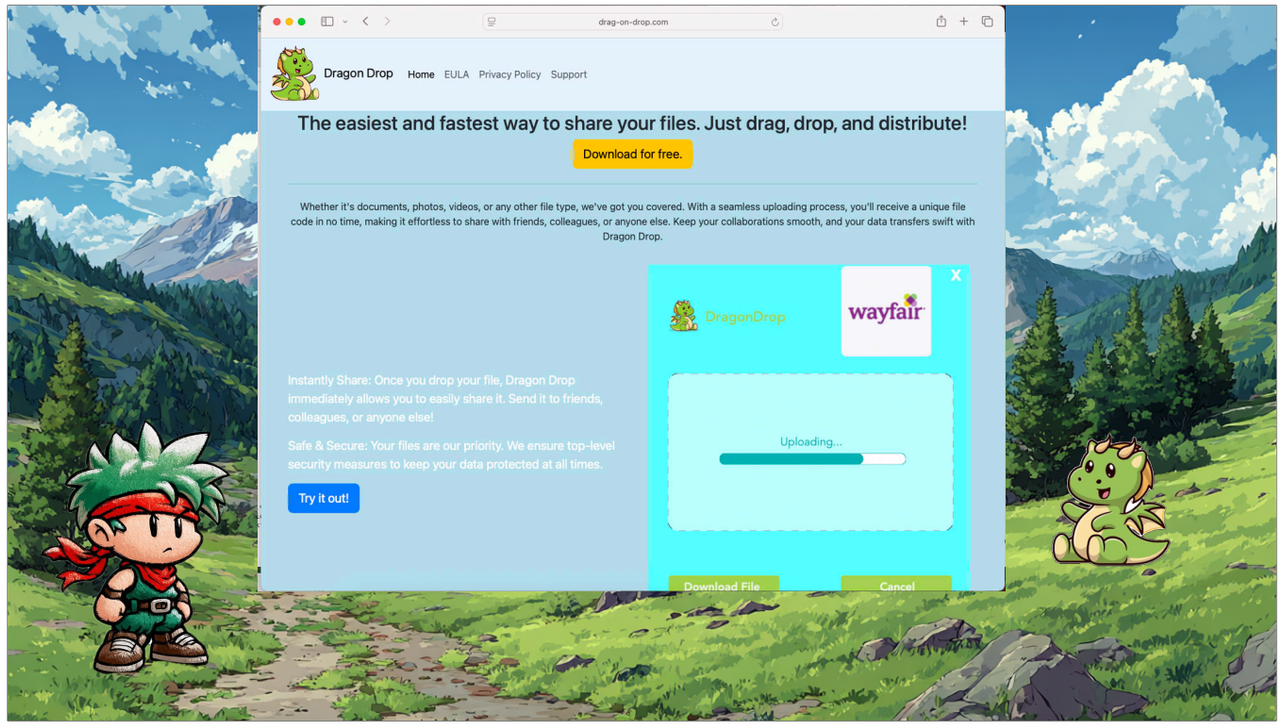
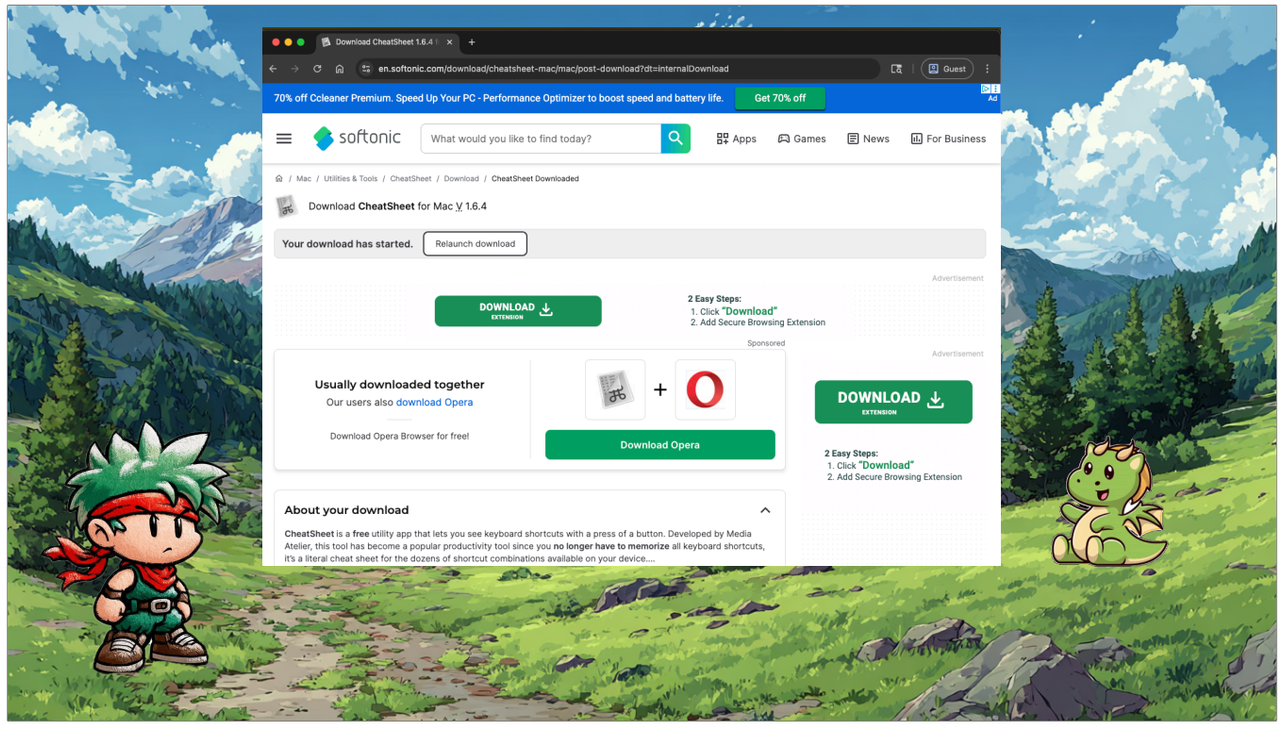

Gotta Catch Them All
Real Encounters with Threat Actors



Dragon drop, an interesting application where if downloaded from drag-on-drop.com does absolutely nothing besides for take your files. It pretends to host it in a location you can share with your friends. But in reality does nothing.



