HOMEMADE RAMEN & THREAT INTEL

A recipe for both
METAPHOR WARNING!!!
WHAT IS RAMEN?
WHAT IS THREAT INTELLIGENCE?
THE GOAL

Understand the combination of tools, inputs, process, & people that lead to creating a threat intelligence capability.
THE TOOLS
“SOMETHING (SUCH AS AN INSTRUMENT OR APPARATUS) USED IN PERFORMING AN OPERATION OR NECESSARY IN THE PRACTICE OF A VOCATION OR PROFESSION”

Merriam-Webster: Tool (Def 2a)
THE TOOLS FOR RAMEN
TOOLS

➤ Tongs
➤ Ladle
➤ “Spider”
➤ Knives & Cutting Boards
➤ “Base Infrastructure:” Pots & Pans, Stove Top Burner
INFRARED THERMOMETER

Aka Kitchen Laser Gun
THE TOOLS FOR CTI
import "pe"
import "hash"

rule dragos_crashoverride_suspicious_export {
  meta:
    description = "CRASHOVERRIDE v1 Suspicious Export"
    author = "Dragos Inc"

  condition:
    pe.exports("Crash")
}

rule dragos_crashoverride_suspicous_wiper {
  meta:
    description = "CRASHOVERRIDE v1 Wiper"
    author = "Dragos Inc"

  strings:
    $s0 = "SYS_BASCON.COM" fullword nocase wide
    $s1 = ".pcmp" fullword nocase wide
    $s2 = ".pcmi" fullword nocase wide
    $s3 = ".pcmt" fullword nocase wide
    $s4 = ".cin" fullword nocase wide

  condition:
    any of ($s*) and pe.exports("Crash")
}

overrun attempt;
flow:to_server,established;
content:"[18 03 03]|";
dep
1;
metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-recon; sid:30609; rev:5;

flow:to_client,established;
content:"byte_test:2,>128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-recon; sid:30514; rev:6;

flow:to_client,established;
content:"byte_test:2,>128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-recon; sid:30516; rev:6;

flow:to_client,established;
content:"byte_test:2,>128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-recon; sid:30517; rev:6;

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,636,692,993,995,2484] - possible ssl heartbleed attempt";
flow:to_server,established;
content:"[18 03 00]|";
dep
balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-admin; sid:30520; rev:3;

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,636,692,993,995,2484] - possible ssl heartbleed attempt";
flow:to_server,established;
content:"[18 03 00]|";
dep
1;
metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-admin; sid:30520; rev:3;

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,636,692,993,995,2484] - possible ssl heartbleed attempt";
flow:to_client,established;
content:"byte_test:2,>128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-admin; sid:30520; rev:3;

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,636,692,993,995,2484] - possible ssl heartbleed attempt";
flow:to_server,established;
content:"[18 03 00]|";
dep
1;
metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-admin; sid:30520; rev:3;

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,636,692,993,995,2484] - possible ssl heartbleed attempt";
flow:to_client,established;
content:"byte_test:2,>128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, serviceclasstype:attempted-admin; sid:30520; rev:3;";}
3RD PARTY SOURCES:
PASSIVE TOTAL & SHODAN
KEY: FITTING INTO YOUR ENVIRONMENT
“Remember, it is never the knife's fault.”

– Daniel Boulud
THE INGREDIENTS
“SOMETHING THAT ENTERS INTO A COMPOUND OR IS A COMPONENT PART OF ANY COMBINATION OR MIXTURE”

*Merriam-Webster: Ingredient*
THE INGREDIENTS FOR RAMEN
**BROTH BASE**

- 1 cup rough diced red delicious apple (about 1)
- 1 cup rough diced garlic (about 3 heads)
- 1 cup rough diced ginger
- 1 medium yellow onion
- 1/2 rack pork baby back ribs
- 12 cups water
- 1 cup soy sauce
NOODLES
BROTH EXTRAS

- 1 sheet kombu
- handful rough chopped dry shiitake mushrooms
- 1 half a diced sweet potato
- Ends of 1 bunch green onions
SERVING EXTRAS

- Slow Poached Eggs
- Nori/Wakame
- Siracha
- Sweet Potato
- Grilled Sweet Potato
THE INGREDIENTS FOR THREAT INTELLIGENCE
YOUR OWN INCIDENTS
YOUR TEAMS
VENDOR REPORTS
HONEYPOTS
PEERS/SHARING COMMUNITIES
3RD PARTY PAID INTELLIGENCE
Real food doesn't have ingredients, real food is ingredients.

–Jamie Oliver
THE RECIPE
“A SET OF INSTRUCTIONS FOR MAKING SOMETHING FROM VARIOUS INGREDIENTS”

Merriam-Webster: Recipe (2)
THE RECIPE FOR RAMEN
STEPS FOR RAMEN

➤ Bring water (Optional add dry shiitakes and nori) to a simmer
➤ Add other ingredients (except noodles) and bring to a boil
➤ Reduce heat and simmer 2.5-3 hours (reduced to about half)
➤ Prepare noodles and serve with extras
INTELLIGENCE CYCLE
F3EAD

FIND

FIX

FINISH

EXPLOIT

ANALYZE

DISSEMINATE
LESSONS LEARNED & PRACTICE
“Today’s innovation is tomorrow’s tradition.”

–Lidia Bastianich
THE COOKS
GREAT COOKS EAT
(CONSUME)
GREAT COOKS COOK
(CREATE)
GREAT COOKS LEARN (GROWTH)
“Cook, cook, and cook. Keep your hands as involved in the kitchen and as much as you can and don’t seek glamour.”

–Gaggan Anand
THE OUTPUT
INTELLIGENCE PRODUCTS
SHORT FORM REPORTS
LONG FORM REPORTS
CONCLUSION
TAKEAWAYS

➤ Think about your tools
➤ Get to know and understand your inputs
➤ Focus on honing your processes
➤ Grow your people
RAMEN RECIPE

➤ 1 cup rough diced red delicious apple (about 1)
➤ 1 cup rough diced garlic (about 3 heads)
➤ 1 cup rough diced ginger
➤ 1 medium yellow onion
➤ 1/2 rack pork baby back ribs
➤ 12 cups water
➤ 1 cup soy sauce

➤ Bring water to a simmer
➤ Add other ingredients and bring to a boil
➤ Reduce heat to low and simmer 2.5-3 hours
➤ Remove ribs & discard veggies, shred pork, & prepare ramen noodles
➤ Plate w/ noodles, broth, pork, & extras then serve
➤ Good extras ideas include Slow Poached Eggs, Nori/Wakame, Siracha, Grilled Sweet Potato
THANKS
“Usually, one’s cooking is better than one thinks it is.”

–Julia Child