An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network

Ahsan Ayub, Andrea Continella, and Ambareen Siraj

Emails: mayub42@students.tntech.edu, a.continella@utwente.nl, asiraj@tntech.edu

2020 IEEE International Conference on Information Reuse and Integration (IRI)

CERIAS
Cybersecurity Education, Research and Outreach Center

August 11-13, 2020

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 - An Ever Growing Menace

- Fastest growing cybercrime
- From 2017 (US$ 533m) to 2018 (US$ 646m), ransomware attack has increased by 21% in the U.S. [a]
- Global ransomware damage predicted US$ 20b in 2021. [b]
- A business will fall victim to a ransomware attack in every 11 seconds by 2021. [b]
- On average, a ransomware attack lasts for 7 days 8 hrs [c]
  - Causing extensive financial and reputational damage

[a] The Cost of Cybercrime by Accenture Security, published in 2019.
[b] 2019 Official Annual Cybercrime Report by Herjavec Group.
[c] Coveware's q1 ransomware marketplace report, published in 2019.

I/O Request Packet (IRP)

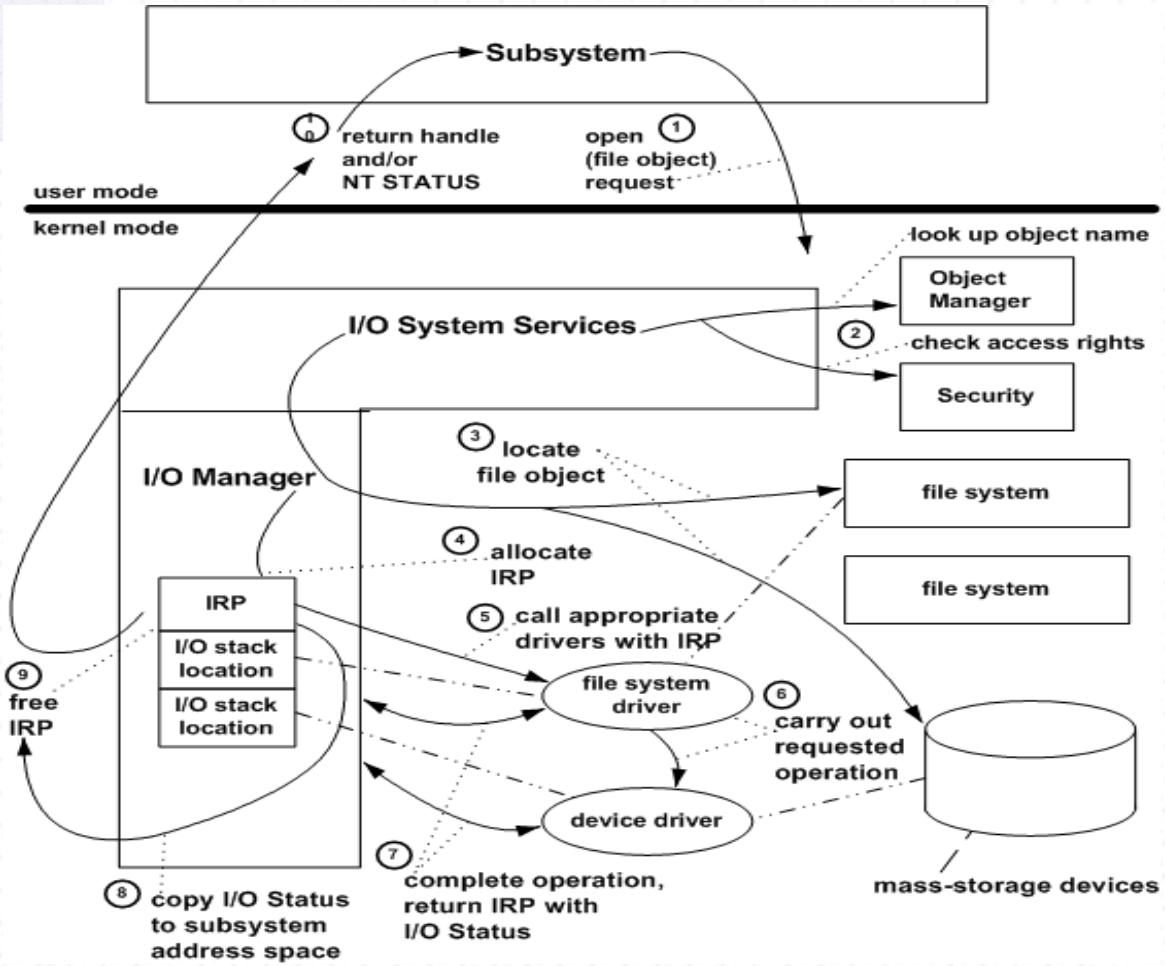

Image Source: Microsoft I/O Docs

Problem Statement

As ransomware defenders and researchers gather IRP logs during ransomware executions and build state-of-the-art solutions to combat against this ever-evolving malware suite, ransomware, our study aims to devise an effective detection scheme by extracting actionable insights from granular activities at the process level as the encryption of the data assets are underway by the ransomware.

Prior Work and Dataset Acquisition

ShieldFS: A Self-healing, Ransomware-aware Filesystem

Andrea Continella
andrea.continella@polimi.it

Alessandro Guagnelli
