Understanding the Behavior of Ransomware: An I/O Request Packet (IRP) Driven Study on Ransomware Detection against Execution Time

Ahsan Ayub and Ambareen Siraj

Tennessee Tech University, Cookeville, USA

Emails: mayub42@tntech.edu and asiraj@tntech.edu

IEEE International Conference on Collaboration and Internet Computing (IEEE CIC 2023)

CERC Cybersecurity Education, Research and Outreach Center

November 1-3, 2023

What is Ransomware?

- A type of malware that takes over the system by affecting the victim machine via email, remote desktop protocol, software vulnerability, etc.
- Mainly two kinds of ransomware –
  - Locker Ransomware
  - Crypto Ransomware

Ransomware Threat Landscape and Motivation

Adversaries use already-developed

- Ransomware-as-a-Service (Raas) Kits

Organizations suffer from

- Financial Loss
- Reputational Loss

Suspected means of initial access

- Software Vulnerabilities
- Credential Attacks
- Phishing
- Abuse of RDP

Ransomware attack on the colonial pipeline network in May 2021

- State of Emergency in 18 states
- USD 4.4 M worth of bitcoin paid

I/O Request Packet (IRP) (1/2)

- A common mechanism for requesting I/O operations between the user and the kernel mode.
- Types of IRP operations
  - IRP
  - FIO (Fast I/O)
  - FSF (File System Filter)
- Process-based Information
  - Process ID, Process Name, Thread ID, and Parent ID.
  - Pre-operation time and Post-operation time.

I/O Request Packet (IRP) (2/2)

- Flag-based Information
  - IRP Flag
  - **IRP Major Operation Type**
  - IRP Minor Operation Type
  - Status
- **File-based Information**
  - File Object
  - File Name
  - Buffer Length
  - Entropy

Research Questions (RQ)

RQ1. Is there any distinguishable pattern(s) present during ransomware encryption?

RQ2. How effectively is it possible to identify the families of ransomware early enough during its infection through continuous monitoring of IRP logs?

IRP-based Dataset Collection

- Continella et al. "Shieldfs: a self-healing, ransomware-aware filesystem." Proceedings of the 32nd annual conference on computer security applications. 2016.
- 383 Ransomware samples' IRP logs
  - Sandbox Environment
  - Target OS: Windows 7 (64-bit)
  - 5 Families: CryptoWall, Crowti, CryptoDefense, Critroni, and TeslaCrypt.
- Large-scale IRP-based benign applications' dataset
  - 1.7 billion IRPs produced by 2,245 different applications.
  - 11 volunteering users (dev, home, and office).

Strategy to Answer RQ1: Sequence Mining and One-Class Classification (1/2)

