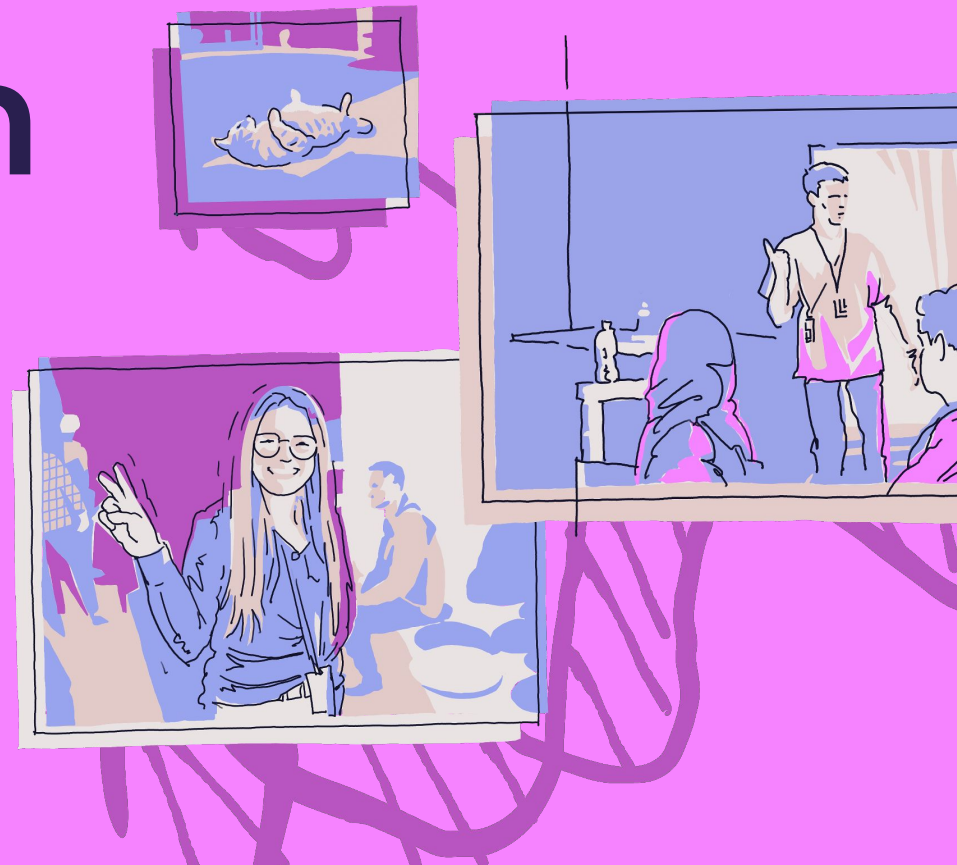
Catch me if you Scan

MITRE-enhanced ML Magic to Solve Mac Malware's Identity Crisis at Scale



We find malware before it finds you.



Kseniia Yamburh

Malware Research Engineer
at Moonlock by MacPaw

@osint_barbie



Nazar Grycshuk

Senior Data Scientist
at Moonlock by MacPaw

in/gryshchuk/

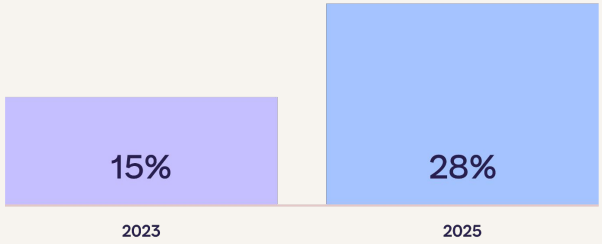
We'll have a job!

Figure	Statistics
Total Mac Users	100.4 Million
Global PC Market Share	15.1%
Annual Macintosh Revenue	$42.3 Billion
macOS Ventura Adoption	74.1%
U.S. Mac User Base	40.3%
Users Aged 18-34	55.7%
macOS U.S. Desktop Market Share	29.62%
Female Mac Users	66%

