# TTP Detail – T1114.003

## TTP Information

Name: Email Forwarding Rule

Description: Adversaries may setup email forwarding rules to collect sensitive information. Adversaries may abuse email forwarding rules to monitor the activities of a victim, steal information, and further gain intelligence on the victim or the victim’s organization to use as part of further exploits or operations.(Citation: US-CERT TA18-068A 2018) Furthermore, email forwarding rules can allow adversaries to maintain persistent access to victim's emails even after compromised credentials are reset by administrators.(Citation: Pfammatter - Hidden Inbox Rules) Most email clients allow users to create inbox rules for various email functions, including forwarding to a different recipient. These rules may be created through a local email application, a web interface, or by command-line interface. Messages can be forwarded to internal or external recipients, and there are no restrictions limiting the extent of this rule. Administrators may also create forwarding rules for user accounts with the same considerations and outcomes.(Citation: Microsoft Tim McMichael Exchange Mail Forwarding 2)(Citation: Mac Forwarding Rules)

Any user or administrator within the organization (or adversary with valid credentials) can create rules to automatically forward all received messages to another recipient, forward emails to different locations based on the sender, and more. Adversaries may also hide the rule by making use of the Microsoft Messaging API (MAPI) to modify the rule properties, making it hidden and not visible from Outlook, OWA or most Exchange Administration tools.(Citation: Pfammatter - Hidden Inbox Rules)

In some environments, administrators may be able to enable email forwarding rules that operate organization-wide rather than on individual inboxes. For example, Microsoft Exchange supports transport rules that evaluate all mail an organization receives against user-specified conditions, then performs a user-specified action on mail that adheres to those conditions.(Citation: Microsoft Mail Flow Rules 2023) Adversaries that abuse such features may be able to enable forwarding on all or specific mail an organization receives.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: collection

## APTs (Intrusion Sets)

* Kimsuky
* LAPSUS$
* Silent Librarian
* Star Blizzard