SAND2020-7306D

The Center for Cyber Defenders

Expanding computer security knowledge

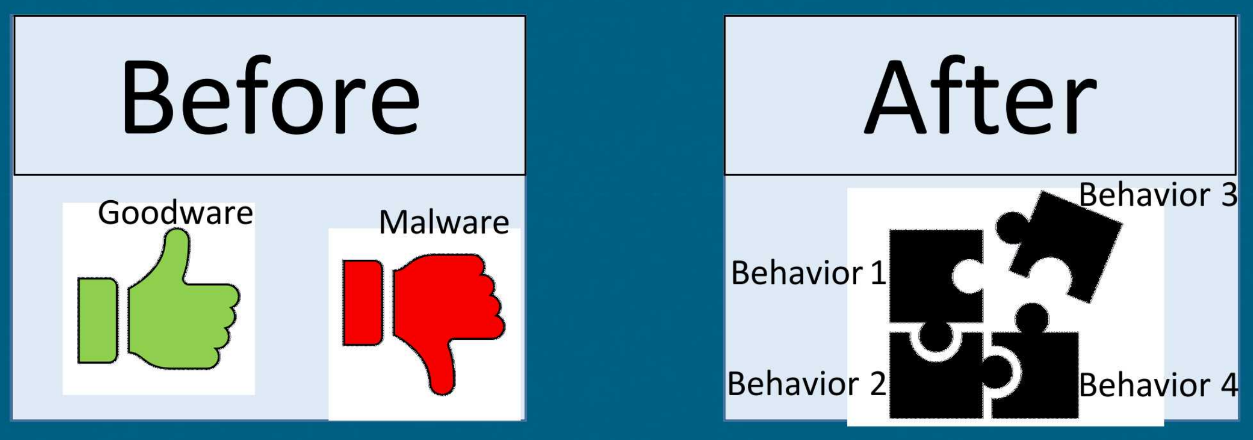
Classifying Malware Behaviors

Bridget Haus, University of Southern California, bhaus@usc.edu

Project Mentor: Nick Johnson, Org. 05953

Problem Statement:

- Malware poses a threat to national security
- Machine learning models claim success in malware detection, but their practical impact is unclear
- To identify novel malware, models must understand general behaviors and characteristics of malware



Objectives and Approach:

- Hand-labeled behaviors for 7 malware families with 9,640 total samples using open threat reports [1]
- Transformed malware files into black and white images (Fig.2)
- Trained two models to classify behaviors of a malware image
  - Baseline convolutional architecture [2]
  - Transfer learning from malware classifier [3]

Results:

- Train on 6 families test on hold out
- Transfer learning beat baseline model
- Majority Class classifier achieves best performance [4]
- Future work exploring performance and defining better experiment

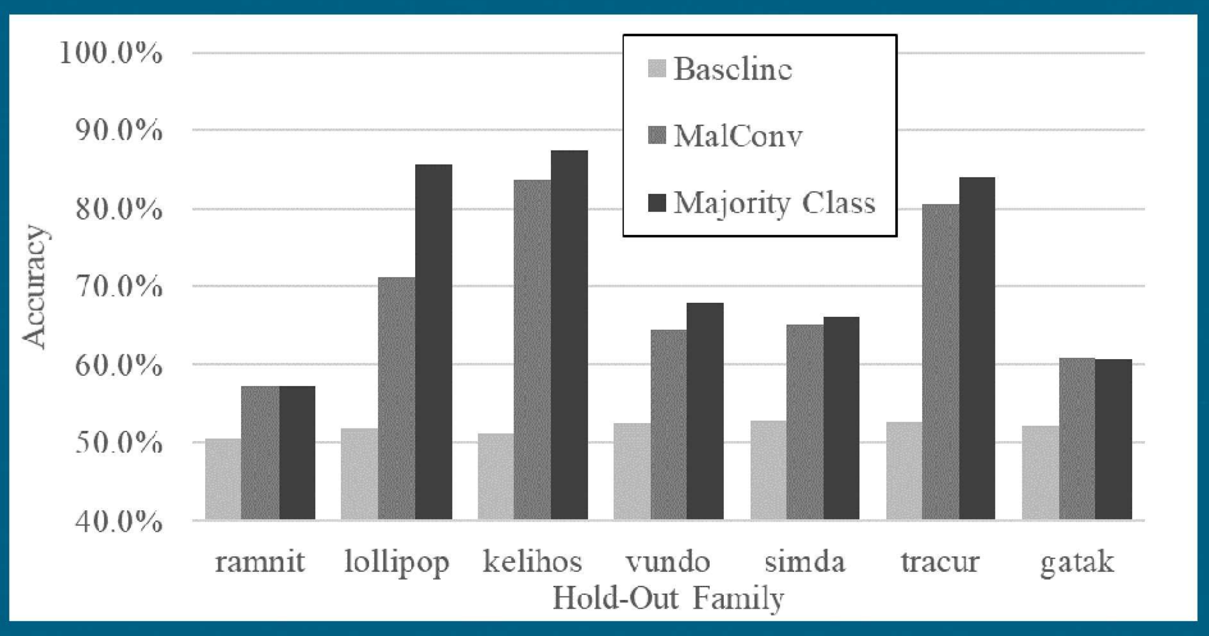


Fig. 3 Classifying Behaviors for Unseen Families

Impact and Benefits:

- Using behavioral labels allow ML models to generalize
- This is a proactive rather than reactive learning approach
- Gives ML models a better chance at zero/few-shot learning
- When a new variant of malware arises, our model will be equipped with a learned understanding of how malware spreads, operates and what it hopes to achieve.