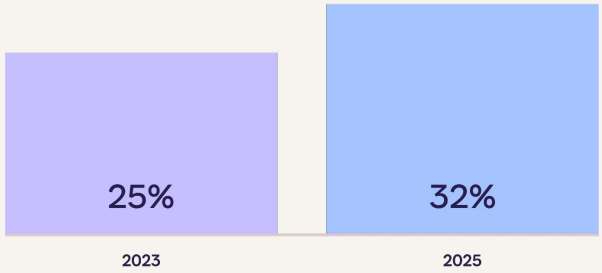


Mac users rethink their immunity to cyber threats but not enough

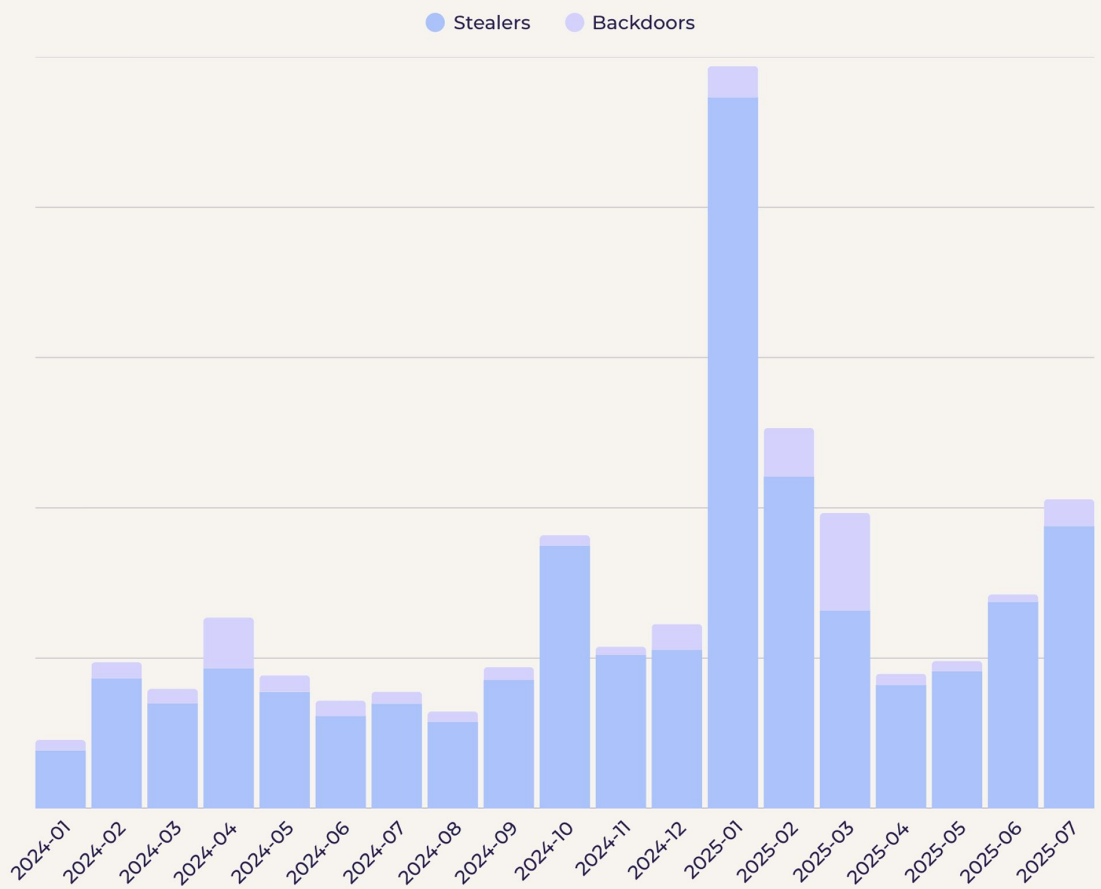
Since 2023, the share of Mac users who think that malware does not exist on macOS has dropped (15% vs. 28%)



Respondents are less confident that cybercriminals are not interested in their data (25% vs. 32%).



Spike in Detections in 2025

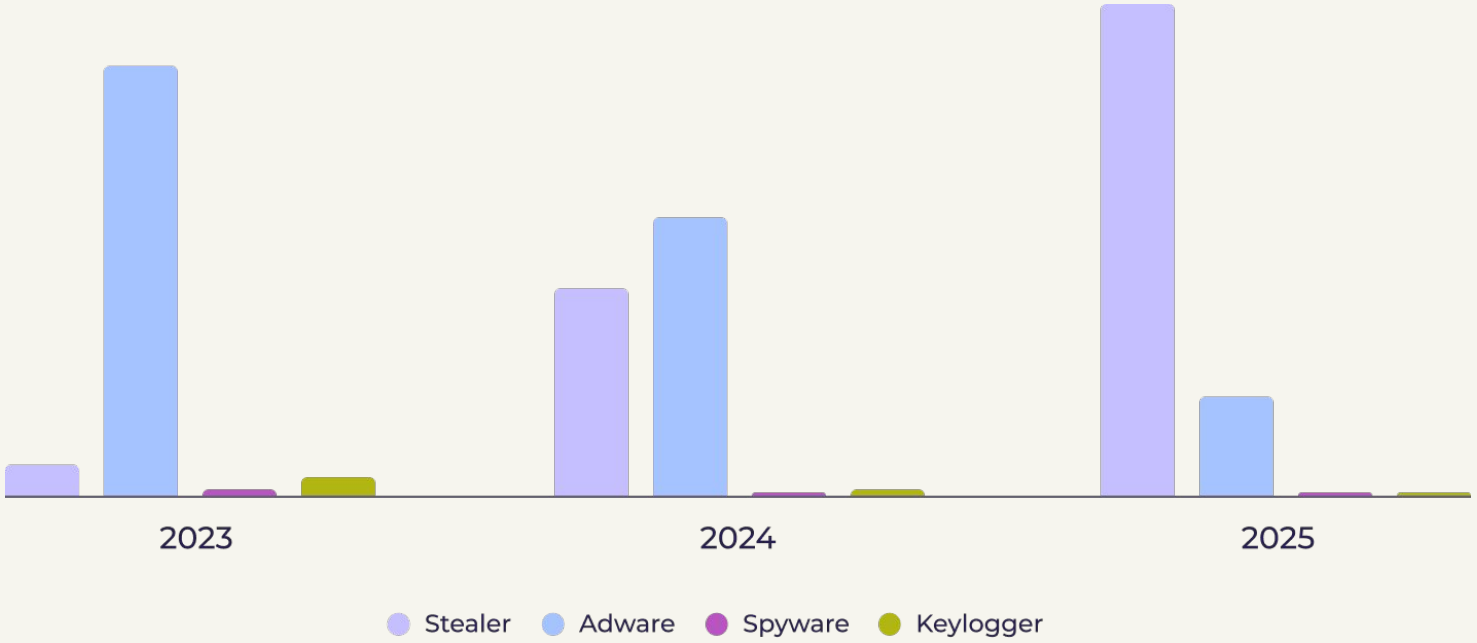


300%

Increase in detection rates since the first detected sample of AMOS with a backdoor feature

