ThreatConnect™

# ThreatConnect® Domain-Spinning Workbench

## Installation and Configuration Guide

**Software Version 1.0**

**July 31, 2020**

30052-02 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: .703.229.4489
www.ThreatConnect.com

# Table of Contents

# OVERVIEW

The ThreatConnect Domain-Spinning Workbench Spaces app provides four different algorithms for identifying potential domain squats related to an input domain name. The list of domain names it provides can be used to take preventative measures against potential squats or to take action against actual squats. Users can import selected domain names into ThreatConnect as Indicators. The methods for identifying squats include open-source algorithms and algorithms developed by the ThreatConnect Research Team.

# DEPENDENCIES

## ThreatConnect Spaces App

- TCS - Domain Spinning v1.0 Spaces app
  Package name: TCS_-_Domain_Spinning_v1.0.tcx

## Playbooks

- Bitsquatting
- DNS Lookup
- DNS Twist
- Domain Squat Import
- DomainTools WHOIS Lookup
- ThreatConnect WHOIS Lookup
- URLCrazy
- XNTwist

# Playbooks Apps

| App Name | Package Name |
|---|---|
| Whois Lookup | TCPB_-_Whois_Lookup_v1.0.tcx |
| Get DomainTools Enrichment | TCPB_-_DomainTools_Enrichment-1.0.zip |
| DNSTwist | TCPB_-_DNSTwist_v1.0.tcx |
| XNTwist | TCPB_-_XNTwist_v1.0.tcx |
| Bitsquatting | TCPB_-_Bitsquatting_v1.0.tcx |
| URLCrazy | TCPB_-_URLCrazy_v1.0.tcx |
| Join Array | TCPB_-_JoinArray_v1.0.zip |
| Split String | TCPB_-_SplitString_v1.0.zip |
| DNS Lookup | TCPB_-_DNS_Lookup_v1.0.tcx |
| Json Path | TCPB_-_JsonPath_v1.0.zip |
| Get Array Length | TCPB_-_GetArrayLength_v1.0.zip |
| Fill Array | TCPB_-_FillArray_v1.0.zip |
| Create ThreatConnect Incident | TCPB_-_IncidentCreate_v1.0.tcx |
| Create ThreatConnect Host | TCPB_-_HostCreate_v1.1.tcx |

| | |
|---|---|
| Create Association | TCPB_-_AssociationCreate_v1.0.tcx |
| Create ThreatConnect Tag | TCPB_-_TagCreate_v1.0.tcx |
| Create ThreatConnect Email Address | TCPB_-_EmailAddressCreate_v1.1.tcx |
| Parse TCEntity | TCPB_-_Parse_TCEntity_v1.0.tcx |
| Create Custom Indicator Association | TCPB_-_CustomAssociationCreate_v1.1.tcx |
| Send Slack Message | TCPB_-_Slack_Messaging_v1.0.zip |

# INSTALLATION

## Spaces App

Use the App Catalog to install the **TCS - Domain Spinning v1.0** SpaceOrganization app. For more information on how to install an app, see the "Apps and Jobs" section of the *ThreatConnect System Administration Guide*.

## Playbooks

Use the App Catalog to install each of the eight Playbooks.

### Recommendations

1. Add "Domain Spinning: " to the beginning of each Playbook's name (e.g., "Domain Spinning: Bitsquatting") so that the Playbooks associated with the Domain-Spinning Workbench app can be easily identified.
2. Save all of the Playbook URLs as text variables in the target Organization for easier entry into the app configuration and subsequent modification. For more information on creating variables, see the "Variables" section of the *ThreatConnect Organization Administration Guide*. This task may be done by an Organization Administrator.

# Custom Association

Follow these steps to create a custom Association so that all imported Hosts and EmailAddresses are associated with each other, with the Host as a primary Indicator:

1. Follow the steps in the "Creating Custom Associations" section of the *ThreatConnect System Administration Guide* to open the **Create Custom Indicator Association** window.
2. Enter the following parameters to create a custom Association called **Domain Registrant Email**:
    - **Name**: Domain Registrant Email
    - **Association Api Branch**: domainRegistrant
    - **Primary Indicator Type**: Host
    - **Associate Non-Primary Indicators**: Uncheck this box.
    - **Indicators**: Check the **EmailAddress** box.