Network Working Group
Internet-Draft
Intended status: Informational
Expires: 11 October 2025

S. Grimminck, Ed.

9 April 2025

A Standard for Safe and Reversible Sharing of Malicious URLs and Indicators

draft-grimminck-safe-ioc-sharing-03

Abstract

This document defines a consistent and reversible method for sharing potentially malicious indicators of compromise (IOCs), such as URLs, IP addresses, email addresses, and domain names. It introduces a safe obfuscation format to prevent accidental execution or activation when IOCs are displayed or transmitted. These techniques aim to standardize the safe dissemination of threat intelligence data. This specification uses the URI syntax defined in RFC 3986 and follows the key word conventions from RFC 2119.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 11 October 2025.

Copyright Notice

Table of Contents

1. Introduction

The secure sharing of malicious artifacts is vital to threat intelligence, open-source intelligence (OSINT), and incident response efforts. However, sharing raw URLs, IP addresses, and email addresses associated with malware or threat actors poses a risk of accidental activation.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document defines a clear and reversible method for obfuscating and de-obfuscating IOCs to support safe sharing across various platforms, formats, and use cases. The requirements language (e.g., "MUST", "SHOULD") follows [RFC2119], and URI syntax adheres to [RFC3986].

2. Terminology

Obfuscating: The process of altering an indicator so that it cannot be accidentally activated or clicked. This was previously referred to as "defanging".

De-obfuscating: The process of restoring an obfuscated indicator to its original, actionable form. This was previously referred to as "refanging".

IOC: Indicator of Compromise - data such as a URL, IP address, domain name, email address, or hash associated with malicious activity.

3. Problem Statement

Inconsistent obfuscation practices hinder the reliable and automated exchange of threat intelligence. For example:

* A URL obfuscated as "h**p://example[.]com" cannot be reliably parsed by tools expecting "hxxp://example[.]com".

* An IP address obfuscated with parentheses (e.g., "192.0.2(.)1") may fail to de-obfuscate in systems expecting "[.]".

Such inconsistencies reduce the effectiveness of threat detection and response.

4. Obfuscation Techniques

The following transformations MUST be consistently applied:

* Replace "http" and "https" schemes with "hxxp" and "hxxps" respectively.

* Replace every period (".") in domain names and IP addresses with "[.]".

* Replace the "@" character in email addresses or credentials with "[@]".

Using encoded characters (such as %2e for ".") SHOULD be avoided to prevent ambiguity.

Examples:

* Original: https://evil.example.com/path
  Obfuscated: hxxps://evil[.]example[.]com/path

* Original: http://username:password@attacker.com
  Obfuscated: hxxp://username:password[@]attacker[.]com

* Original: user@phishing.example.com
  Obfuscated: user[@]phishing[.]example[.]com

* Original: http://192.0.2.1
  Obfuscated: hxxp://192[.]0[.]2[.]1

* Original: http://[2001:db8::1]:8080
  Obfuscated: hxxp://[2001:db8::1]:8080

Note: Credentials in URIs (e.g., _username:password_) are included here for illustrative purposes only. Sharing credentials, even in obfuscated form, is strongly discouraged in operational contexts.

Note: IPv6 addresses enclosed in square brackets MUST retain their colon-based syntax (e.g., "::") and brackets. These characters are essential to URI parsing and MUST NOT be altered. Obfuscation should apply only to components such as the scheme ("http") or domains, not to the IPv6 address syntax.

5. De-obfuscation Techniques

Tools designed to ingest obfuscated data SHOULD automatically reverse these transformations in a deterministic manner:

* Convert "hxxp" and "hxxps" back to "http" and "https" respectively.

* Convert "[.]" back to ".".

* Convert "[@]" back to "@".

De-obfuscation MUST maintain the original semantics of the data to avoid misinterpretation. Examples:

* Obfuscated: hxxps://evil[.]example[.]com/path
  De-obfuscated: https://evil.example.com/path

* Obfuscated: user[@]phishing[.]example[.]com
  De-obfuscated: user@phishing.example.com

6. Example Use Cases

Common scenarios include:

* **OSINT Sharing**: A report lists obfuscated URLs (e.g., "hxxp://malware[.]com/payload") to prevent accidental clicks.

* **Email Communication**: Security teams share obfuscated IOCs like "attacker[@]example[.]com" in email threads.

* **Threat Intelligence Platforms**: Automated ingestion of obfuscated IPs (e.g., "192[.]0[.]2[.]1") for blocklist updates.

7. Security Considerations

While these obfuscation techniques reduce the risk of accidental activation of malicious indicators, obfuscated data SHOULD always be handled with caution.

Repeated application of obfuscation without proper context or normalization MAY result in ambiguous or non-reversible transformations. Implementations SHOULD avoid multiple layers of obfuscation without canonicalization.

* Obfuscated URLs in PDFs may still be rendered as hyperlinks; use plain-text formatting.

* Systems processing obfuscated indicators MUST treat them as potentially harmful data, applying sandboxing or isolated environments for analysis.

* Credentials (e.g., _username:password_) SHOULD NOT be shared, even in obfuscated form, due to inherent security risks.

8. Implementation Guidance

Software designed to parse threat intelligence feeds should explicitly support these obfuscation and de-obfuscation standards. Implementations SHOULD verify correct de-obfuscation through unit tests and validation scripts. Example test case:

```
Test Input: "hxxp://192[.]0[.]2[.]1"
Expected Output: "http://192.0.2.1"
```

9. Edge Cases and Special Handling

Internationalized Domain Names (IDNs): Obfuscate punycode domains similarly (e.g., "xn--example[.]com").

Non-Standard URI Schemes: For schemes like "ftp", apply analogous obfuscation (e.g., "fxp://example[.]com").

IPv6 Literals in URIs: Do not alter colon characters (":") or brackets ("[", "]") in IPv6 addresses. For example, "[2001:db8::1]" MUST remain unchanged. Only scheme names or domain elements surrounding them should be obfuscated.

10. IANA Considerations

This document has no IANA actions.

11. Normative References

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Author’s Address

Stefan Grimminck (editor)
Email: ietf@stefangrimminck.nl