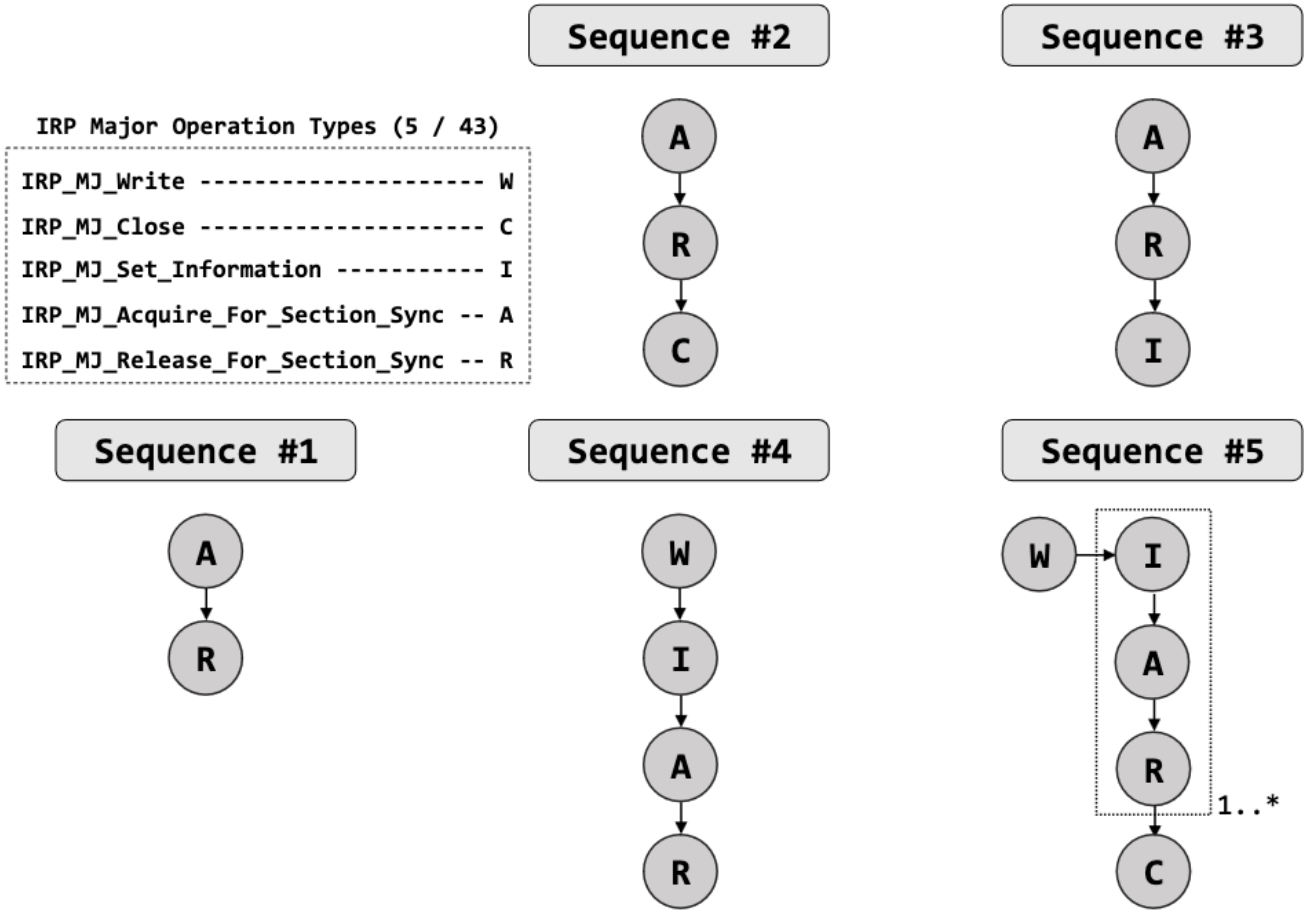

Fig. 1. Notable sequences observed from the IRP Major Operation Type feature for all ransomware samples' IRP logs.

Strategy to Answer RQ1: Sequence Mining and One-Class Classification (2/2)

Sequences	*Min*	*Q1*	*Median*	*Mean*	*Q3*	*Max*	*Max Outlier*
#1	90.5	663.25	1,337.5	1,615.15	2,061.38	3,388.5	5,597.5
#2	17.5	233.38	554.5	669.25	926.25	1,452	2,077
#3	0	22.75	67.25	138.88	122.25	201.5	1,043
#4	2	13.88	26.75	210.25	159.5	276.5	1,801.5
#5	0	1.25	3	18.9	15.5	27	128.5

Fig. 2. Summarized statistical counts of notable sequences observed from the IRP major operation type feature for all ransomware samples' IRP logs over 5 minutes time frame.

Strategy to Answer RQ2: Multiclass Classification

- We selected Decision Tree, Random Forest, Extra Tree, and Bagging classifiers and constructed the following Artificial Neural Networks (ANN).
  - A fully connected network with one input layer, one hidden layer, and one output layer.
  - The output layer contains 21 neurons to predict all the ransomware families.
  - Selected ReLU activation function for both the input and hidden layer, while used softmax activation function for the output layer.
- Reported performance for 15, 20, 25, 30, 35, and 40 minutes of IRP logs.