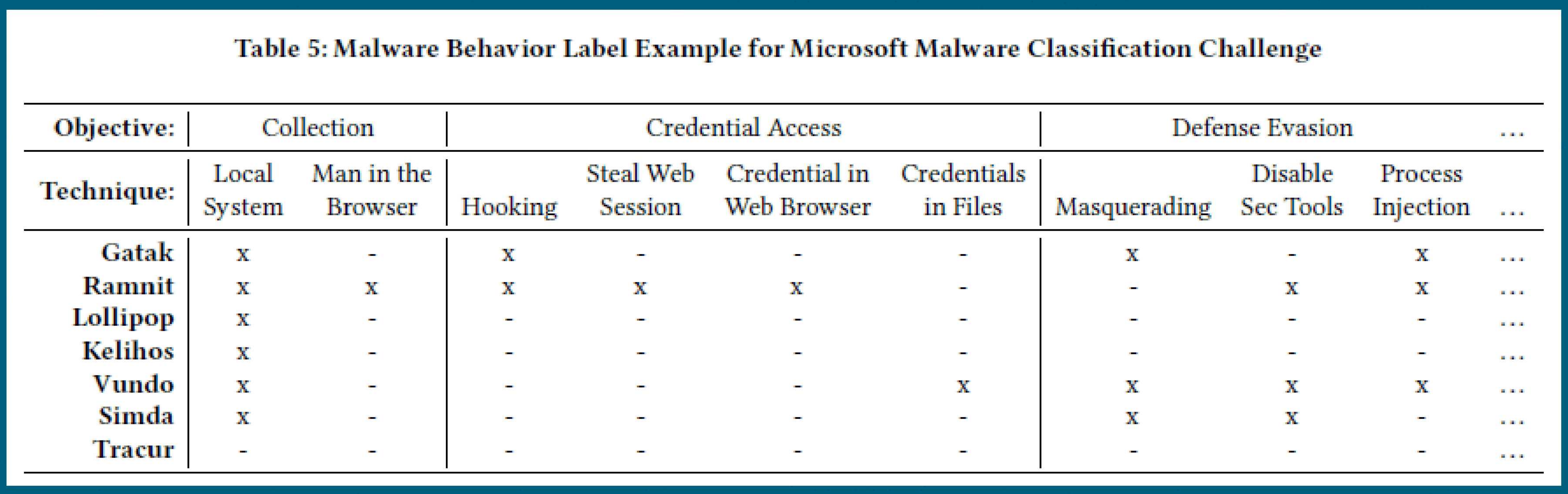


Table 5: Malware Behavior Label Example for Microsoft Malware Classification Challenge

Objective:	Collection		Credential Access				Defense Evasion			…
Technique:	Local System	Man in the Browser	Hooking	Steal Web Session	Credential in Web Browser	Credentials in Files	Masquerading	Disable Sec Tools	Process Injection	…
Gatak	x	-	x	-	-	-	x	-	x	…
Ramnit	x	x	x	x	x	-	-	x	x	…
Lollipop	x	-	-	-	-	-	-	-	-	…
Kelihos	x	-	-	-	-	-	-	-	-	…
Vundo	x	-	-	-	-	x	x	x	x	…
Simda	x	-	-	-	-	-	x	x	-	…
Tracur	-	-	-	-	-	-	-	-	-	…

Fig. 1 Example of behavioral labels

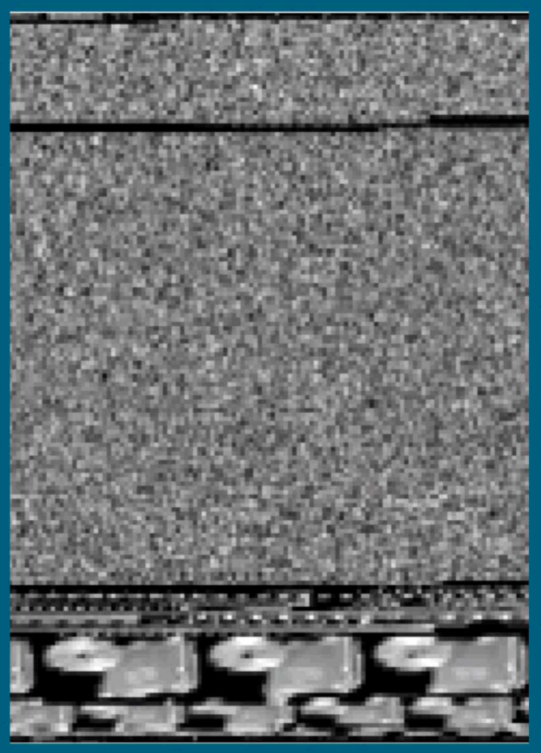


Fig. 2 Example of malware represented as grey scale image

[1] https://github.com/MBCProject/mbc-markdown
[2] https://pytorch.org/tutorials/beginner/blitz/cifar10_tutorial.html
[3] https://arxiv.org/abs/1710.09435
[4] https://arxiv.org/abs/2005.01800

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-XXXX X.