alessandro.guagnelli@polimi.it

Giovanni Zingaro
giovanni.zingaro@polimi.it

Giulio De Pasquale
giulio.depasquale@polimi.it

Alessandro Barenghi
alessandro.barenghi@polimi.it

Stefano Zanero
stefano.zanero@polimi.it

Federico Maggi
federico.maggi@polimi.it

DEIB, Politecnico di Milano, Milan, Italy

Venue: ACSAC (Annual Computer Security Applications Conference), **2016**.

Dataset Processing

Raw Dataset Acquisition
Acquire raw ransomware irp logs for further processing

Dataset Cleaning and Formatting
Clean and format every log in the dataset comprising both malicious and benign logs

Group Dataset
Group all the logs in the dataset with the pair of Process ID and Process Name

Extract Ransomware Process(es)
Find Process ID and Process Name of the ransomware from the grouped dataset

Label Class
Label malicious to ransomware logs and benign to the remaining logs at the class feature

Ransomware Family Labeling

SHA256 Hashes

```
00ce22ce923e246990e43289b8b5b8191cbfc28dbee6d30b66226df0aa14b7bd,
02ab9c0071097e87bcc8993d0c3e1ca9f4d2152d08f0b4b42d74ede223ab3290,
03aefcbe87c5208024b36ee3d013bc2d7840c4916faeba4b792654231ff73978,
...
```

VirusTotal Report

```
{“sha1”: “e239478bc677c1f95653a5e7d32ae2aeb2e49c57”, “sha256”:
“00ce22ce923e246990e43289b8b5b8191cbfc28dbee6d30b66226df0aa14b7bd”,
“md5”: “95a5b938c5a554ae2ea356f7bf888cda”, “scan_date”: “2020-01-21
23:38:44”, “av_labels”: [["Kaspersky", "Trojan.Win32.Yakes.nfwi"], ...]},
...
```

AVClass

```
00ce22ce923e246990e43289b8b5b8191cbfc28dbee6d30b66226df0aa14b7bd  Yakes
0222fcf49a6c2d7aaec2bbd54d32a9ca9168c0f3ee5ca0ee1ba1489a56b46bd6  Upatre
09bf0e7dd1b2f4e6a40bca448c5bba35be4ae99c3d6310eb25577a65ee2c51ca  Crowti
...
```