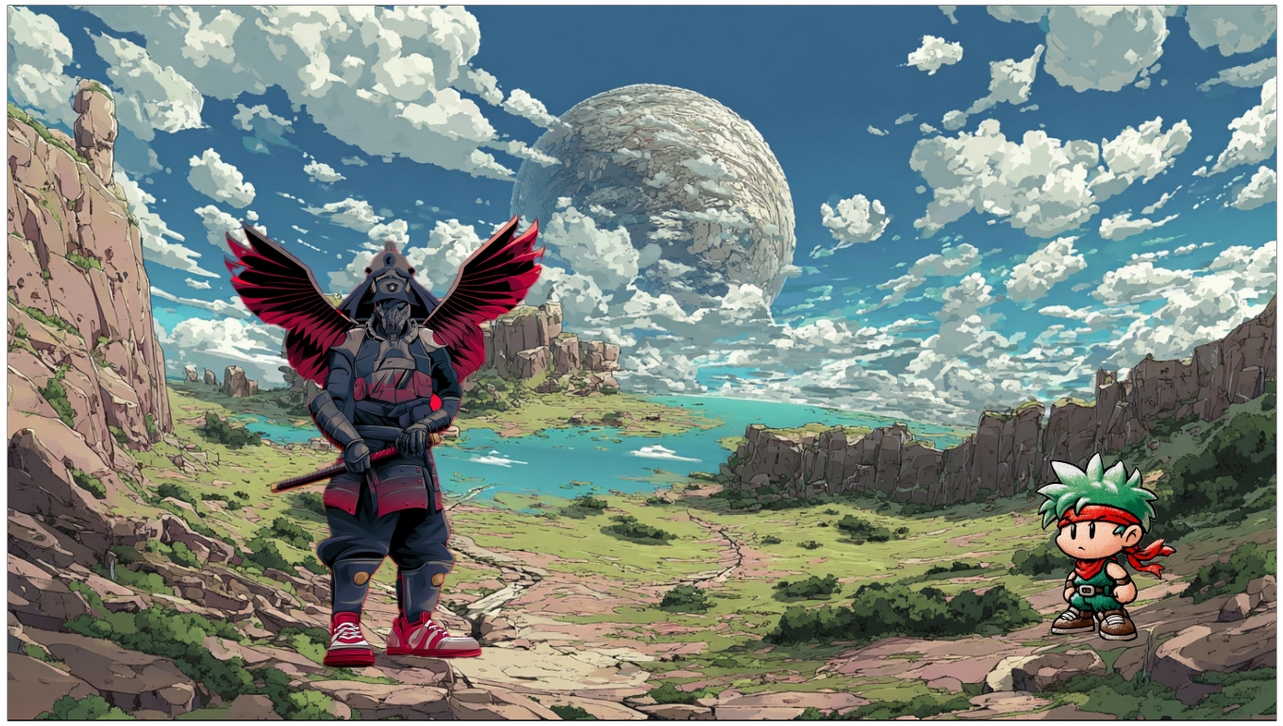
- We discovered a different version of the app called dragon drop.app that was also embedded inside of shareware programs hosted on softonic



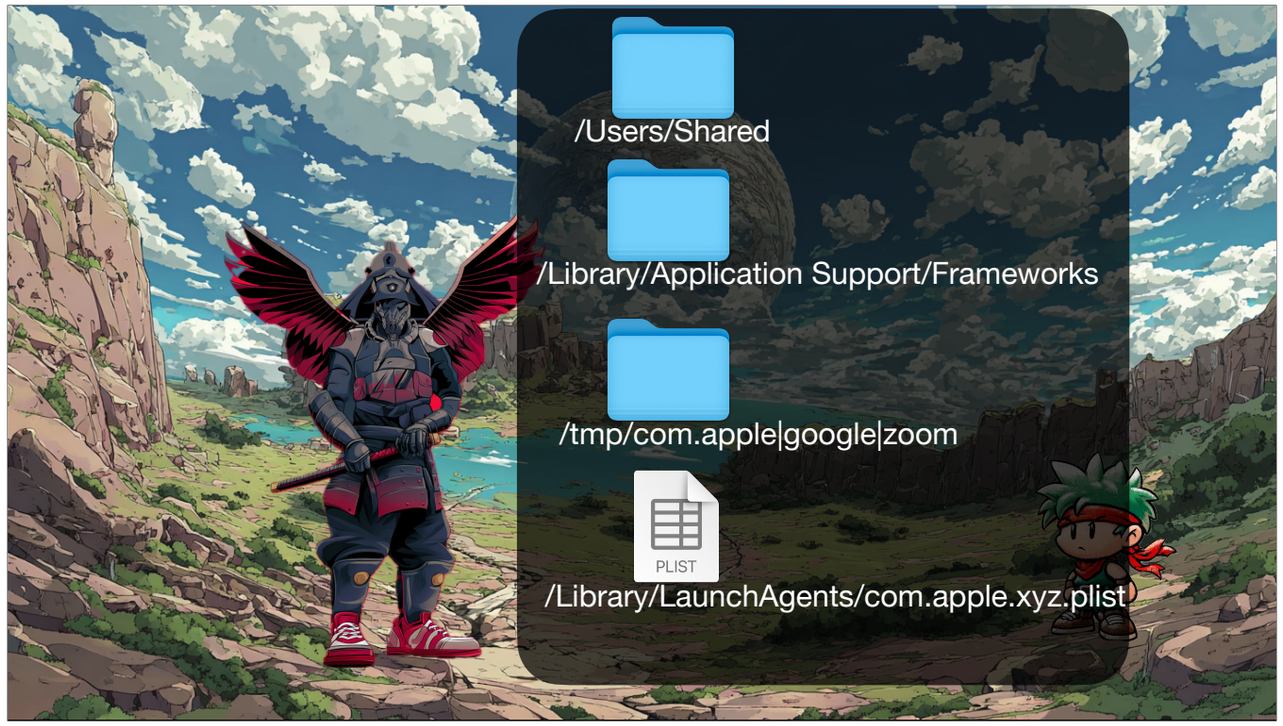
- After installing a signed open source app called AppPolice in the background, it would remove itself and install an ad-hoc signed executable instead. This seemed like it was setup to install avoid detection while gaining code execution.



