# TTP Detail – T1567.004

## TTP Information

Name: Exfiltration Over Webhook

Description: Adversaries may exfiltrate data to a webhook endpoint rather than over their primary command and control channel. Webhooks are simple mechanisms for allowing a server to push data over HTTP/S to a client without the need for the client to continuously poll the server.(Citation: RedHat Webhooks) Many public and commercial services, such as Discord, Slack, and `webhook.site`, support the creation of webhook endpoints that can be used by other services, such as Github, Jira, or Trello.(Citation: Discord Intro to Webhooks) When changes happen in the linked services (such as pushing a repository update or modifying a ticket), these services will automatically post the data to the webhook endpoint for use by the consuming application.

Adversaries may link an adversary-owned environment to a victim-owned SaaS service to achieve repeated [Automated Exfiltration](https://attack.mitre.org/techniques/T1020) of emails, chat messages, and other data.(Citation: Push Security SaaS Attacks Repository Webhooks) Alternatively, instead of linking the webhook endpoint to a service, an adversary can manually post staged data directly to the URL in order to exfiltrate it.(Citation: Microsoft SQL Server)

Access to webhook endpoints is often over HTTPS, which gives the adversary an additional level of protection. Exfiltration leveraging webhooks can also blend in with normal network traffic if the webhook endpoint points to a commonly used SaaS application or collaboration service.(Citation: CyberArk Labs Discord)(Citation: Talos Discord Webhook Abuse)(Citation: Checkmarx Webhooks)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: exfiltration