# TTP Detail – T1056.001

## TTP Information

Name: Keylogging

Description: Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. In order to increase the likelihood of capturing credentials quickly, an adversary may also perform actions such as clearing browser cookies to force users to reauthenticate to systems.(Citation: Talos Kimsuky Nov 2021)

Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes.(Citation: Adventures of a Keystroke) Some methods include:

\* Hooking API callbacks used for processing keystrokes. Unlike [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004), this focuses solely on API functions intended for processing keystroke data.
\* Reading raw keystroke data from the hardware buffer.
\* Windows Registry modifications.
\* Custom drivers.
\* [Modify System Image](https://attack.mitre.org/techniques/T1601) may provide adversaries with hooks into the operating system of network devices to read raw keystrokes for login sessions.(Citation: Cisco Blog Legacy Device Attacks)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: collection

**•** mitre-attack: credential-access

## Malware

* ADVSTORESHELL
* Agent Tesla
* AppleSeed
* Astaroth
* Attor
* BADNEWS
* BISCUIT
* BabyShark
* BadPatch
* Bandook
* BlackEnergy
* CHIMNEYSWEEP
* CHOPSTICK
* Cadelspy
* Carbanak
* Cardinal RAT
* Catchamas
* Clambling
* Cobalt Strike
* Cobian RAT
* CosmicDuke
* Crimson
* Cuba
* DOGCALL
* DUSTTRAP
* DarkComet
* DarkGate
* DarkTortilla
* DarkWatchman
* Daserf
* Derusbi
* Dtrack
* Duqu
* DustySky
* ECCENTRICBANDWAGON
* EvilGrab
* Explosive
* FakeM
* FlawedAmmyy
* FunnyDream
* Fysbis
* Grandoreiro
* GreyEnergy
* HTTPBrowser
* Helminth
* InvisiMole
* JPIN
* KGH\_SPY
* KONNI
* Kasidet
* KeyBoy
* Kivars
* Lokibot
* MacMa
* MacSpy
* Machete
* MarkiRAT
* Matryoshka
* Metamorfo
* MgBot
* Micropsia
* Mispadu
* MoonWind
* NETWIRE
* NanoCore
* NavRAT
* NetTraveler
* NightClub
* Okrum
* OwaAuth
* Peppy
* PlugX
* PoetRAT
* PoisonIvy
* PowerLess
* Prikormka
* Proton
* QakBot
* RCSession
* ROKRAT
* RTM
* Regin
* Remexi
* Remsec
* Revenge RAT
* Rover
* RunningRAT
* SLOTHFULMEDIA
* SMOKEDHAM
* SslMM
* Sykipot
* TajMahal
* ThiefQuest
* TinyZBot
* Trojan.Karagany
* Unknown Logger
* VERMIN
* WarzoneRAT
* XAgentOSX
* XLoader
* Zeus Panda
* ZxShell
* gh0st RAT
* jRAT
* metaMain
* njRAT
* yty

## Tools

* AsyncRAT
* Empire
* Imminent Monitor
* PcShare
* PoshC2
* PowerSploit
* Pupy
* QuasarRAT
* Remcos
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT28
* APT3
* APT32
* APT38
* APT39
* APT41
* APT42
* APT5
* Ajax Security Team
* Darkhotel
* FIN13
* FIN4
* Group5
* HEXANE
* Ke3chang
* Kimsuky
* Lazarus Group
* Magic Hound
* OilRig
* PLATINUM
* Sandworm Team
* Sowbug
* Threat Group-3390
* Tonto Team
* Volt Typhoon
* menuPass