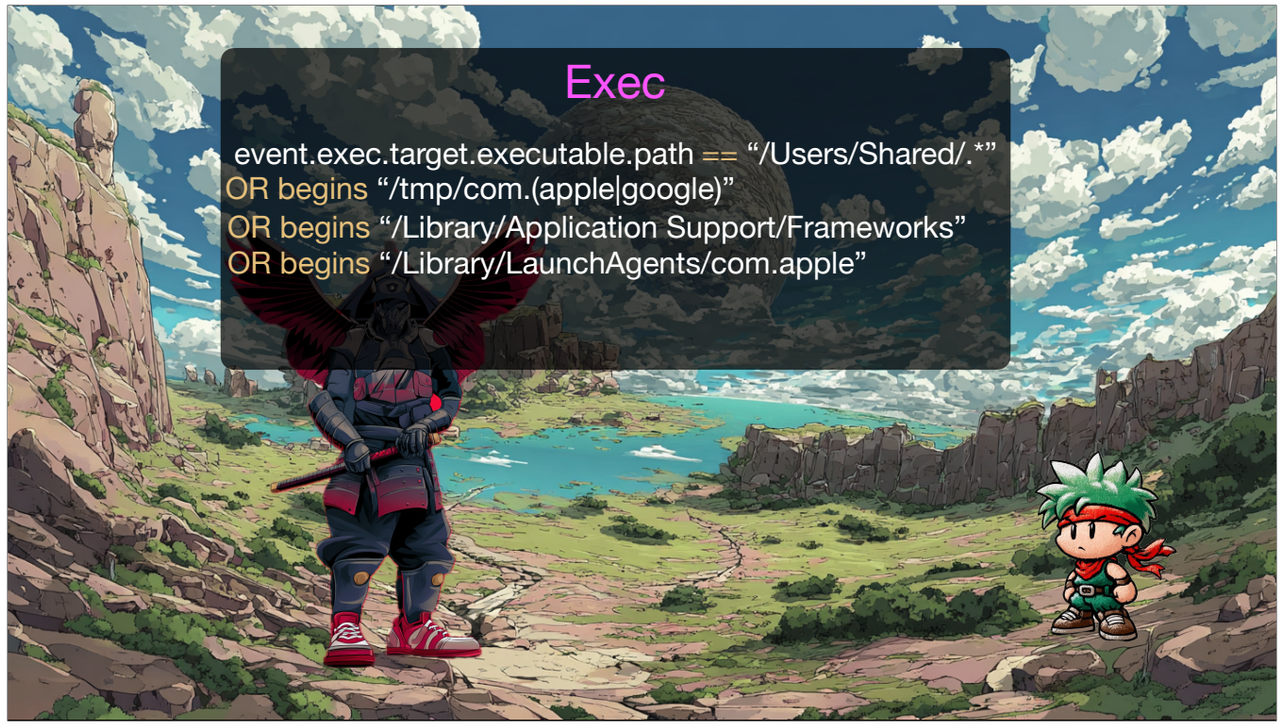
DragonDrop performs a self delete. This can be a good indicator that something suspicious is at play. However, this is best paired at a time where other detections are occurring on the system at the same time as self deleting is often performed by applications when updating and etc.



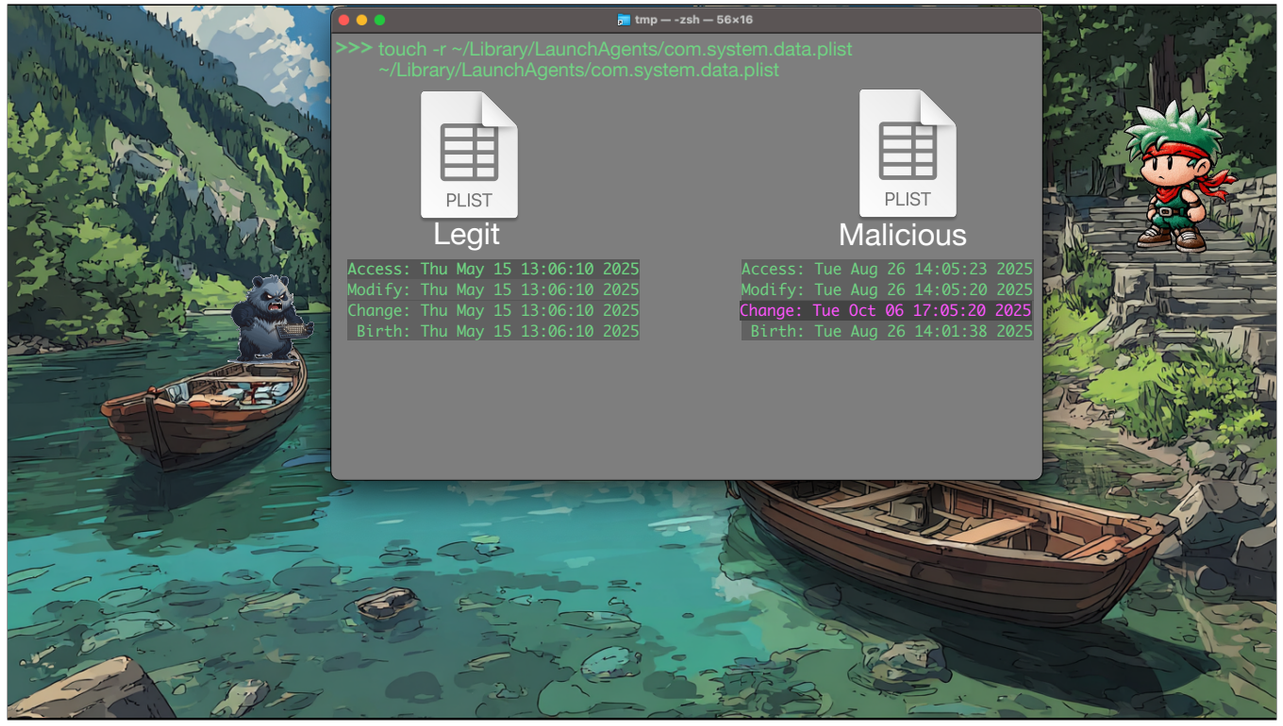
Lazarus group also known as the chollima as tracked by CrowdStrike is perhaps the most prolific APT threat actor on macOS.



