# TTP Detail – T1119

## TTP Information

Name: Automated Collection

Description: Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals.   
  
In cloud-based environments, adversaries may also use cloud APIs, data pipelines, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data.(Citation: Mandiant UNC3944 SMS Phishing 2023)   
  
This functionality could also be built into remote access tools.   
  
This technique may incorporate use of other techniques such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) and [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570) to identify and move files, as well as [Cloud Service Dashboard](https://attack.mitre.org/techniques/T1538) and [Cloud Storage Object Discovery](https://attack.mitre.org/techniques/T1619) to identify resources in cloud environments.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* AppleSeed
* Attor
* BADNEWS
* Bankshot
* Comnie
* Crutch
* DarkGate
* FunnyDream
* GoldFinder
* Helminth
* InvisiMole
* LightNeuron
* LoFiSe
* Lumma Stealer
* MESSAGETAP
* Metamorfo
* Micropsia
* NETWIRE
* OutSteel
* PACEMAKER
* PoetRAT
* Proxysvc
* RTM
* Raccoon Stealer
* Ramsay
* RotaJakiro
* Rover
* StrelaStealer
* StrongPity
* T9000
* TajMahal
* USBStealer
* VERMIN
* Valak
* WindTail
* Zebrocy
* ccf32

## Tools

* Empire
* Mythic
* NPPSPY
* Pacu
* PoshC2
* ROADTools
* ShimRatReporter

## APTs (Intrusion Sets)

* APT1
* APT28
* Agrius
* Chimera
* Confucius
* Ember Bear
* FIN5
* FIN6
* Gamaredon Group
* HAFNIUM
* Ke3chang
* Mustang Panda
* OilRig
* Patchwork
* RedCurl
* Sidewinder
* Threat Group-3390
* Tropic Trooper
* Winter Vivern
* menuPass