KARAMBIT.AI

SoURCE CODE Program: Lightning Talk

Andrew Hendela
andrew@karambit.ai

The Karambit.AI Team

Andrew Hendela
Co-founder

- 2 time DARPA PI, multi-program contributor
- Over a decade of cybersecurity research and development leadership

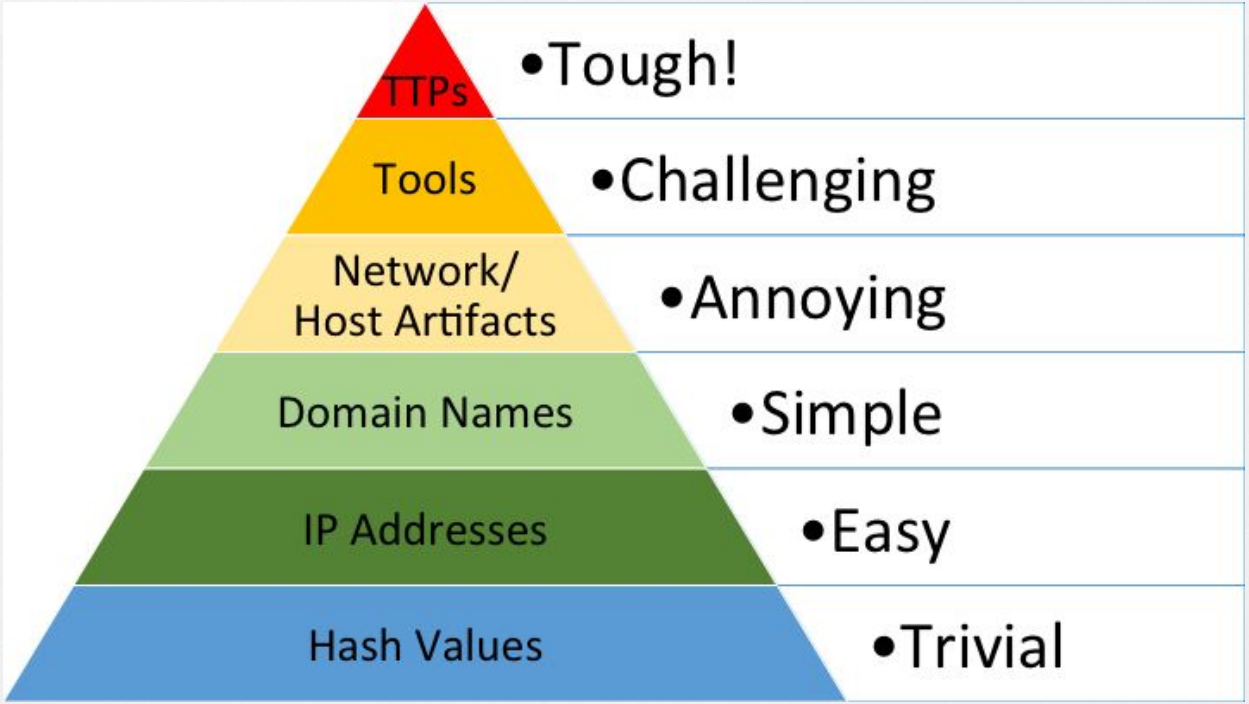
We have been working together for 9 years automating hard cybersecurity problems

cyber attribution,
exploit development,
malware analysis,
vulnerability research,
software supply chain security

Eric Lee
Co-founder

- Scalable program analysis R&D
- Offensive cybersecurity
- Developed autonomous bug-hunting system for the world's first all-machine cyber hacking tournament