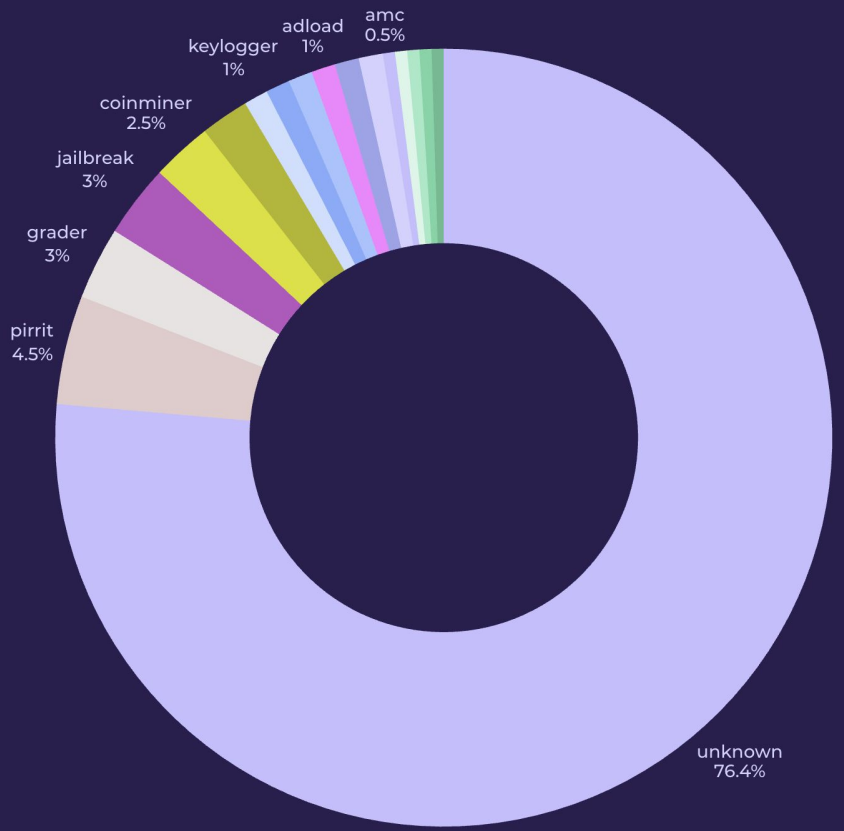


Major malware types are fusing into a broader — and more dangerous — category of modular stealers

