Indicators of Compromise (IoCs) and Their Role in Attack Defence

draft-ietf-opsec-indicators-of-compromise

History

- Brought to SECDISPATCH at IETF 107
- Brought to OPSEC mailing list early 2021
- Updates based on reviews and feedback
- Presented in OPSEC meeting at IETF 111
- Adopted by OPSEC WG in January 2022
  - No further reviews or comments
- Latest version published earlier this month

Motivation

- To document this existing operational security technique and capture best practice
- To share knowledge with protocol engineers on a commonly used and important technique in cyber defence
- To prevent this technique being overlooked in protocol design
  - Engineers can make protocol design choices that affect IoC availability
  - 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 document

Abstract

Indicators of Compromise (IoCs) and Their Role in Attack Defence
draft-ietf-opsec-indicators-of-compromise-01

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.

What are IoCs?

- Indicators of Compromise (IoCs) are observable artefacts relating to an attacker or their activities, such as their tactics, techniques, procedures, and associated tooling and infrastructure
- Examples:
  - IPv4 and IPv6 addresses
  - Domain names
  - Cryptographic hashes of malicious binaries
  - Attack tools and their code structure and execution characteristics
  - Attack techniques which can be observed in network traffic or system artefacts

Outline

- IoC Fundamentals
  - What are IoCs?
  - Pyramid of Pain
  - IoC Lifecycle
- Using IoCs effectively
  - Opportunities
  - Case Studies – Cobalt Strike and APT33
- Operational Limitations
  - Time and Effort
  - Precision
- Best Practice

Next Steps

- Further reviews and comments from the WG welcomed
- Is this document ready for Working Group Last Call?