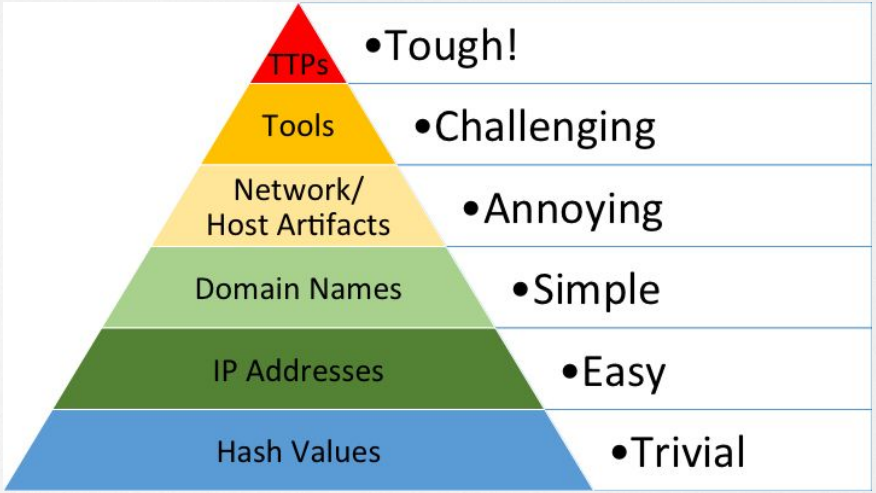
The Pyramid of Pain



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

What does this tell you about Attribution?

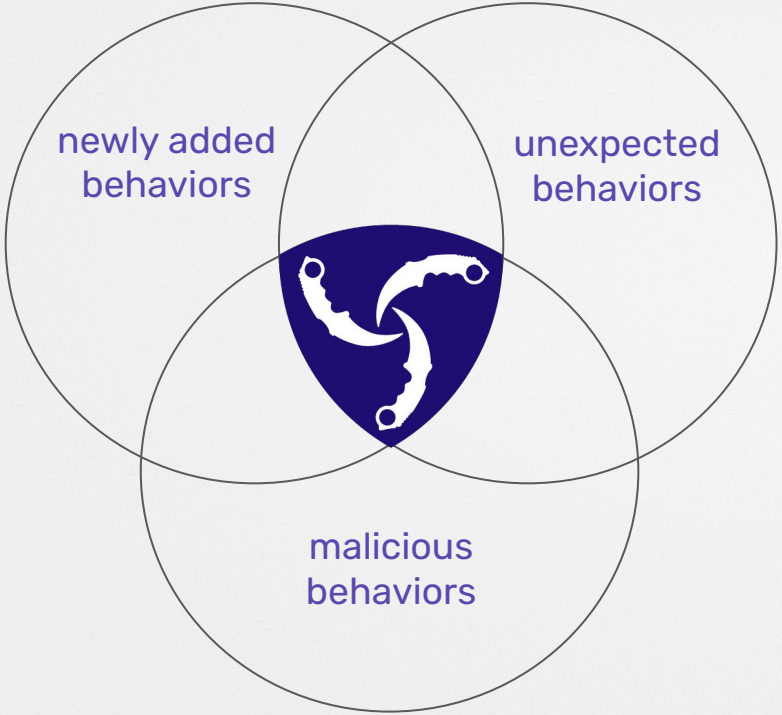
- Humans: expensive
  Infrastructure: cheap
  - Malware is better for attribution than C2
  - Change in TTPs requires change in behavior



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Karambit.AI

Automated Reverse Engineering to build Software Bills of Behaviors



We extract behaviors from binaries *without execution* and link them between samples and version to enhance ease of attribution and detection

TTP Malware Linkage

Search Query

rule_matches:'start minifilter driver'
rule_matches:'register minifilter driver'
rule_matches:'encode data using XOR'
rule_matches:'persist via Winlogon Helper DLL registry key'

SEARCH

8691322b2e93b7767bff762c3bc7a185fe279e0a5799e20bd6063035e8e27f5d

41f4823e7da9c45f09b62dcb9486b5c48d02c31efc37f0f643584c30b2f442ba

0ce8b85193481c3d701fa0499685f931ade5a26989b0ffd8565f7248072ff0ec

Why is this hard?

