# TTP Detail – T1020

## TTP Information

Name: Automated Exfiltration

Description: Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.(Citation: ESET Gamaredon June 2020)

When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: exfiltration

## Malware

* Attor
* CosmicDuke
* Crutch
* Doki
* Ebury
* Hannotog
* LightNeuron
* Machete
* OutSteel
* Peppy
* Raccoon Stealer
* Rover
* Solar
* StrelaStealer
* StrongPity
* TINYTYPHON
* TajMahal
* USBStealer

## Tools

* Empire
* ShimRatReporter

## APTs (Intrusion Sets)

* Gamaredon Group
* Ke3chang
* RedCurl
* Sidewinder
* Tropic Trooper
* Winter Vivern