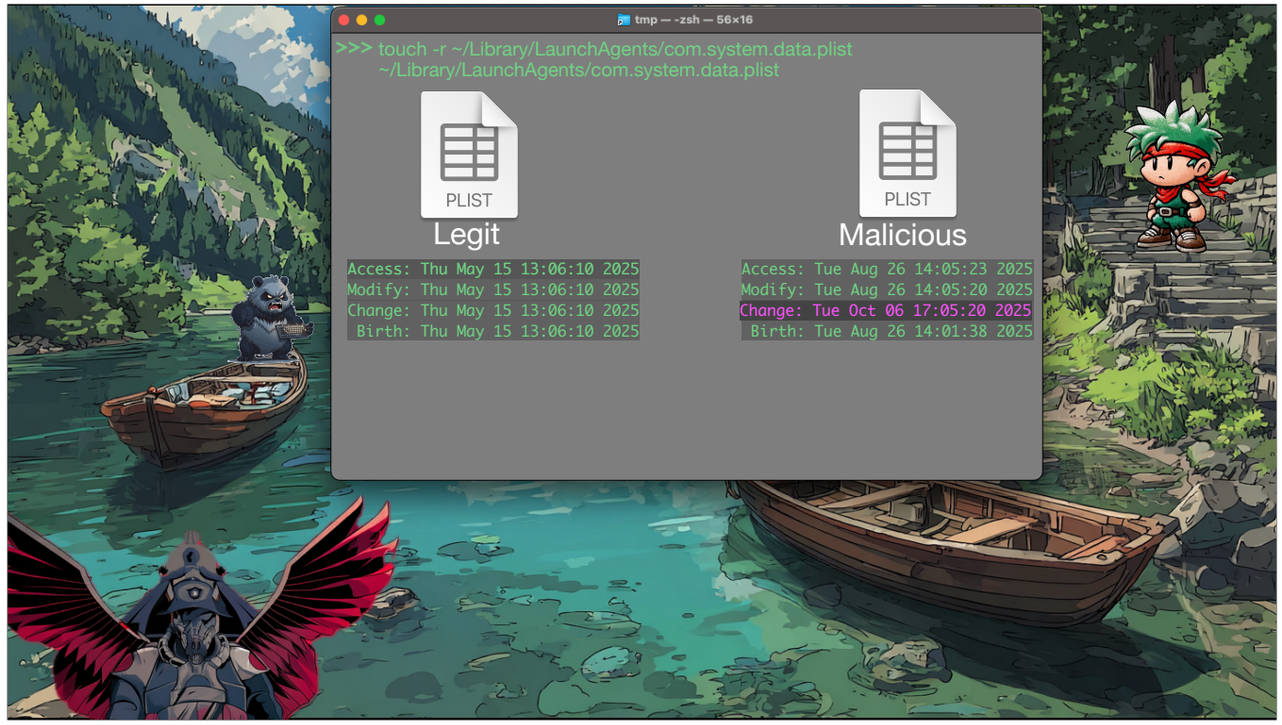
This threat actor often visits a lot of similar file names and folders in which they place their malware.



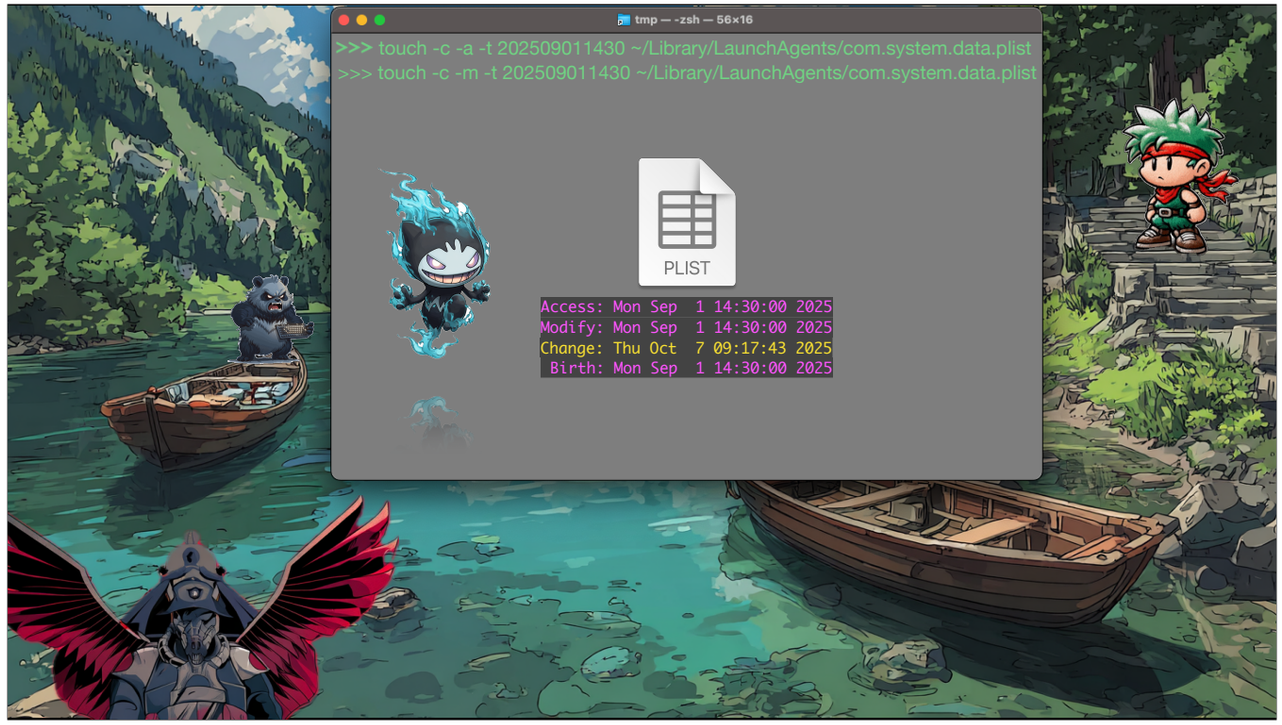
Look for execution of executables that run from these locations and have similar file naming schemes. Filtering down to unsigned executables can also help.