- Cybersecurity is inherently a *conflict* against other humans
  - No TTP is inherently malicious
  - Adversaries will change TTPs depending on target
  - Attackers will evade defenses

No Behavior is Inherently *Malicious*

Wannacry

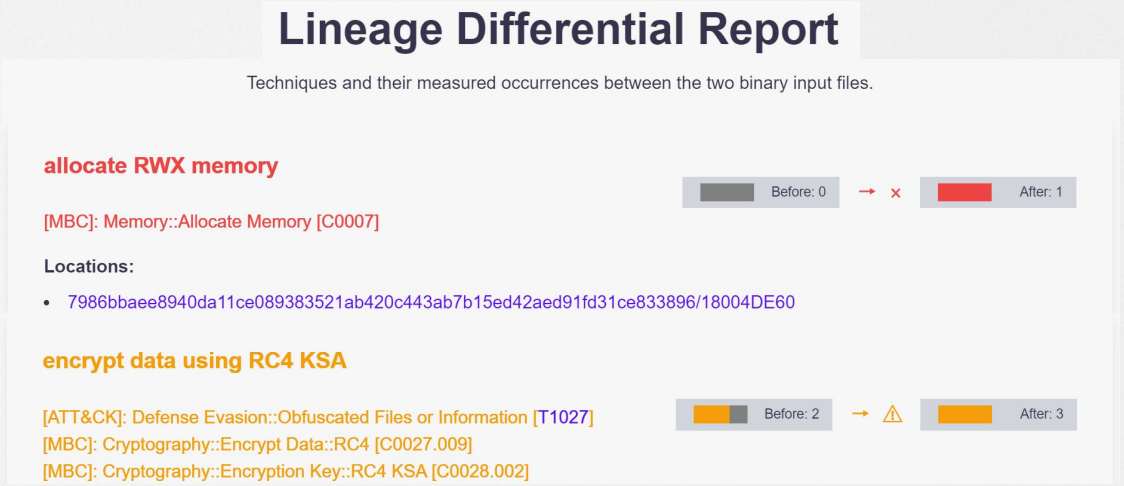
Microsoft BitLocker

Ransomware and Full Disk Encryption perform the same behavior

KARAMBIT.AI

TTP and Behavior-level Analysis

We can automatically detect small behavior changes engineered to evade antivirus and security teams, and link them to TTPs