Data Distribution – Ransomware IRP Logs

Ransomware Family (Sample Size)	Class	Types of IRP Operations			Flags			File System Information				
		IRP Operation	FSF Operation	FIO Operation	IRP Flag	Unique Major Operation Type	Status	File Object	Unique File Accessed	Total File Accessed	Buffer Length	Entropy
Critroni	Malicious	119,028	191	257	16	**17**	13	5,467	10,251	303,082	988	3,965
(2)	Benign	190	66	63	8	11	4	40	21	354	529	11
Crowti	Malicious	219,734	116,364	1,166	16	15	11	11,225	16,660	224,861	17,621	23,042
(23)	Benign	266	162	290	9	11	4	48	22	830	556	66
CryptoDefense	Malicious	131,344	101,837	867	16	15	11	11,999	17,264	212,562	**22,765**	24,329
(6)	Benign	268	136	190	9	11	4	48	21	826	599	61
CryptoWall	Malicious	131,444	95,052	1,015	16	15	11	8,079	15,994	228,009	5,708	16,884
(17)	Benign	263	146	192	8	11	4	47	22	804	526	60
Dalexis	Malicious	217,532	200	980	14	15	10	8,905	17,431	427,810	1,147	2,912
(1)	Benign	227	118	207	8	11	4	43	21	811	459	70
Deshacop	Malicious	500,284	136,120	7,843	14	15	12	5,158	19,766	508,256	3,162	21,810
(2)	Benign	256	144	196	9	11	4	47	21	787	472	65
High	Malicious	417,447	1,178	544	13	15	10	11,716	19,712	**711,972**	19,381	44,084
(1)	Benign	221	116	152	8	11	4	42	21	662	370	40
Parite	Malicious	406,462	101,702	6,321	14	15	12	5,246	16,921	412,897	3,384	19,457
(1)	Benign	256	148	389	9	11	4	46	21	813	499	65
Processhijack	Malicious	291,645	84,697	4,359	14	15	12	5,806	13,449	296,118	2,141	13,989
(1)	Benign	238	94	139	8	11	4	40	21	582	478	34
Pwszbot	Malicious	96,803	85,176	490	15	15	11	9,626	15,473	262,780	5,617	15,825
(1)	Benign	256	116	127	8	11	4	49	22	577	512	22
Seven	Malicious	175,124	152,269	942	16	15	11	10,637	17,509	272,084	15,649	23,448
(1)	Benign	264	132	157	8	11	4	46	22	805	502	56
TeslaCrypt	Malicious	611,678	**267,387**	26,953	14	15	11	**32,708**	30,564	638,757	3,759	21,472
(1)	Benign	250	94	86	8	11	4	42	21	519	579	30
Tinba	Malicious	**653,943**	194,433	**27,630**	14	15	**14**	9,044	**35,162**	681,707	12,042	**47,949**
(1)	Benign	255	165	420	8	11	4	46	21	812	466	74
Tpyn	Malicious	177,600	65,748	1,612	16	16	11	7,546	10,917	179,402	6,206	16,158
(1)	Benign	260	135	154	8	11	4	48	22	707	448	22
Upatre	Malicious	131,771	99,159	905	16	15	11	10,650	16,267	202,118	10,417	19,381
(56)	Benign	265	147	195	8	11	4	48	21	826	527	62
Vobfus	Malicious	297,730	138	444	12	14	7	11,280	14,193	438,984	6,722	20,453
(1)	Benign	220	84	137	7	11	4	32	21	427	350	30
Yakes	Malicious	177,218	92,796	1,159	16	15	11	8,869	13,101	192,897	8,105	19,401
(150)	Benign	266	148	198	9	11	4	48	22	827	535	61
Zbot	Malicious	166,258	104,951	888	16	15	11	10,629	16,457	208,110	13,302	22,757
(6)	Benign	266	135	163	8	11	4	48	22	780	559	53
Median	Malicious	197,566	97,106	998	15	15	11	9,335	16,558	284,101	6,464	19,955
Results	Benign	256	135	176	8	11	4	47	21	796	507	58

Fig. 1: Data distribution of notable feature spaces for of victim machine's IRP logs during ransomware execution (approx. 90 minutes).

Data Distribution – Benign IRP Logs

User Type	Operating System Version	Types of IRP Operations			Flags			File System Information				
		IRP Operation	FSF Operation	FIO Operation	IRP Flag	Unique Major Operation Type	Status	File Object	Unique File Accessed	Total File Accessed	Buffer Length	Entropy
Developer	Windows 10	129	10	36	6	9	3	17	11	166	537	2
Home	Windows 8.1	281	36	68	7	10	4	51	21	605	46	3
Office	Windows 10	143	18	87	6	8	4	18	9	412	610	13
Home	Windows 7	51	0	20	6	6	2	11	4	78	141	1
Home	Windows 7	190	48	26	7	10	4	28	26	314	919	**84**
Developer	Windows 10	92	24	40	6	9	4	27	18	169	1,233	5
Developer	Windows 8.1	276	4	78	6	7	2	18	25	549	3,380	33
Home	Windows 8.1	**414**	38	83	9	12	**7**	37	36	**765**	**7,474**	54
Home	Windows 8.1	354	**100**	**212**	**13**	12	6	**68**	**47**	683	4,459	36
Home	Windows 7	161	4	14	5	8	4	9	5	203	798	25
Office	Windows 7	170	13	27	5	8	4	10	14	205	2,270	17
Median Results		170	18	40	6	9	4	18	18	314	919	25

Fig. 2: Data distribution of notable feature spaces for benign users' IRP logs during a random session (10 minutes).