Addressing RQ1 – One-Class Classification

Algorithm	Sequences	Performance Parameter	Performance in Time Chunks (in minutes)						
			15	20	25	30	35	40	Median
One-Class SVM	#1, #2, and #3	Error Train	10.64%	11.11%	10.26%	8.51%	8.18%	9.52%	9.89%
		Error Novel Regular	**6.25%**	**19.05%**	11.11%	9.38%	**2.70%**	14.29%	10.25%
	#4 and #5	Error Train	10.64%	11.11%	10.26%	9.57%	8.18%	9.52%	9.92%
		Error Novel Regular	25.00%	19.05%	11.11%	15.62%	10.81%	4.76%	13.37%
	#1, #2, #3, and #4	Error Train	12.77%	11.11%	11.54%	10.64%	10.00%	9.52%	10.88%
		Error Novel Regular	**6.25%**	28.57%	**7.41%**	**6.25%**	8.11%	9.52%	**7.76%**
	All	Error Train	12.77%	**7.94%**	8.97%	11.70%	10.00%	9.52%	9.76%
		Error Novel Regular	12.50%	23.81%	**7.41%**	12.50%	8.11%	7.14%	10.31%
Isolation Forest	#1, #2, and #3	Error Train	10.64%	11.11%	10.26%	10.64%	10.00%	10.32%	10.48%
		Error Novel Regular	**6.25%**	28.57%	18.52%	9.38%	5.41%	7.14%	8.26%
	#4 and #5	Error Train	10.64%	11.11%	10.26%	10.64%	10.00%	10.32%	14.96%
		Error Novel Regular	25.00%	14.29%	18.52%	15.62%	13.51%	11.90%	10.48%
	#1, #2, #3, and #4	Error Train	10.64%	11.11%	10.26%	10.64%	10.00%	10.32%	10.48%
		Error Novel Regular	12.50%	23.81%	18.52%	12.50%	10.81%	11.90%	12.50%
	All	Error Train	10.64%	11.11%	10.26%	10.64%	10.00%	10.32%	10.48%
		Error Novel Regular	**6.25%**	28.57%	14.81%	12.50%	10.81%	**2.38%**	11.66%
Local Outlier Factor	#1, #2, and #3	Error Train	8.51%	9.52%	10.26%	9.57%	9.09%	9.52%	9.52%
		Error Novel Regular	**6.25%**	28.57%	18.52%	12.50%	10.81%	4.76%	11.66%
	#4 and #5	Error Train	**4.26%**	**7.94%**	**5.13%**	**4.26%**	**5.45%**	**6.35%**	**5.29%**
		Error Novel Regular	18.75%	**19.05%**	14.81%	9.38%	13.51%	11.90%	14.16%
	#1, #2, #3, and #4	Error Train	8.51%	9.52%	8.97%	**4.26%**	**5.45%**	9.52%	8.74%
		Error Novel Regular	18.75%	23.81%	14.81%	9.38%	5.41%	**2.38%**	12.10%
	All	Error Train	8.51%	**7.94%**	10.26%	7.45%	8.18%	**7.14%**	8.06%
		Error Novel Regular	**6.25%**	23.81%	18.52%	9.38%	10.81%	4.76%	10.10%
Robust Covariance	#1, #2, and #3	Error Train	25.53%	25.40%	25.64%	25.53%	25.45%	25.40%	25.49%
		Error Novel Regular	43.75%	42.86%	33.33%	25.00%	21.62%	21.43%	29.17%
	#4 and #5	Error Train	25.53%	25.40%	25.64%	25.53%	25.45%	25.40%	25.49%
		Error Novel Regular	31.25%	28.57%	25.93%	21.88%	27.03%	23.81%	26.48%
	#1, #2, #3, and #4	Error Train	25.53%	25.40%	25.64%	25.53%	25.45%	25.40%	25.49%
		Error Novel Regular	43.75%	42.86%	37.04%	25.00%	27.03%	19.05%	32.04%
	All	Error Train	25.53%	25.40%	25.64%	25.53%	25.54%	25.40%	25.53%
		Error Novel Regular	43.75%	33.33%	25.93%	18.75%	21.62%	21.43%	23.78%

Fig. 3. Comparison chart of different novelty detection algorithms' performance for ransomware samples' derived sequence counts from the IRP Major Operation feature of IRP logs.