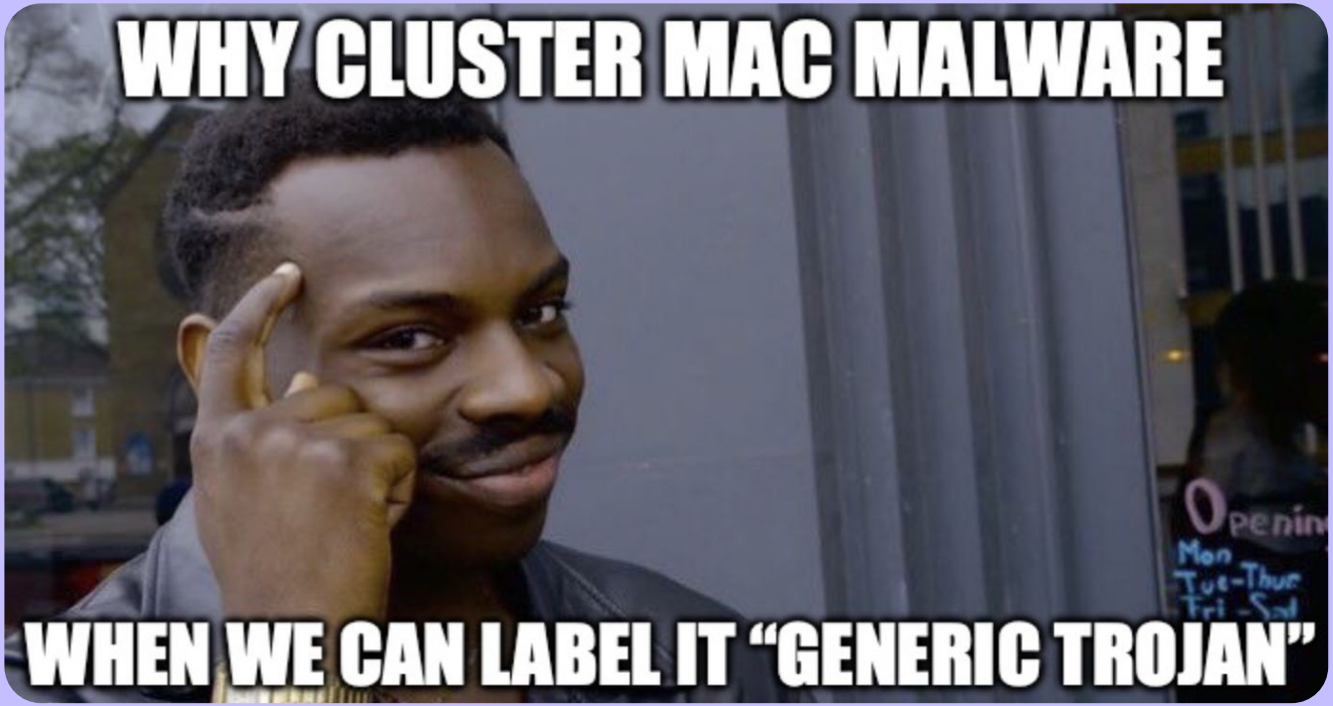


76,4%

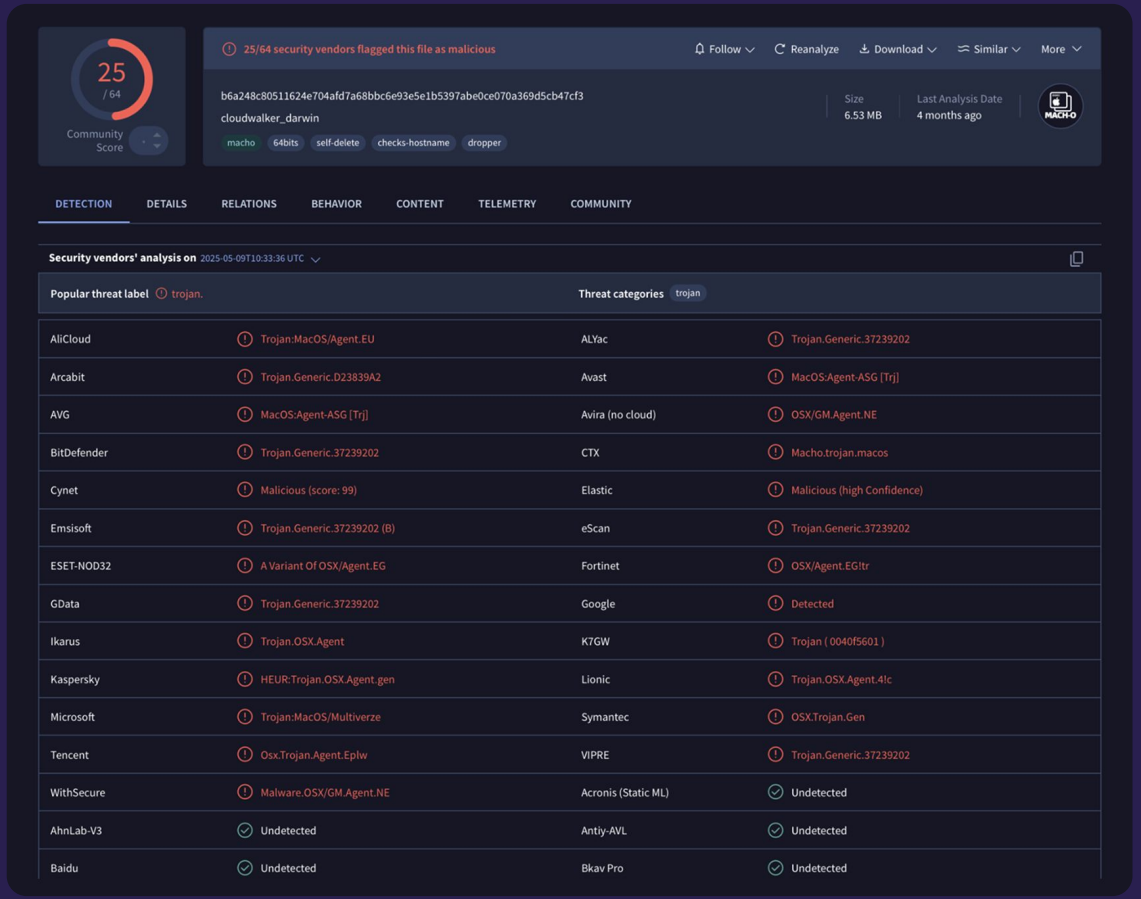
of unidentified
Mac malware



Rumour has it



Generic trojan that is actually a backdoor



TLS 1.3 Artifacts + WebSocket

```
TLS 1.3, server CertificateVerify
NoCertificateVerification
No "Connection: upgrade" header
No "Upgrade: websocket" header
No "Sec-WebSocket-Version: 13" header
MissingConnectionUpgradeHeaderMissingUpgradeWebSocketHeader
websocket read:
websocket send:
get_ws
```

Proxying / Tunneling



```
Proxy-Authorization: basic
Proxy-Authorization: basic  HTTP/1.1
Proxy-Connection: Keep-Alive
SOCKS proxy:  timed out connecting
```