Artificial Neural Network (ANN)

- Effectively built to learn the underlying patterns of both benign and ransomware impacted IRP logs
- Experimental goals on performing detection for:
  1. Each family (trained and tested over a single family in every iteration) or single family-wise iteration;
  2. One ransomware family by being trained over all the samples of a different family; and
  3. All the ransomware families (trained and tested over all the samples).
- Split the dataset into training (80%) and testing (20%) set in a stratified fashion for every experiment

Experimental Setup

- Incorporated Early Stopping methodology to ensure the built ANN model neither got underfitted nor overfitted
- ANN's structure –
  - ReLU activation function in both the Input and Hidden layer while Sigmoid activation function in the Output layer
  - Used Adam optimization algorithm and Binary Cross Entropy (BCE) loss function for model compilation
  - Included 20% validation set from training set to monitor Early Stopping
  - Selected 128 batch size and 100 epochs for training
  - During testing, computed Accuracy, Recall, Precision, and F_1 scores to evaluate model's performance in three experimental settings

Experimental Findings (1/2)

Ransomware Family	Sample Size	Accuracy	Precision Score	Recall Score	F_1 Score
Critroni	2	0.9987	0.9976	0.998	0.9978
Crowti	23	0.996	0.9978	0.9965	0.9972
CryptoDefense	6	0.9983	0.9981	0.9988	0.9985
CryptoWall	17	0.9988	0.9989	0.9988	0.9984
Dalexis	1	0.9987	0.9988	0.9988	0.9983
Deshacop	2	0.9988	0.9988	0.9989	0.9989
High	1	0.9988	0.9973	0.9986	0.9984
Parite	1	0.9986	0.9986	0.9987	0.9986
Processhijack	1	0.9987	0.9987	0.9988	0.9988
Pwszbot	1	0.9988	0.9981	0.9985	0.9983
Seven	1	0.9988	0.9988	0.9988	0.9988
TeslaCrypt	1	0.9984	0.9988	0.9953	0.9975
Tinba	1	0.9986	0.9982	0.9989	0.9985
Tpyn	1	0.9985	0.9981	0.9987	0.9989
Upatre	56	0.9989	0.9988	0.9987	0.9982
Vobfus	1	0.9984	0.9986	0.9985	0.9981
Yakes	150	0.9975	0.9967	0.9985	0.9981
Zbot	6	0.9983	0.9981	0.9988	0.9984
Summary	272 (total)	0.9986 (median)	0.9984 (median)	0.9987 (median)	0.9984 (median)

Fig. 3: Performance of the binary classification using ANN for Single ransomware family wise iteration.

Experimental Findings (2/2)

Training Family	Testing Family	Accuracy	Precision Score	Recall Score	F_1 Score
Upatre	Crowti	0.9976	0.9969	0.9987	0.9983
Yakes	Zbot	0.9989	0.9984	0.9988	0.9981

Fig. 4: Performance of the binary classification using ANN for training with one family, testing with another.

- In every case for this experiment setting, we found performance scores of the model within the range of 99.7% +/- 0.2%.
- For training and testing with all the families experiment setting, we achieved 99.8% accuracy, 99.74% precision score, 99.86% recall score, and 99.85% F_1 score.

Conclusion and Future Work

- IRP logs from 272 ransomware samples (belonged to 18 ransomware families) and 11 benign machines
- Designed three experimentation settings to show that the built ANN model can effectively –
  - Detect variants of ransomware samples for each ransomware family;
  - Discover the underlying pattern of a new ransomware family on which it was not trained over; and
  - Predict IRP logs from variants of ransomware families.
- Achieved accuracy, precision, recall, and F_1 scores in the range of 99.7% +/- 0.2% for every experiment setting
- Early detection and multiclass classification

Acknowledgement

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

THANK YOU!

Happy to take any questions you may have…