Team 7 Attack

Colton, Daehee, Richa

Black Box Attack

- Dropper
  - Program used: Iexpress packer
    - Application provided by windows to pack multiple pe files into single package
  - Packed Malware with Calc.exe
  - Completely bypassed our own model
- Adding Signature
  - Most malwares were missing signatures in the pe file
  - Adding signature confused our model

White Box Attack

- Major Target: Team 2, Team 4
  - Both team had dropper detection pipeline

Bypasses		Defemse						
Attack		Team 1	Team 2	Team 3	Team 4	Team 5	Team 6	Team 7
Team 1		100%	31.75%	100%	3.17%	100%	100%	100%
	Combined	0.00%	12.70%	4.76%	47.62%	14.29%	1.59%	3.17%
	Garbage	0.00%	3.17%	0.00%	0.00%	15.87%	0%	0%
	Section	1.59%	46.03%	6.35%	12.70%	53%	1.59%	4.76%
Team 2	UPX	0.00%	10.45%	8.96%	44.44%	14%	0%	5.97%
Team 3		100%	39.68%	100%	19.05%	100%	100%	100%
Team 4								
Team 5								
Team 6								
Team 7		100%	47.62%	100%	12.70%	100%	100%	100%

White Box Attack

- Pack malware with bigger benign PE file:
  - Detected Malwares were mostly larger Malwares
  - Used notepad++(6MB) instead of calc.exe(27KB)
  - *Packed file did not exceed Original file size + 5MB
- Nested Dropper
  - Nested dropping increased goodware probability
  - More samples bypassed using nested dropper
  - Stopped here to not exceed file size limitation