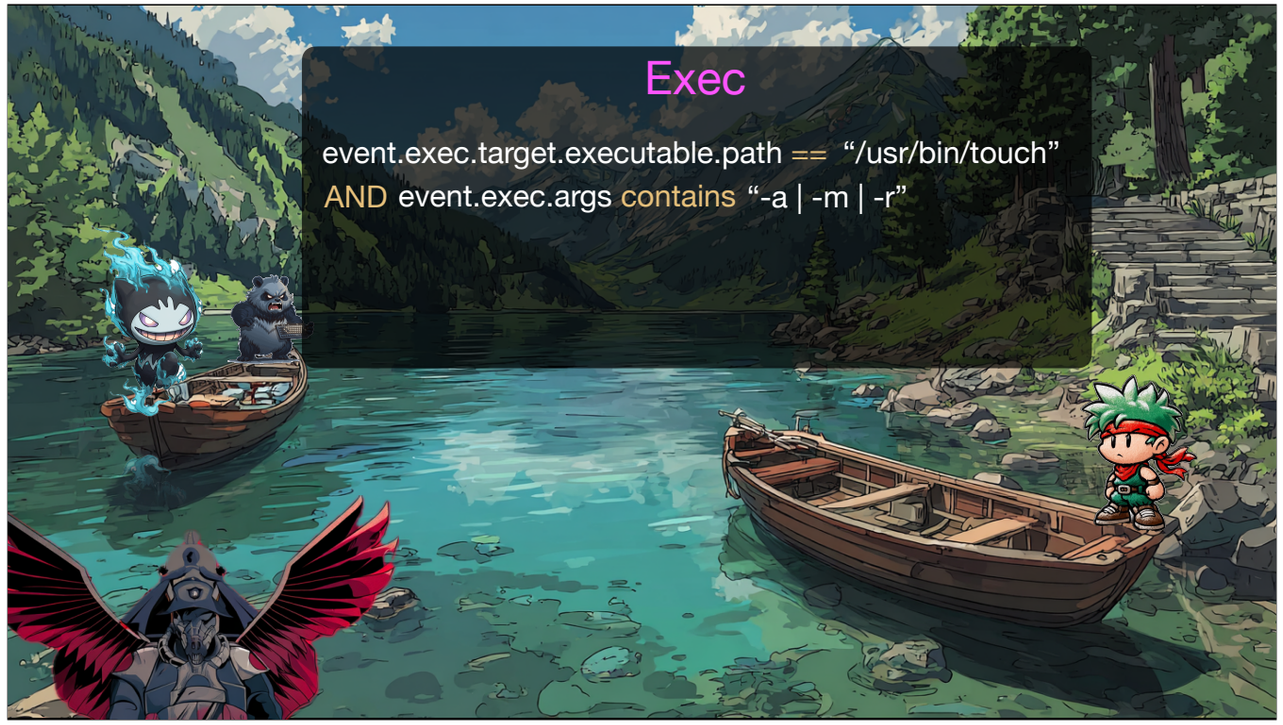
In an intrusion I was analyzed, I saw an attacker that used the touch command in order to take the timestamps of a legitimately installed launch agent and apply those timestamps to a maliciously installed timestamp. From the perspective of Access modify, change, and birth timestamp, this approach no only modifies the change timestamp to be the current time.



- The chollima has also been known to use this timestomping trick despite the fact that it doesn’t even achieve much anymore.



- The ChillyHell malware uses a proper time stomping technique with touch that actually does properly modify the timestamps



Looking for touch running with some of these arguments can be pretty rare. They can be good indicators that something strange has happened. Tune accordingly for your environment.



I once saw an intruder use the bonjour functionality from the command line to search for other ssh servers that were broadcasting on the network. A clever technique given bonjour is already broadcasting the fact that ssh is running on a computer. This saves the attacker the work of a noisy network scan.



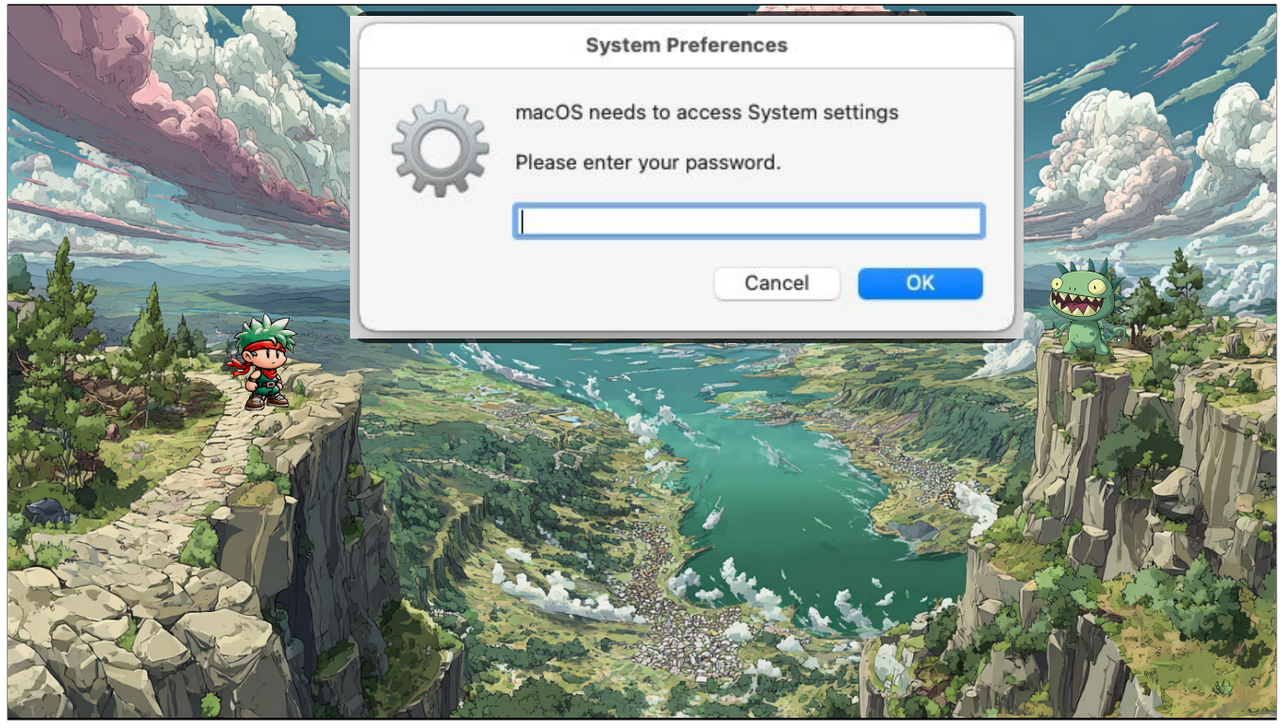
I once saw an attacker make many mistakes with netcat, treating it as though it was the linux netcat listener.



