Indicators of Compromise

draft-paine-smart-indicators-of-compromise-00

Draft

- Available on Datatracker: https://tools.ietf.org/html/draft-paine-smart-indicators-of-compromise-00
- And Github: https://github.com/smart-rg/drafts/blob/master/draft-paine-smart-indicators-of-compromise-00.txt
- Had comments and detailed review from a couple of people – more feedback welcome!

Motivation

- To share knowledge with protocol engineers on a commonly used and important technique in cyber defence
- To prevent this technique being accidentally ignored
  - Engineers can make protocol design choices that affect IoC availability
  - And we'd like the IETF community at large to consider the impact of IoC availability
- To bring cyber defence expertise into the IETF and share it through this Informational RFC

Draft introduction

Indicators of Compromise (IoCs) and Their Role in Attack Defence
draft-paine-smart-indicators-of-compromise-00

Abstract

Indicators of Compromise (IoCs) are an important technique in attack defence (often called cyber defence). This document outlines the different types of IoC, their associated benefits and limitations, and discusses their effective use. It also contextualises the role of IoCs in defending against attacks through describing a recent case study. This draft does not pre-suppose where IoCs can be found or should be detected - as they can be discovered and deployed in networks, endpoints or elsewhere - rather, engineers should be aware that they need to be detectable (either by endpoint security appliances or network-based defences, or ideally both) to be effective.

Draft structure

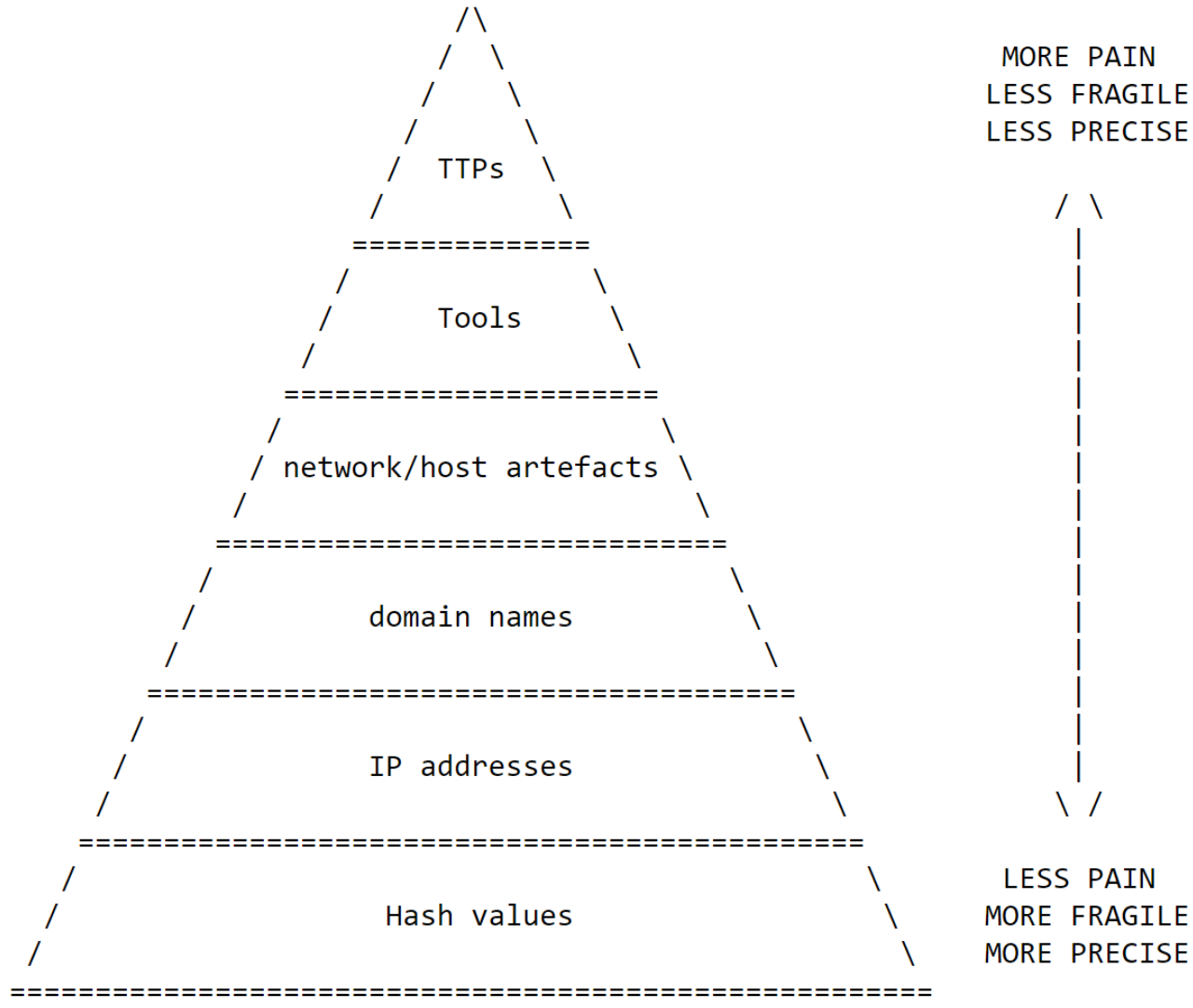
Table of Contents

What are IoCs?

Indicators of Compromise (IoCs) are artefacts observed about an attacker; their techniques, tactics, procedures or associated tooling and infrastructure. These indicators can be observed at a combination of network or host levels and can, with varying degrees of confidence, help to identify an occurrence of an intrusion or associated activity to a known intrusion set. These IoCs are used by network defenders (blue teams) to protect their networks. Examples of IoCs can include:

- IP addresses
- domain names
- TLS Server Name Indicator values
- certificate information
- signatures such as binary code patterns and strings
- hashes of malicious binaries or scripts

Pyramid of pain



Next Steps

- Possibly MILE, SACM?
- Open to suggestions from the chairs…