Bank of England PRA

STAR-FS Targeting Report Specification

Simulated Targeted Attack & Response Assessments

Contents

Executive Summary

This document presents the specification for the Targeting Report deliverable developed by the Threat Intelligence Service Provider (TISP) during the Threat Intelligence phase of the STAR-FS assessment.

It should be noted that the specification presented in this report represents the minimum standard expected. There is an expectation that the TISP will extend the template so they can offer additional value to the commissioning firm/FMI.

Comments and feedback on this document are welcome from all parties and should be sent to **STAR-FS@crest-approved.org**. Please place "[STAR-FS TARGETING REPORT FEEDBACK]" in the subject line of the email.

This document should be used in the threat intelligence phase, as described in section 6 of the **STAR-FS implementation guide**.

Legal Disclaimer

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice, and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances. The sponsors and authors of this document shall accept no responsibility for any errors, omissions or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed within it.

Copyright notice

1. Introduction

Purpose of this document

An output of the STAR-FS Threat Intelligence (TI) phase is the Targeting Report. This deliverable is produced by the TISP for delivery to the firm/FMI. The Targeting Report is for use by:

- STAR-FS TISP — to show what kind of threat intelligence the commissioning Firm/FMI will require as a minimum;
- STAR-FS Penetration Testing service provider (PTSP) — to show what kind of intelligence will be provided for the purpose of configuring their penetration tests.

As described in the STAR-FS implementation guide, during the Threat Intelligence phase of a STAR-FS assessment the TISP conducts a broad-based targeting exercise to emulate a threat actor's approach to acquiring targets. This involves gathering background information both on and from the target organisation using intelligence sources such as OSINT, TECHINT and FININT. The output of this activity is a Targeting Report as specified by this document.

Equipped with this report, and the Threat Intelligence Report, the PTSP will have a firm evidential basis for designing and justifying a realistic and effective penetration test.

For the purpose of clarity, the definitions of "threat" and "intelligence" are set out below:

Threat

- an expression of intent to do harm, i.e., deprive, weaken, damage or destroy;
- an indication of imminent harm;
- an agent, in pursuit of its goals, that is regarded as harmful;
- a harmful agent's actions comprising of tactics, techniques, and procedures (TTPs).

Intelligence

- Information that provides relevant and sufficient understanding for mitigating a potentially harmful event.

2. Introduction

Overview

The Targeting Report is a bespoke report generated by the TISP during the Targeting stage of a STAR-FS assessment. It identifies, on a system-by-system basis, the attack surfaces of people, processes and infrastructure relating to the commissioning firm/FMI.

The Targeting Report constitutes a valuable input into the Threat Intelligence Report that is also developed by the TISP. For example, any relevant assets identified (such as an exposed insecure server) should be integrated into scenarios and exploited by threat actors.

Equipped with this report, and the Threat Intelligence Report, the PTSP will have a firm evidential basis for designing and justifying a realistic and effective penetration test.

The Targeting Report document is not an HM Government-produced document and therefore should carry a protective marking that is mutually enforced by the commissioning and delivery parties. For example: "COMMERCIAL IN CONFIDENCE".

Production of this report is mandatory and the STAR-FS templates will be audited and sampled on a regular basis to ensure standards remain high.

The structure and content of the Targeting Report is as follows:

- the first section, Scope, defines the overall scope of the targeting exercise;
- subsequent sections then follow for each system in scope, each section providing system-specific detail about associated people, process and infrastructure attack surfaces.

This will enable PTSP to utilise each section of the Targeting Report independently according to the scenario being applied. Providing PTSP with individual targeting packs for each system will also enable greater granularity around a system's key defence weaknesses to be defined.

It should be noted that the specification presented in this section represents the minimum standard expected. There is an expectation that TISP will extend the template defined below so they can offer additional value to the commissioning firm/FMI.

The above sections are covered in more detail below:

Scope

This section defines the overall scope of the targeting exercise.

Objectives

Objective of the targeting as determined by the commissioning firm/FMI, bearing in mind that the overall objective of a STAR-FS assessment is to establish the resilience of an Important Business Service (IBS) to attack.

Important Business Services

Details of the IBS agreed to be tested by the Regulator and the commissioning Firm/FMI. This will include:

- geographies concerned with the delivery and use of the IBS;
- languages in use;
- brands of the operating company involved;
- third parties involved in the delivery of the IBS;

Depending on the organisation, the IBS under test will vary and a sub-set may be selected.

Targeting Methods

Summary of the targeting methods used. This will include intelligence sources such as OSINT, TECHINT and FININT as well as activities such as research, monitoring and forensics.

Ethical Standard Statement

A statement of confirmation from the TISP that it has observed an appropriate ethical standard for conducting targeting activities.

Systems

Each system in scope for a STAR-FS test should provide detail about associated people, process, and infrastructure attack surfaces specific to that system.

Information provided in this section should include photographs, screen shots, diagrams, forum messages, social media messages, etc., to add as much impact as possible.

People

This sub-section should provide information about human targets related to the target system. It should include:

- business personnel and stakeholders — those that have authority;
- technical personnel and stakeholders — those that have access to the target;
- third parties that support the target system;
- users and service delivery partners that can be used to influence access to the target.

The Targeting report should examine how these individuals can be influenced and controlled. It should also highlight the types of information that can be gathered by examining the online footprint.

Processes

This sub-section should provide a list of key processes that surround the target system such as enrolment, service management, help desk, etc. The purpose of enumerating these is to explore how the integrity of a process may be disrupted in order to gain access to the target.

Infrastructure

This sub-section should provide a list of key of the technical controls that surround the target system. It should list the technologies used and show how these might be accessed through public or private routes.