Look for all dns-sd activity and tune for your environment. It’s not an overly noisy command. Also monitor for times where netcat is executed with -e or —exec switches as this implies someone is attempting to achieve execution of a payload over netcat in a way that doesn’t work. Legitimate software wouldn’t do this making it a low FP detection (though perhaps a high red team detection)

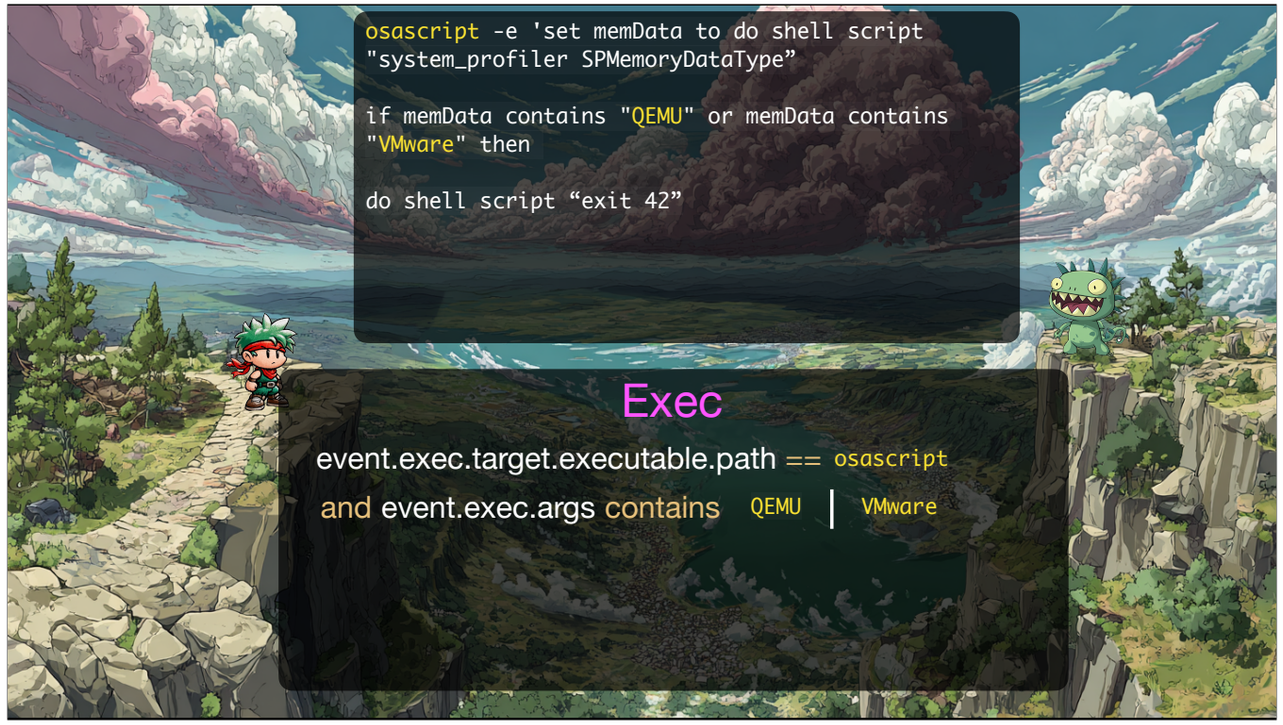


Infostealers are explosive right now and have been the past few years. They highly frequently prompt the user via AppleScript to enter their password using a command that looks like this.


System Preferences
macOS needs to access System settings
Please enter your password.
Cancel
OK



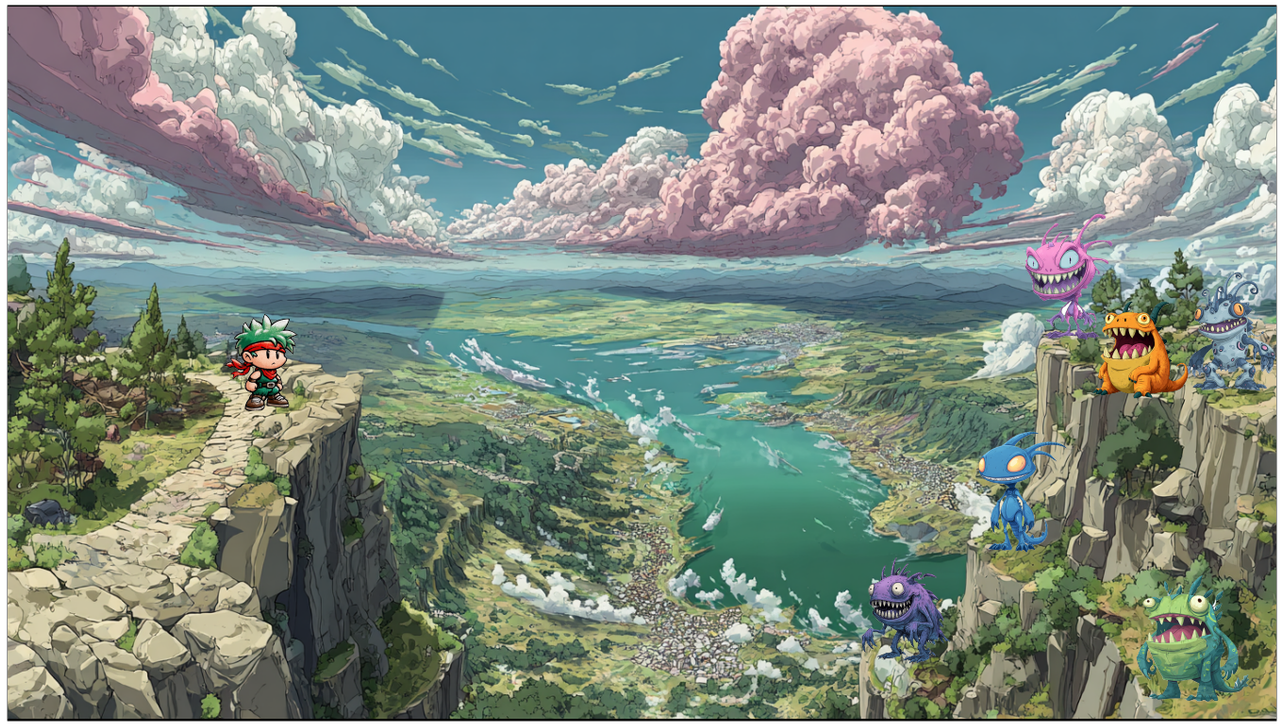
Look for when AppleScript runs with various words that could mean a password is being prompted for. This may lead to high FP’s depending on what scripts your admins are running.