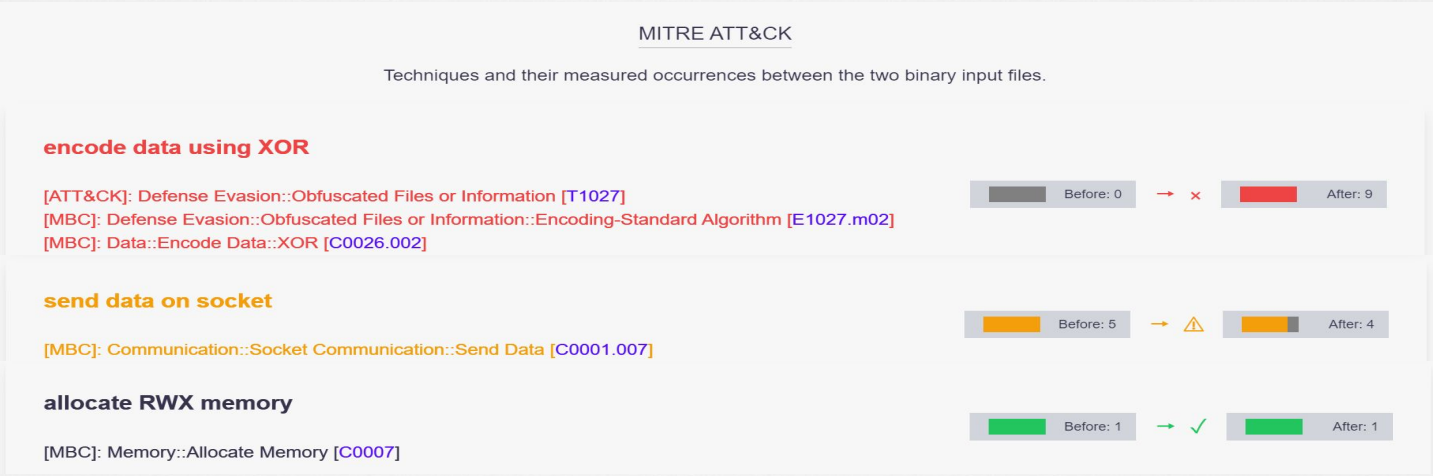


Detecting 3CX

View 3CX results Online: https://karambit.ai/app/diff/3CX-ffmpeg.json

KARAMBIT.AI

Adversaries will obfuscate malware

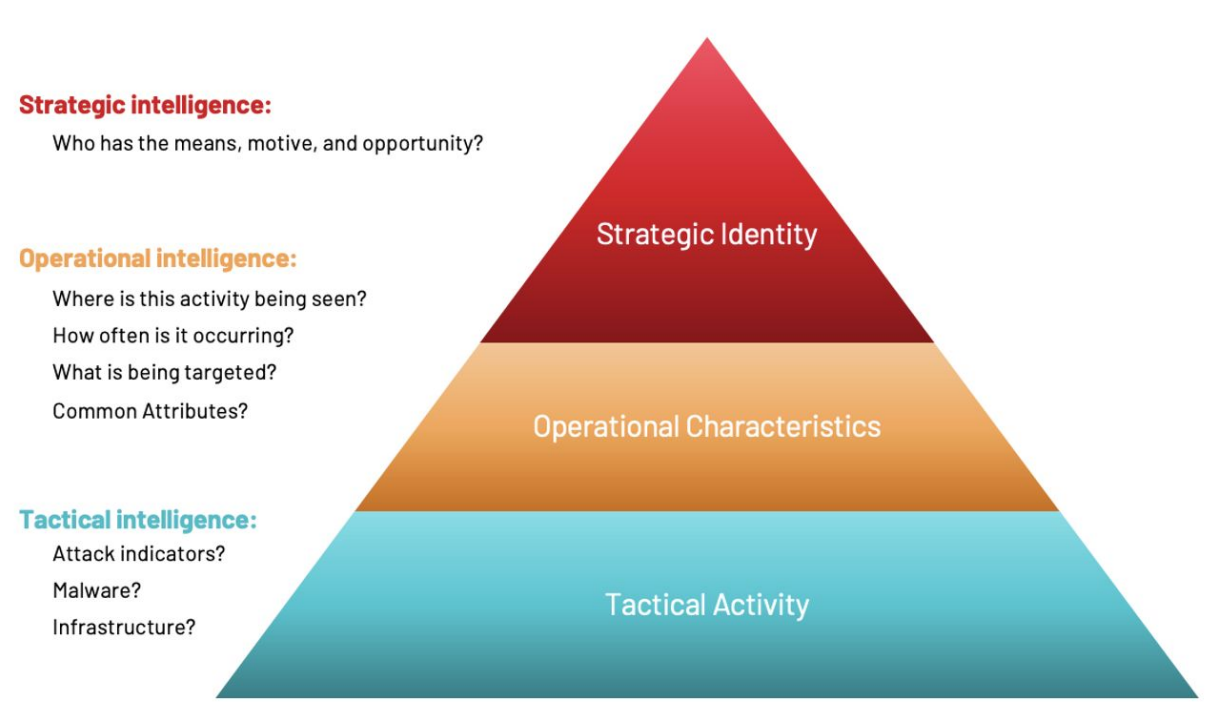


Exemplar Mirai Obfuscated With Tigress Obfuscator

- We can detect the attempts at obfuscation and evasion which become indicators of malware for attribution
- We defeat many forms of obfuscation, finding behaviors even after obfuscation has occurred

KARAMBIT.AI

Attribution Impact: Strategic Intelligence



https://www.mandiant.com/resources/blog/trade-offs-attribution

Try it out: https://karambit.ai/sign_up

Andrew Hendela
andrew@karambit.ai
https://karambit.ai
www.linkedin.com/in/andrew-hendela