Indicators of Compromise

draft-paine-smart-indicators-of-compromise

Ollie Whitehouse, NCC Group

History

- Available on Datatracker: https://tools.ietf.org/html/draft-paine-smart-indicators-of-compromise-03

- Presented -00 at secdispatch in IETF 109
- Revised based on feedback on list and in meeting
- Brought to OPSEC mailing list this year
- Thanks to Nancy Camwinget and Fernando Gont for their thorough reviews on -02

Motivation

- To document this existing operational security practice as a baseline
- To share knowledge with protocol engineers on a commonly used technique in cyber defence
- To prevent this technique being accidentally ignored
  - Engineers can make protocol design choices that affect IoC availability
  - So we'd like the IETF community at large to know about IoC techniques
- To bring cyber defence expertise into the IETF and share it through an Informational RFC, and begin cross-pollination of industry experiences

Draft introduction

Indicators of Compromise (IoCs) and Their Role in Attack Defence
draft-paine-smart-indicators-of-compromise-03

Abstract

Cyber defenders frequently rely on Indicators of Compromise (IoCs) to identify, trace, and block malicious activity in networks or on endpoints. This draft reviews the fundamentals, opportunities, operational limitations, and best practices of IoC use. It highlights the need for IoCs to be detectable in implementations of Internet protocols, tools, and technologies - both for the IoCs' initial discovery and their use in detection - and provides a foundation for new approaches to operational challenges in network security.

Draft structure

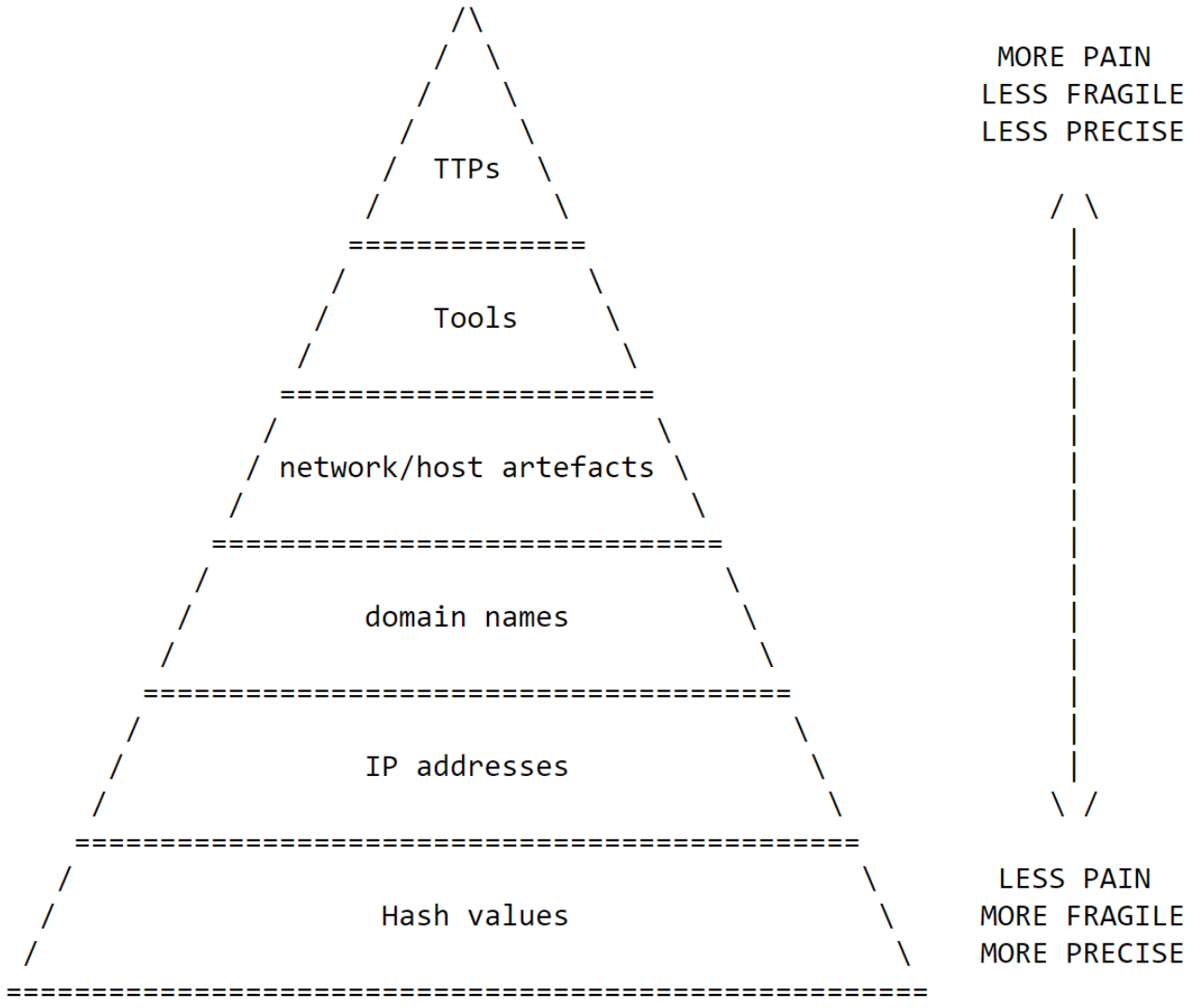
Old

New

What are IoCs?

- IPv4 and IPv6 addresses in network traffic.
- DNS domain names in network traffic, resolver caches or logs.
- TLS Server Name Indication values in network traffic.
- Code signing certificates in binaries or TLS certificate information (such as SHA256 hashes) in network traffic.
- Cryptographic hashes (e.g. MD5, SHA1 or SHA256) of malicious binaries or scripts when calculated from network traffic or file system artefacts.
- Attack tools (such as Mimikatz) and their code structure and execution characteristics.
- Attack techniques, such as Kerberos golden tickets, which can be observed in network traffic or system artefacts.

Pyramid of pair



IoC Lifecycle

- New section based on feedback
  - Discovery
  - Assessment
  - Sharing
  - Deployment
  - Detection
  - Reaction
  - End of Life

Questions/Next Steps

- Further feedback and comments welcome from this group
- Is the work in scope for opsec?
- Would the group consider WG adoption?