Glitch-Cat

Subscribe Sign in

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

- Use `Launchd` for initial and recurring execution (Scheduled Task/Job: Launchd [T1053.004])

Persistence

Persistence is all about retaining access to th
credentials, and other interruptions. If we lo
the Objective-See post, we find that Green La

- Persist via a `LoginItem` (Boot or Logon A
[T1547.011])
- Persist via RC scripts (Boot or Logon Ini
[T1037.004])

- Use of custom routines to decrypt strings (Deobfuscate/Decode Files or Information [T1140])
- Ability to self-delete once installed (Indi
[T1070.004])
- Masquerade as `GrowlHelper` (Masquerad
[T1036.004])
- And as `Software Update Check` (Masqu
[T1036.004])
- Decrypt strings in-memory, per CIA gui
[T1027])

Glitch-Cat

- Determine the current date and time (System Time Discovery [T1124])

Lateral Movement

We have not seen Green Lambert access rem
Movement blank.

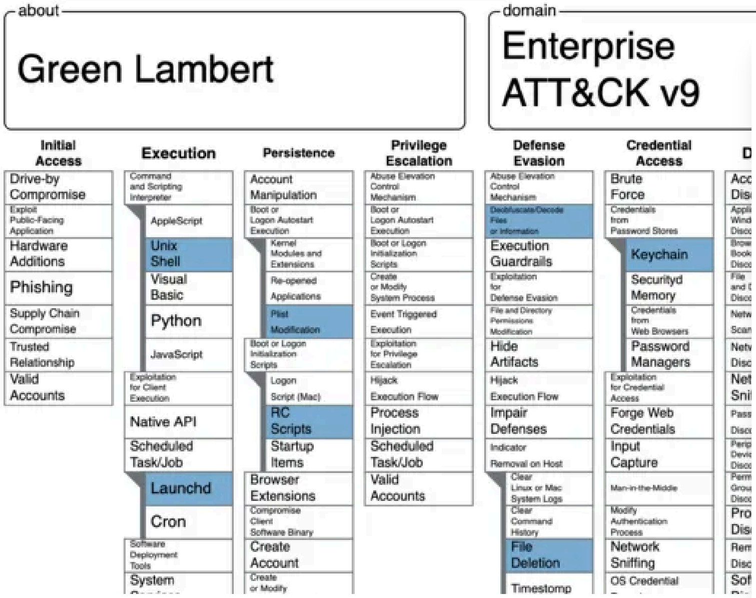
Collection

We don't know how Green Lambert treats co
blank.

Command and Control

Glitch-Cat

this visualization.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force
Exploit Public-Facing Application	AppleScript	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Deobfuscate/Decode Files or Information	Credentials from Password Stores
Hardware Additions	Unix Shell	Kernel Modules and Extensions	Boot or Logon Initialization Scripts	Execution Guardrails	Keychain
Phishing	Visual Basic	Re-opened Applications	Create or Modify System Process	Exploitation for Defense Evasion	Securityd Memory
Supply Chain Compromise	Python	Plist Modification	Event Triggered Execution	File and Directory Permissions Modification	Credentials from Web Browsers
Trusted Relationship	JavaScript	Boot or Logon Initialization Scripts	Exploitation for Privilege Escalation	Hide Artifacts	Password Managers
Valid Accounts	Exploitation for Client Execution	Logon Script (Mac)	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Credential Access
	Native API	RC Scripts	Process Injection	Impair Defenses	Forge Web Credentials
	Scheduled Task/Job	Startup Items	Scheduled Task/Job	Indicator Removal on Host	Input Capture
	Launchd	Browser Extensions	Valid Accounts	Clear Linux or Mac System Logs	Man-in-the-Middle
	Cron	Compromise Client Software Binary		Clear Command History	Modify Authentication Process
	Software Deployment Tools	Create Account		File Deletion	Network Sniffing
	System	Create or Modify		Timestomp	OS Credential

Glitch-Cat

Happy hunting!

Subscribe to

By Runa Sandvik · Laur

A research blog fror

Type your email...

＋ Like this post

Gli
tch-

Glitch-Cat

A research blog from Runa Sandvik.

Let me read it first ›

Already a subscriber? Sign in

Glitch-Cat

Type your email... Subscribe

Gli
tch-

Glitch-Cat

A research blog from Runa Sandvik.

Let me read it first

Already a subscriber? Sign in