Addressing RQ2 – Multiclass Classification

Performance Parameter		Decision Tree	Random Forests	Extra Tree	Bagging	ANN
Accuracy (in minutes)	15	92.69%	92.48%	92.45%	92.69%	79.78%
	20	92.90%	92.85%	92.90%	92.91%	80.29%
	25	93.65%	93.56%	93.56%	93.67%	80.01%
	30	93.79%	93.68%	93.76%	93.79%	80.55%
	35	93.86%	93.71%	93.80%	93.89%	80.53%
	40	93.92%	93.77%	93.86%	93.94%	80.55%
Precision (in minutes)	15	92.63%	92.48%	92.35%	92.62%	92.03%
	20	92.13%	92.40%	92.48%	92.48%	89.10%
	25	93.23%	93.08%	93.08%	93.27%	89.80%
	30	93.24%	93.13%	93.23%	93.25%	91.60%
	35	93.23%	93.04%	93.21%	93.24%	72.82%
	40	93.07%	92.89%	93.04%	93.09%	89.74%
Recall (in minutes)	15	88.65%	88.46%	88.46%	88.65%	69.88%
	20	89.49%	89.38%	89.43%	89.50%	71.43%
	25	90.44%	90.30%	90.32%	90.44%	71.52%
	30	90.95%	90.81%	90.91%	90.95%	72.47%
	35	91.21%	90.98%	91.12%	91.22%	90.41%
	40	91.27%	91.08%	91.19%	91.28%	73.01%
F_1 (in minutes)	15	90.00%	89.82%	89.75%	90.00%	76.65%
	20	90.28%	90.41%	90.47%	90.53%	76.68%
	25	91.47%	91.32%	91.32%	91.49%	77.45%
	30	91.76%	91.63%	91.73%	91.76%	79.25%
	35	91.92%	91.71%	91.86%	91.93%	79.31%
	40	91.89%	91.69%	91.82%	91.90%	77.99%

Fig. 4. Comparison chart of different machine learning algorithms' performance for multiclass classification using IRP logs of 21 ransomware families.

Case Study: Comparison with Collected IRP Logs From Users' Machines (Benign) (1/2)

File System Features	*Min*		*Median*		*Mean*		*Max*	
	Users	*Ransomware*	*Users*	*Ransomware*	*Users*	*Ransomware*	*Users*	*Ransomware*
File Accessed (Unique)	30	1,667	519	3,065	1,583.64	2,851	9,277	3,715
File Objects (Unique)	47	1,135	378	1,899	470.18	2,059	1,521	3,231
Buffer Length (Mean)	8,192	5,870	32,768	21,125	42,891.8	20,734	141,626.25	37,435
Entropy (Mean)	0.066	0.077	0.549	0.125	0.502	0.12	0.79	0.16

Fig. 5. Comparison of statistical counts of file system features between A complete session of 11 users' machines and over 5 minutes average time frame of ransomware execution.

Case Study: Comparison with Collected IRP Logs From Users' Machines (Benign) (2/2)

Sequences	*Min*		*Median*		*Mean*		*Max*	
	Users	*Ransomware*	*Users*	*Ransomware*	*Users*	*Ransomware*	*Users*	*Ransomware*
#1	604	13,668	17,658	27,353	51,984.27	29,813.5	319,548	63,642
#2	110	1,668	1,748	12,663	2,922.09	11,698.33	10,773	22,586
#3	0	165	63	1,574.5	328	3,235.78	1,863	34,984
#4	0	475	276	1,483	2,788	4,154.11	15,600	17,848
#5	0	23	110	96.5	636.18	322.72	3,154	2,015

Fig. 6. Comparison of statistical counts of notable sequences observed from IRP major operation type feature between A complete session of 11 users' machines and ransomware.

Summary

- We extracted five notable sequences that significantly set ransomware apart from the benign processes.
- We utilized the One-Class Classification to discover new ransomware based on the counts of such extracted sequences from different time chunks of the IRP log.
- We employed several machine learning classification algorithms to empirically investigate their performances and report our findings on multiclass classification tasks.

Acknowledgement

The work reported in this paper has been supported by Cybersecurity Education, Research & Outreach Center (CEROC) at Tennessee Tech University.

THANK YOU!