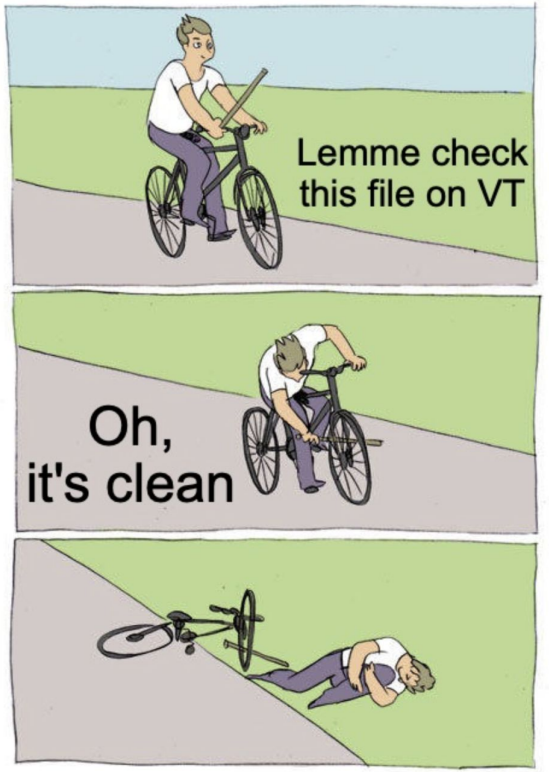
Key config parameters reveal backdoor traits

```
get_req
post_resp
DownloadArg
DownloadRemoteArg
CmdlineArg
PtyArg
ConfigureArg
CancelArg
LSArg
CDArg
CPArg
MVArg
RMArg
MKDirArg
CatArg
TouchArg
ProcessKillArg
NetstatArg
PathCompressArg
```

```
sleep_time
dead_time
wait_time
tls
proxy
virtual_procs
self_delete
server_pub
RequestConfig
SessionConfig
RequestCommon
```

😬

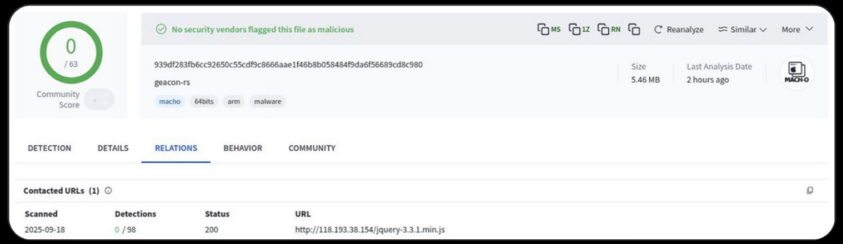
Could it be worse?



0-detect case

MalwareHunterTeam
@malwrhunterteam

FUD on VT, Mac Cobalt sample, "geacon-rs":
939df283fb6cc92650c55cdf9c8666aae1f46b8b058484f9da6f56689cd8c980
Guess the "rs" in the filename means Rust...
118.193.38[.]154
@1ZRR4H



Moonlock Ark

SHA256: 939df283fb6cc92650c55cdf9c8666aae1f46b8b058484f9da6f56689cd8c980

ml:macho_c:v1:backdoor

22/09/2025	macho_classification v1	-1	-1	backdoor

0-detect case

Moonlock Ark

SHA256: 8b3a13340d10f0370404eb5618a5ca2137a5bc9a0de7bd4a7fe45bf33f6b87ac

ml:macho_c:v1:backdoor

26/09/2025	macho_classification v1	-1	-1	backdoor

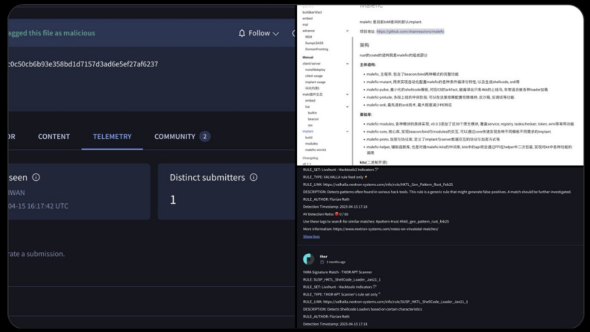
Nextron Research ⚡
@nextronresearch

This Malefic C2 implant was uploaded to VT from Taiwan in April:
virustotal.com/gui/file/23781...

Another variant (macOS) showed up from a US IP in May:
virustotal.com/gui/file/8b3a1...

- Detected by our generic YARA rules (THOR)
- 0/65 AV detections
- Uploaded as “java”
- Rust-based implant framework:
wiki.chainreactors.red/IoM/manual/imp...

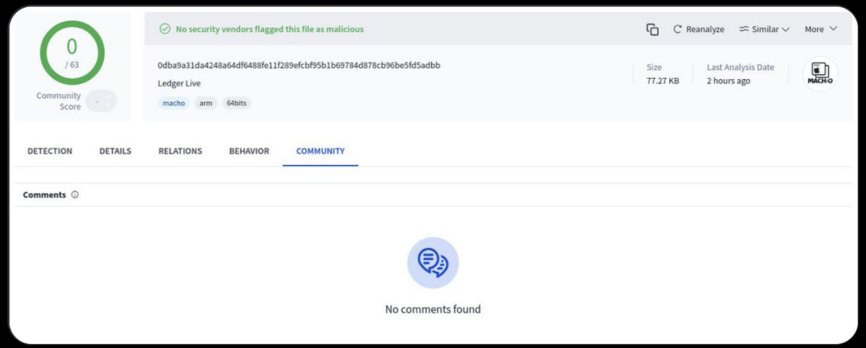
Could’ve been a real infection - not just someone playing around.
No detections, no noise. Just a quiet drop into the void.
Might be interesting for anyone watching cross-strait ops - or just into Rusty implants.

