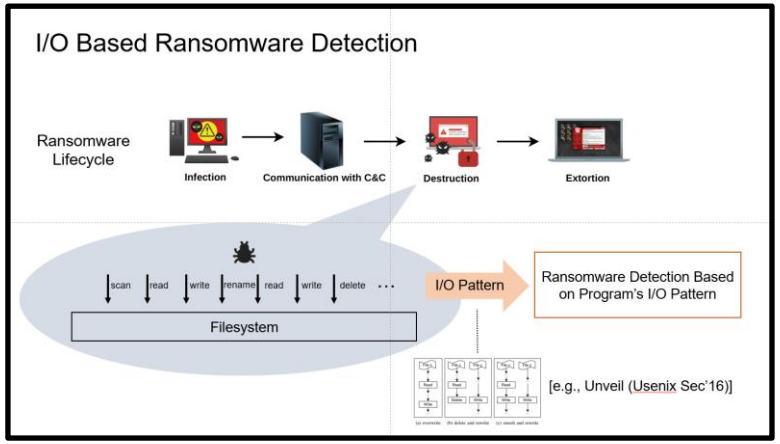
Potential Benefits

- Prototype is released in https://github.com/ChijinZ/Animagus.
- Vendors can collect numerous kinds of Animagus behavior logs to fine-tune the heuristics of their detectors.

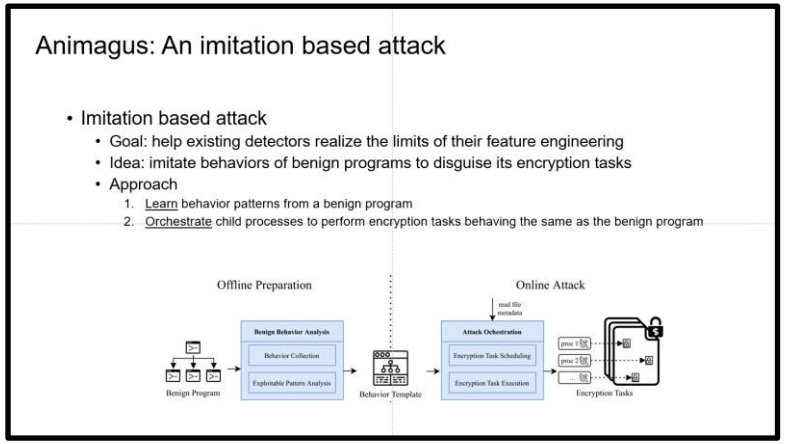


Summary

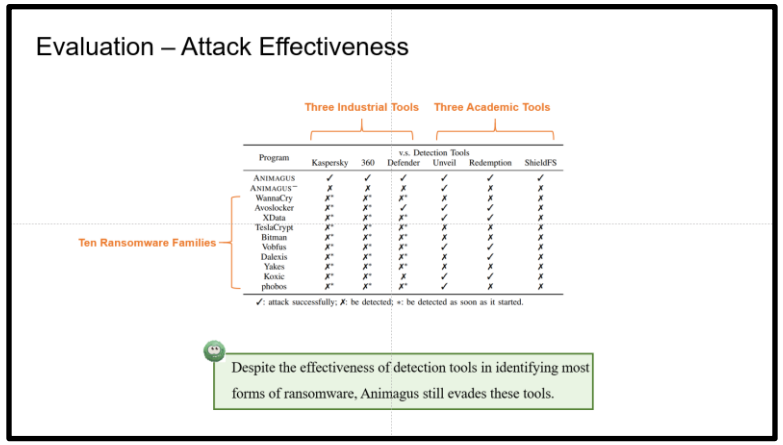
Goal: reveal the limits of ransomware detectors



Method: learn behaviors from benign programs



Evaluation: effectively evade existing detectors



Benefit: leverage the tool to improve their detectors