# TTP Detail – T1114.001

## TTP Information

Name: Local Email Collection

Description: Adversaries may target user email on local systems to collect sensitive information. Files containing email data can be acquired from a user’s local system, such as Outlook storage or cache files.

Outlook stores data locally in offline data files with an extension of .ost. Outlook 2010 and later supports .ost file sizes up to 50GB, while earlier versions of Outlook support up to 20GB.(Citation: Outlook File Sizes) IMAP accounts in Outlook 2013 (and earlier) and POP accounts use Outlook Data Files (.pst) as opposed to .ost, whereas IMAP accounts in Outlook 2016 (and later) use .ost files. Both types of Outlook data files are typically stored in `C:\Users\<username>\Documents\Outlook Files` or `C:\Users\<username>\AppData\Local\Microsoft\Outlook`.(Citation: Microsoft Outlook Files)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* Carbanak
* CosmicDuke
* Crimson
* Emotet
* KGH\_SPY
* LunarMail
* QakBot
* Smoke Loader

## Tools

* Empire
* Out1
* Pupy

## APTs (Intrusion Sets)

* APT1
* Chimera
* Magic Hound
* RedCurl
* Sea Turtle
* Winter Vivern