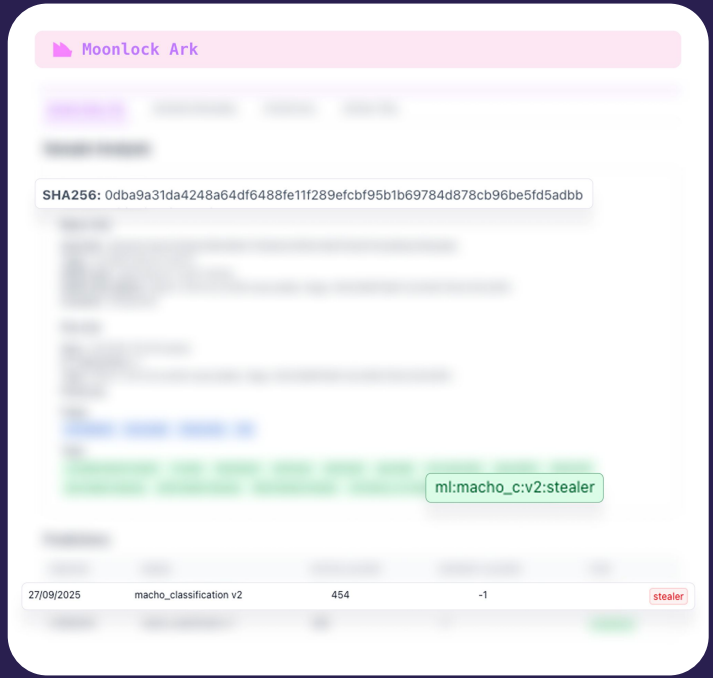


0-detect case

MalwareHunterTeam
@malwrhunterteam

Inside is this "Ledger Live" sample, that is also FUD on VT just as the archive:
0dba9a31da4248a64df6488fe11f289efcbf95b1b69784d878cb96be5fd5adbb







MITRE-enhanced ML Magic to Solve Mac Malware's Identity Crisis at Scale

The Problem



Gigabytes of data from different sources



Different files types, packed, obfuscated, archives, scripts



Classify Files by malware type





Aggregate files to malware collections



Time restrictions



Give suggestions for reverse engineers

How do you find a needle in a digital haystack that's always growing?

The answer isn't to search harder. It's to build a smarter magnet.

Our approach

Multiclass classification model that classify on malware types

Embedding model to find similar malware files



Moonlock Ark. System that orchestrate feeds, pipelines, models and analytics



macOS Malware Classification models

macOS Malware Classification models

Multiclass classification:

0.96

F1 score

macOS Malware Classification models

Binary classification:

0.97

F1 score

F1: 0.89

Enhancing Mac OS Malware Detection through Machine Learning and Mach-O File Analysis

Andrew Thaeler*, Yagmur Yigit*, Leandros Maglaras*, William J Buchanan*,
Naghmeh Moradpoor*, and Gordon Russell*
* School of Computing, Engineering and The Build Environment,
Edinburgh Napier University, United Kingdom
Email: 40497204@live.napier.ac.uk, yagmur.yigit@napier.ac.uk, L.Maglaras@napier.ac.uk,
b.buchanan@napier.ac.uk N.Moradpoor@napier.ac.uk, G.Russell@napier.ac.uk

F1: 0.946

An Application of Machine Learning to Analysis of Packed Mac Malware

Kimo Bumanglag, *Dakota State University*

Date of Award
Spring 5-2022

macOS Malware Classification models

Dataset

Amount of data

Different samples

Label Annotation



Time based Train/Test split

macOS Malware Classification models

Feature engineering

Talk with the team, Inspire team to share ideas, get some insight

Learn how they detect malware manually



Learn for signature reverse engineering creates

SWARM (c) list of MITRE-enhanced small rules to detect some techniques and practices



Learn from mistakes

macOS Malware Classification models

Model

🌳 ⚡ 🤖

Algorithms based on boosted decision trees

🕑 🔁 📈

And K fold validation with time alignment

macOS Malware Classification models

Results

Not exist in VT at Inference time

e2835812a24c253861ba228a420c14de6e53b6dd139119745888761b73e23350
stealer vt.not_found

d6db94fde24addfa3bf4f4b1711093315ca54c06bedef77359bf616783d8848f
stealer vt.not_found

26c268877b855baf0ffa456e118de809bbc1f41d8ede7fa7114d015306680cad
stealer vt.not_found

d2dcd9a18cd1961f81b7e646f31f6b9666f3675c497e6e9eb89b3271ca45b6b1
stealer vt.not_found

3fe7ce1ee39e73af0bc9eb3c4330d43033a226a1517065c7ce58aa4a39c93626
stealer vt.not_found

850b84ba99ccba9f1800b99f3b06ba40c3afb679fff1697d1a1007726fa652da
stealer vt.not_found

7dbc85153419c123f297b84a39ea973e62ee48f8aba097cdb59eed841db51521
stealer vt.not_found

Undetected by Other Vendors at Inference time

30b066d21c64cb782dd2495ddc27232a8795629806d8aa3a49b63d871eea0d61
adware vt.clean

6bd58f77e947f0b8c1ed12e079ae4d998a9f46480dc556228f31c00bb2660d0f
riskware vt.clean

e370b2a8cb0052cab05c3e6f2571d556ffa2090ee8b25a61cc465248741b37dc
stealer vt.clean

