Green Lambert and ATT&CK — Glitch-Cat

By Oct 18 Written By Runa Sandvik

Published: 2001-10-18 · Archived: 2026-04-06 01:19:25 UTC

On October 1, I gave a talk at Objective By The Sea about a CIA implant called Green Lambert. The recording is available on YouTube and the written post on Objective-See's blog. Inspired by a talk Adam Pennington and Cat Self gave about ATT&CK for macOS, I decided to map Green Lambert to that framework.

MITRE ATT&CK

The MITRE ATT&CK framework is a great way to document adversary tactics and techniques based on real-world observations. In writing this blog post, I also found that it's a helpful way to identify what you know and don't know about an adversary and/or a piece of malware. If you haven't used ATT&CK before, check out the resources from CISA and MITRE.

Initial Access

The first tactic in the matrix is Initial Access, which consists of techniques used to gain entry to a system. As I wrote in the post for Objective-See, "we don't know how this implant makes it onto a target system; the type of system it's used on; or the geographical location of a typical target." For that reason, we'll leave this blank.

Execution

The next tactic, Execution, focuses on techniques used to run the implant on the target system. Comparing MITRE's list with my post on Objective-See, we find that Green Lambert can:

- Use shell scripts for execution (Command and Scripting Interpreter: Unix Shell [T1059.004])
- Use `Launchd` for initial and recurring execution (Scheduled Task/Job: Launchd [T1053.004])

Persistence

Persistence is all about retaining access to the system across restarts, changed credentials, and other interruptions. If we look at the section about Entry Points in the Objective-See post, we find that Green Lambert can:

- Persist via a `LoginItem` (Boot or Logon Autostart Execution: Plist Modification [T1547.011])
- Persist via RC scripts (Boot or Logon Initialization Scripts: RC Scripts [T1037.004])
- Persist via `LaunchAgent` (Create or Modify System Process: Launch Agent [T1543.001])
- Persist via `LaunchDaemon` (Create or Modify System Process: Launch Daemon [T1543.004])

- Persist via shells (Event Triggered Execution: Unix Shell Configuration Modification [T1546.004])
- Use `Launchd` for initial and recurring execution (Scheduled Task/Job: Launchd [T1053.004])

Privilege Escalation

We have not seen Green Lambert gain elevated access, so we'll leave Privilege Escalation blank.

Defense Evasion

The Defense Evasion tactic looks at how an adversary avoids detection. In this case, that means:

- Use of custom routines to decrypt strings (Deobfuscate/Decode Files or Information [T1140])
- Ability to self-delete once installed (Indicator Removal on Host: File Deletion [T1070.004])
- Masquerade as `GrowlHelper` (Masquerading: Masquerade Task or Service [T1036.004])
- And as `Software Update Check` (Masquerading: Masquerade Task or Service [T1036.004])
- Decrypt strings in-memory, per CIA guidelines (Obfuscated Files or Information [T1027])

Credential Access

Credential Access looks at techniques used to steal credentials, such as account names and passwords. During initial triage of Green Lambert, we found a string that (at least) suggests the following technique.

- Use of `SecKeychainFindInternet…` (Credentials from Password Stores: Keychain [T1555.001])

Discovery

For Discovery, we'll look for ways that Green Lambert gains knowledge about the system. We don't have a lot of information to go on, just a few clues from our initial triage and what appears to be a configuration file and/or system survey. Green Lambert can:

- Determine the Linux version and system uptime (System Information Discovery [T1082])
- Determine proxy settings (System Network Configuration Discovery [T1016])
- Determine the current date and time (System Time Discovery [T1124])

Lateral Movement

We have not seen Green Lambert access remote systems, so we'll leave Lateral Movement blank.

Collection

We don't know how Green Lambert treats collected data, so we'll leave Collection blank.

Command and Control

Command and Control consists of techniques used for communication. Green Lambert can:

- Make a DNS request (Application Layer Protocol: DNS [T1071.004])
- Communicate with hostname and IP address (Fallback Channels [T1008])
- Use a proxy for communications (Proxy [T1090])

Exfiltration

We don't know how Green Lambert steals data from the system, so we'll leave Exfiltration blank.

Impact

We don't have any data to suggest Green Lambert destroys the target, so we'll leave Impact blank.

Let's visualize it!

Plugging (almost all) the information gathered into the ATT&CK Navigator, we get this visualization.

Conclusion

That's it! (I think. Please let me know if I've missed anything.) As the visualization above shows, there's a lot more to dig into here. For example, you can use @osxreverser's Delambert plugin to decrypt more strings. Or you can take a closer look at command line arguments. Or how the Green Lambert generates the victim ID. Or what the implant collects and how it exfiltrates data.

Happy hunting!
