Green Lambert and ATT&CK

Runa Sandvik
Oct 18, 2021

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

Glitch-Cat

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

- Use of custom routines to dec [T1140])
- Ability to self-delete once inst])
- Masquerade as `GrowlHelpe`])
- And as `Software Update` [T1036.004])
- Decrypt strings in-memory, p])

Credential Access

Credential Access looks at techniq passwords. During initial triage of e 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:

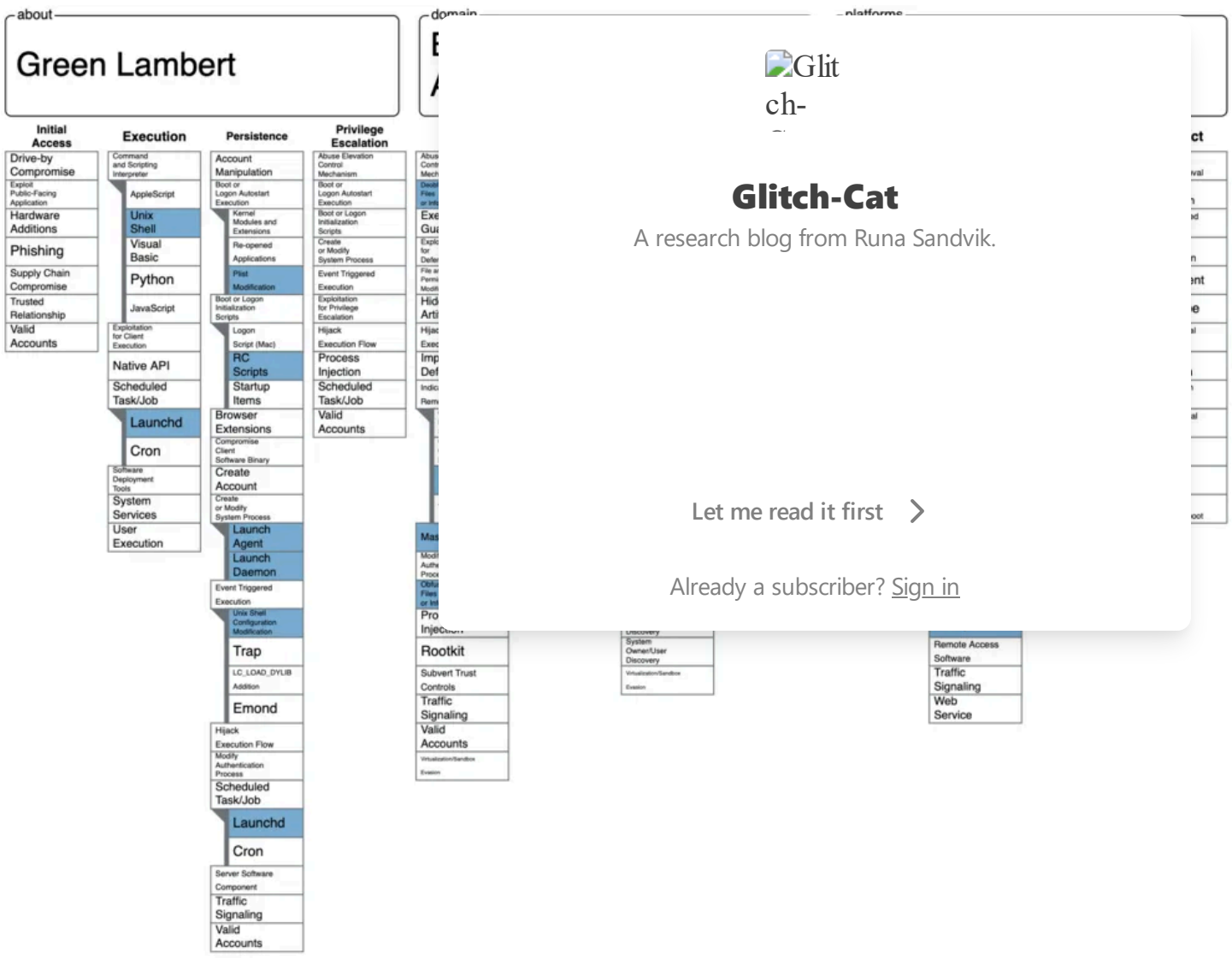
- Determine the Linux version and system uptime (System Information Discovery [T1082])
- Determine proxy settings (System Network Configuration Discovery [T1016])
- Determine the current date and time (System Time Discovery [T1124])

Lateral Movement

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

Glitch-Cat

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!

Glitch-Cat

Failed to load posts