# TTP Detail – T1213

## TTP Information

Name: Data from Information Repositories

Description: Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, such as Credential Access, Lateral Movement, or Defense Evasion, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization (i.e., [Transfer Data to Cloud Account](https://attack.mitre.org/techniques/T1537)).

The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository:

\* Policies, procedures, and standards
\* Physical / logical network diagrams
\* System architecture diagrams
\* Technical system documentation
\* Testing / development credentials (i.e., [Unsecured Credentials](https://attack.mitre.org/techniques/T1552))
\* Work / project schedules
\* Source code snippets
\* Links to network shares and other internal resources
\* Contact or other sensitive information about business partners and customers, including personally identifiable information (PII)

Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include the following:

\* Storage services such as IaaS databases, enterprise databases, and more specialized platforms such as customer relationship management (CRM) databases
\* Collaboration platforms such as SharePoint, Confluence, and code repositories
\* Messaging platforms such as Slack and Microsoft Teams

In some cases, information repositories have been improperly secured, typically by unintentionally allowing for overly-broad access by all users or even public access to unauthenticated users. This is particularly common with cloud-native or cloud-hosted services, such as AWS Relational Database Service (RDS), Redis, or ElasticSearch.(Citation: Mitiga)(Citation: TrendMicro Exposed Redis 2020)(Citation: Cybernews Reuters Leak 2022)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* MgBot
* P.A.S. Webshell
* Raccoon Stealer
* Troll Stealer

## APTs (Intrusion Sets)

* APT28
* FIN6
* Sandworm Team
* Sea Turtle
* Turla