8d1cb9797a78381cc2fa6ccb0369f136eeb07e2f94765cf923bef3a3a41f2c7e
riskware vt.clean

d40652486f6d0a0cb01a1d77ebc2d1569f4beb22b60de2206ec5db41e4efb2fd
stealer vt.clean

cd78a77d40682311fd30d74462fb3e614cbc4ea79c3c0894ba856a01557fd7c0
stealer vt.clean

d10012c99b413391aeb5a49aae6ebb653328054eeb266c59800cf88f77f62383
stealer vt.clean

macOS Malware embedding model

Similar Files search

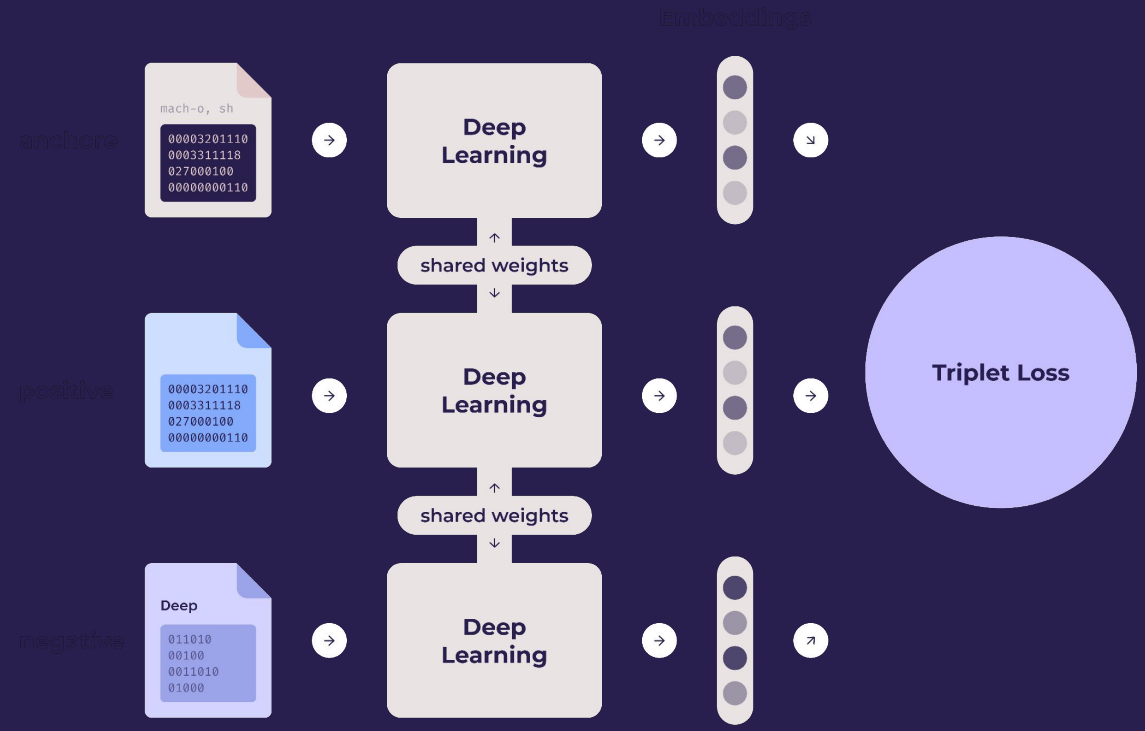
Finds similar file

Creates collections

Scores collections

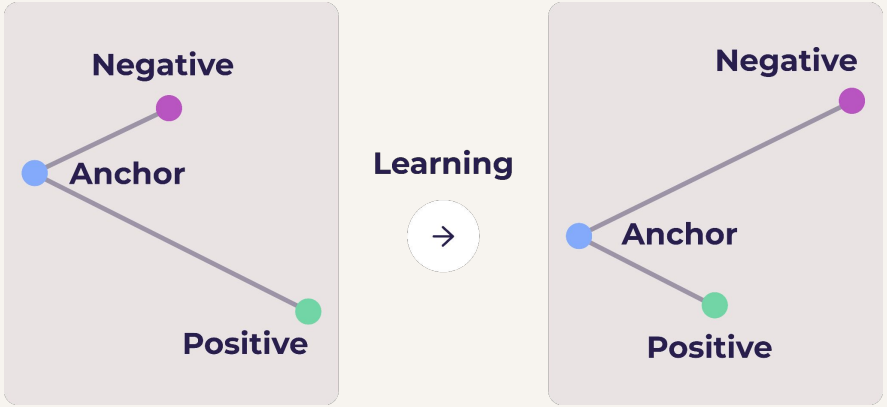
Similar Files search

Model



Similar Files search

Triplet loss



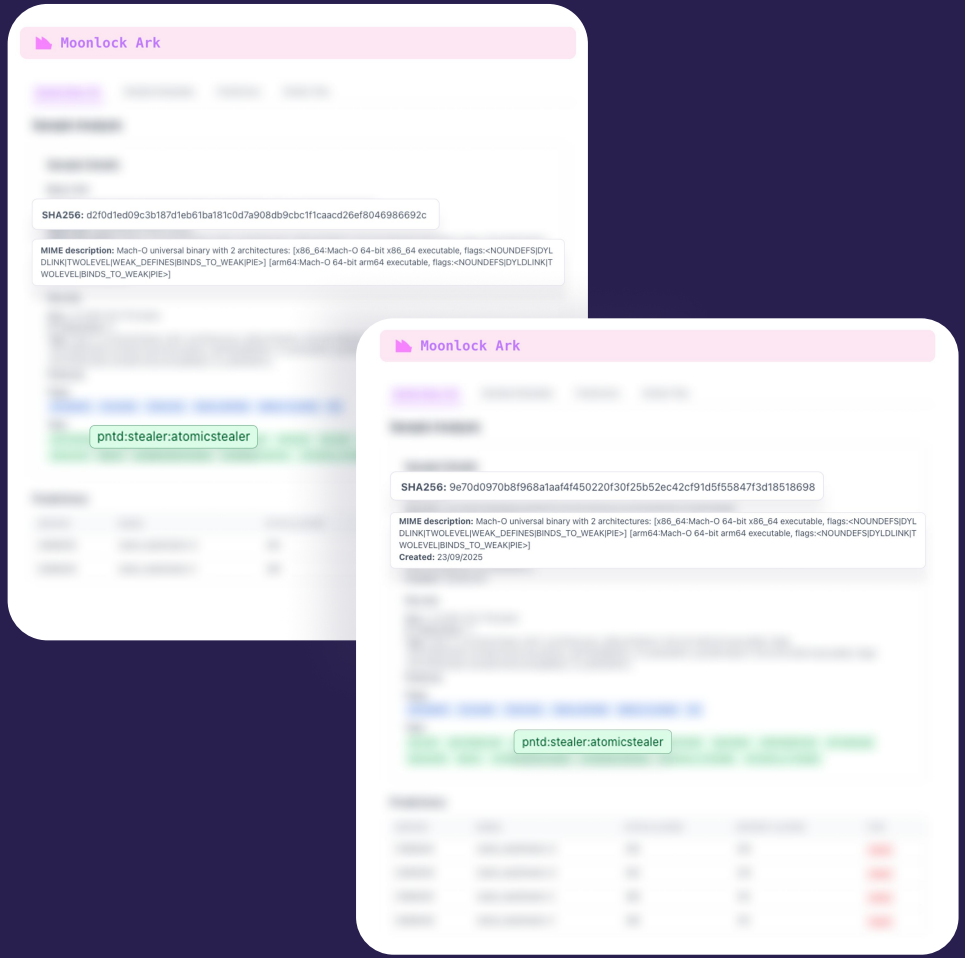
Negative samples - should be similar, and not to easy to separate

Use yara, collections, malware types and other annotation

Similar Files search

Results

cosines similarity =1



macOS Malware Classification models

Results

Grow professionally much faster

Reduces stress, when you have somebody to help you

Build even stronger system, and focusing on hardest parts

Much less stolen data, damaged reputation, and falling infrastructure

Wrapping up



Broad labels like "generic trojan" hide true malware nature and impact, causing confusion



Prioritization suffers, creating blind spots in security operations



Analyst workload increases due to need for deeper investigation of ambiguous threats



Response delays weaken defense against fast-evolving Mac malware variants



Accurate, granular classification is critical to focus resources on highest risks

Key takeaways