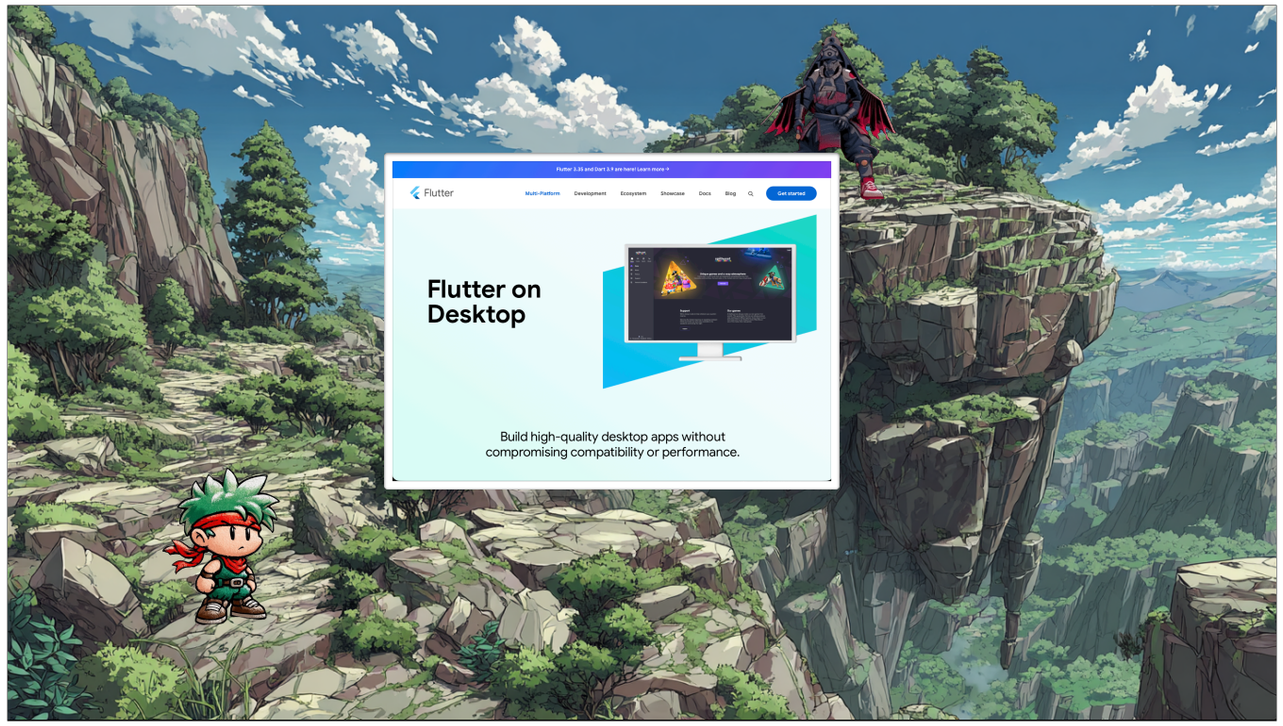
Infostealers have also started heavily implementing anti-vm checks in AppleScript. You can look for these pretty easily with a low FP ratio



Dscl is frequently used by info stealers to verify if the password that was entered by the user was entered correctly.



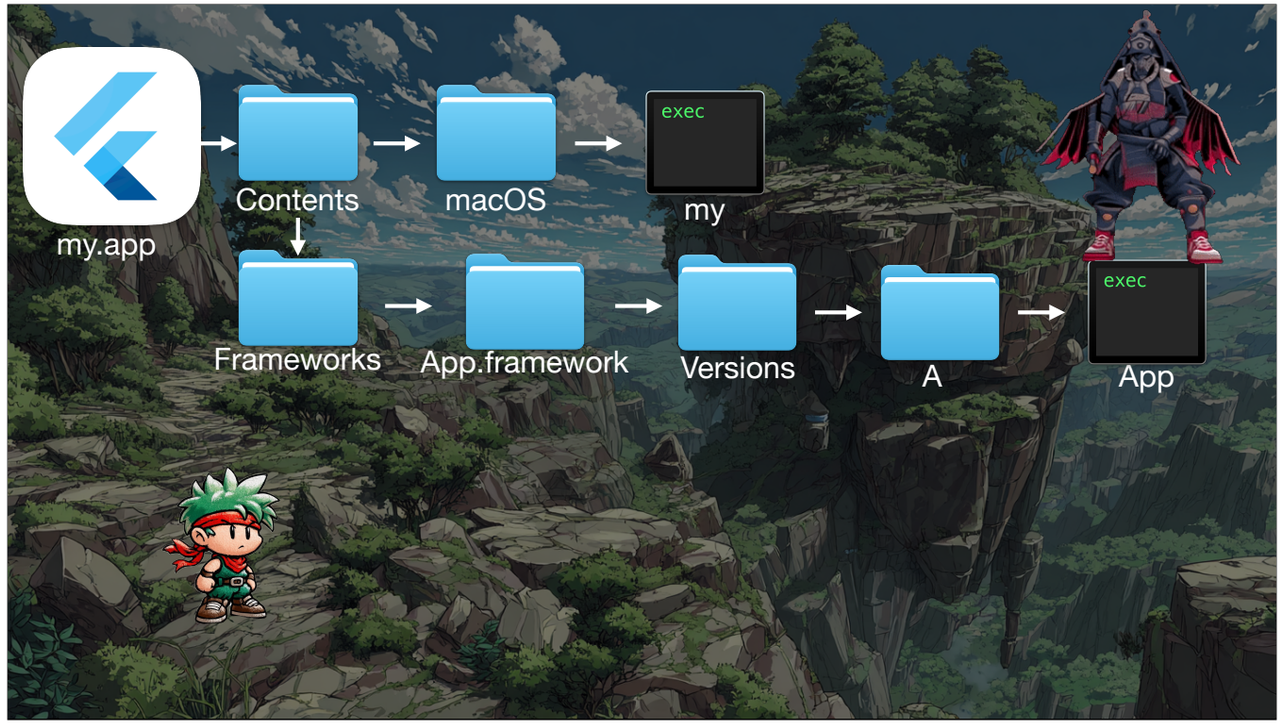
- After you detect one info stealer the problem is, a many more seem to pop up within the next week.



We have seen the chollima testing building apps for macOS using the cross-platform flutter framework.



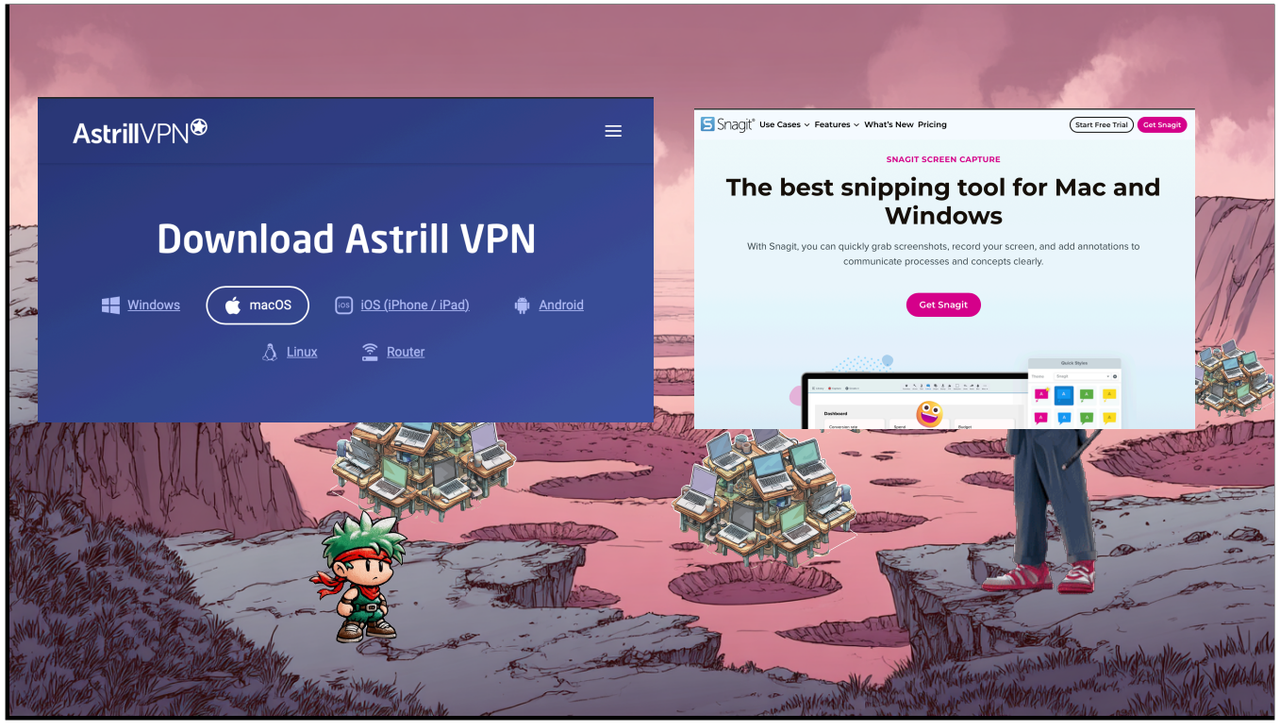
We saw them testing this by embedding a backdoor that Jamf tracks as thiefbucket directly into a open source minesweeper flutter based application



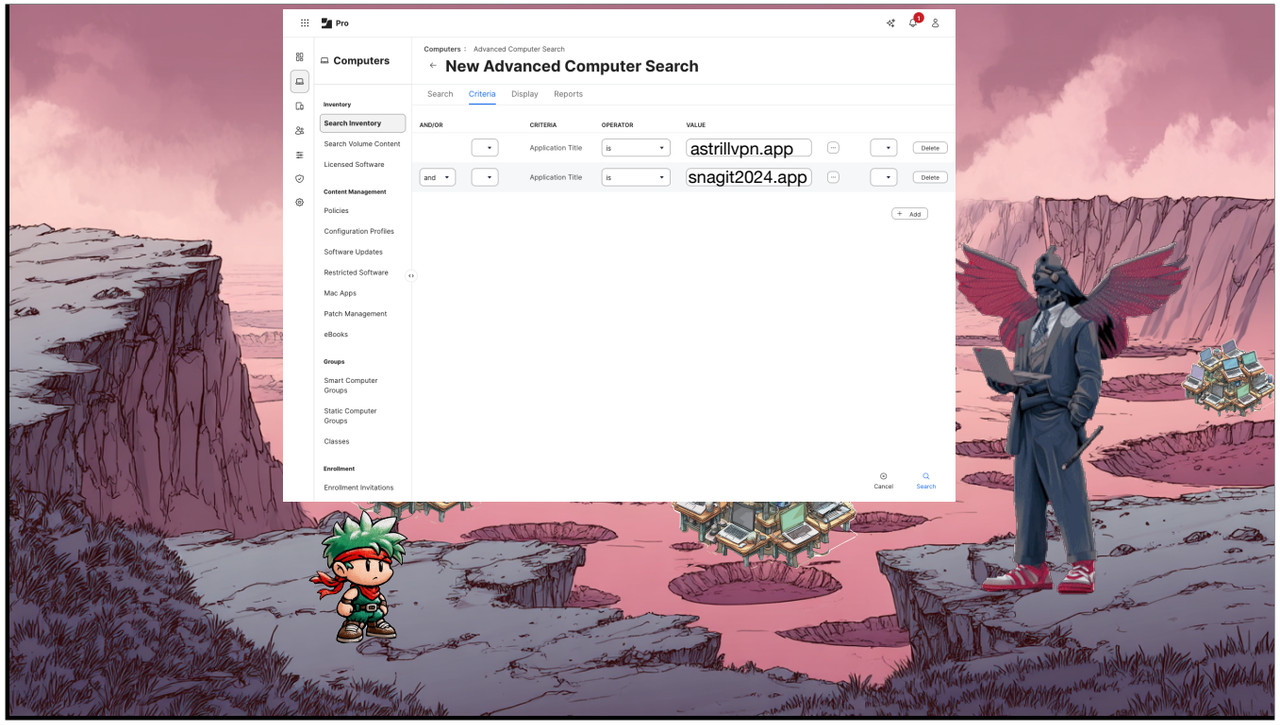
- When taking this approach the malicious code ends up being compiled into a dylib that flutter loads separate from the main application binary
- Discussing detections on this would require an entirely separate talk



- Many have heard of the laptop farms set up by Shadow IT worker campaigns. Many different pieces of software are used to login to these laptop farms.



Using legitimate tools makes this attacker harder to track.
Astrill VPN is used by the attacker and legitimate tooling such as snagit2024 is used to take screenshots.



You don’t even need a SIEM to do this kind of investigation. Use mdm to search your fleets for combinations of this software running. Identify computers running them and continue investigation from there.



For those looking to learn more about Threat Hunting macOS as well as read more stories about attackers, you can order my book

https://themittenmac.com/threat-hunting-book/