1

Fewer Blind Spots: Enhanced detection reduces unknown threats

2

Faster Triage: Automated scoring accelerates incident response

3

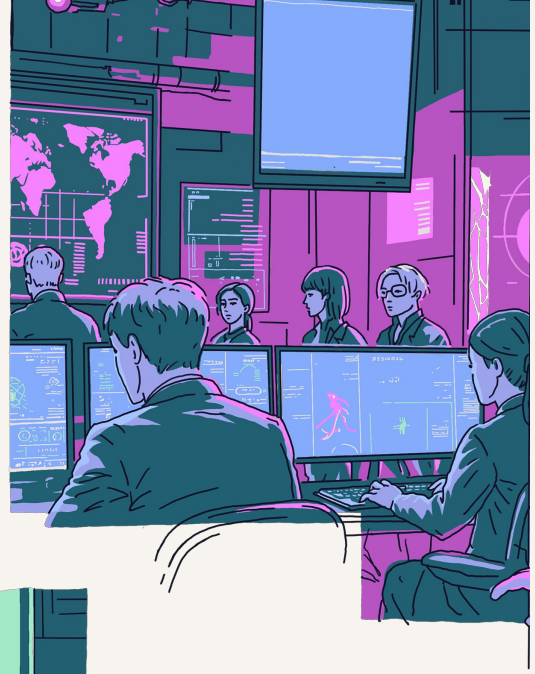
Clearer Priorities: Detailed classification guides reverse engineers to critical samples first

4

Proactive Defense: Holistic approach enables teams to keep pace with evolving Mac threats

Mac malware researchers, let's collaborate, share insights, and strengthen Mac security together!

If you spot new lures, look-alike download flows, or suspicious files, share them with @moonlock_lab





@moonlock_lab

How We Can Collaborate: Research, Triage & Knowledge Sharing

Sanity-check suspicious samples collaboratively

Work together to quickly identify threats by jointly reviewing suspicious samples, pop-ups, or installs during case triage.



Co-analyze emerging malware tactics

Conduct research sprints together to analyze new malware tactics and publish findings.

Share community signals responsibly

Exchange indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) to protect the community faster.



Accelerate detection and defense across Mac ecosystem

By collaborating openly, the community speeds up identifying and defending against threats targeting macOS.

Your feedback matters! 👉



Moonlock in Beta

Thank you! 🫶



Kseniia Yamburh

Malware Research Engineer
at Moonlock by MacPaw

xiu@macpaw.com



Nazar Grycshuk

Senior Data Scientist
at Moonlock by MacPaw

nazar@macpaw.com

@osint_barbie

in/gryshchuk/

Q&A

