

Forum: [Hack Forums](#)

Thread: [MOS Legendary Static Crypt ~ 0/63 VirusTotal macOS Loader](#)

Hackers - October 12, 2025, 8:07 pm

MOS Legendary Static Crypt

A starter kit for devs to learn encryption and methods for privacy in static analysis

This codebase only uses public, safe technologies such as XOR encryption, TMP file save, and regular macOS open/run from disk methods.

By clicking the link below you agree to only use the codebase as a reference, for legal purposes that are specifically educational, authorized, and for personal use only on devices owned solely by you.

<https://github.com/LNodesL/MOS-Legendary-Static-Crypt>

This scan result is only shown here to prove that the loader is not malicious. This codebase also does not modify runtime behaviors or attempt to conceal or otherwise hide runtime actions. This method is a demonstration of TMP/disk file loading on macOS and general encryption for packaged programs, for privacy & security. This program follows best practices and does not attempt to manipulate memory, kernel operations, or processes.

Software converted to bytes

Bytes encrypted with basic XOR

XOR value in header file

Header file in runtime stub

Push decrypted bytes to TMP file

Run TMP file

It shouldn't be that easy to get 0/63 on VT., but IT IS.

Read more about it...

Spoiler ([Click to View](#))

This is another proof of concept that achieved 0/63 on VT for a macOS loader.

I used industry standard flags as well as public samples for testing & research purposes only. Test files are shown in comparison links below.

I am making this thread because it is interesting to see how far behind VirusTotal is for Mac in general.

They only have a few runtime scans, and those are obviously not great.

I think they may be over relying on static analysis.

<https://www.virustotal.com/gui/file/05540d9820d420c5edf50dafbfd50eafaaa85f9fd7390ae835318f64edfa52d/behavior> (0/63)

vs

<https://www.virustotal.com/gui/file/205f5052dc900fc4010392a96574aed5638acf51b7ec792033998e4043efdf6c/behavior> (36/61)

This does not appear to be a VT-specific problem...

<https://virusscan.jotti.org/en-US/filescanjob/64vsbbj9ob> (0/13)

vs

<https://virusscan.jotti.org/en-US/filescanjob/zcrsudgii2> (11/13)

Here's an example build script that demonstrates what's being done on the dev side:

Code [h1]!/bin/bash[h1]

[h1]Build script for the complete system[h1]

set -e

echo "=== Building Software ==="

cd software

make clean

make

echo "Software built successfully"

echo "=== Packaging Executable ==="

cd ../packager

python3 packager.py ../software/hello_world -o ../runtime/software.h

echo "Executable packaged successfully"

echo "=== Building Runtime ==="

cd ../runtime

make clean

```
make
echo "Runtime built successfully"

echo "=== Build Complete ==="
```

The software directory is for a hello world test program.

The first real build step is the Python packager. It converts any source file to bytes (in this case a Unix executable file), and uses XOR. It pushes this to the output file, the software.h header file.

The next step builds the runtime, which has software.h included.

In the runtime program, there is nothing malicious or sneaky.

It creates a tmp file, and then after that it decrypts the software.h bytes and pushes them to the tmp file.

Then it uses a system func to execute/open the tmp file (the software that was packaged).

You can see also that the Behavior tab does show detections.

This is because this method does not perform any runtime changes for the loaded program.

With how easy it was for static (compared to Windows), we can't just say runtime is easy too. Mac has a lot of protections in place for runtime memory, processes, etc. However, like other kernels, there are syscalls, low level methods, etc.

If you are a fellow blue teamer looking into the current defenses, to identify weak spots, then 'objective-see' is a Git contributor that has sample programs for testing purposes.

normalperson223 - October 12, 2025, 9:41 pm

interesting

7 - October 14, 2025, 10:05 pm

Great thread a true legend.

Looking forward to delving into this one

Hackers - October 15, 2025, 11:13 am

(Oct 14, 2025 10:05 PM)7 Wrote: [\[CITE\]](#) Great thread a true legend.

Looking forward to delving into this one

I'll probably do another one that shows people how they can request run-as-admin/root/sudo on the current program, so user can enter PW to escalate privs.

I use this in my NMAP GUI program because some nmap scans require root. Simple to do

Since I have a new Mac, I'm revisiting some of the Windows topics but doing it for macOS because it seems like nobody has really touched this stuff as much. It's interesting.

mac is a lot more secure, I can already tell, so it makes for a good challenge to see what can or can't be done in userland.

7 - October 15, 2025, 11:20 am

but with homebrew? Isn't that making it easier?

Hackers - October 15, 2025, 11:36 am

(Oct 15, 2025 11:20 AM)7 Wrote: [\[CITE\]](#) but with homebrew? Isn't that making it easier?

I think I know what you mean - if you meant something else, LMK, but... brew, npm, pip, and a few others are probably some of the most popular spread, install, and persistence methods around...

I imagine there's a lot that can be done with those

for macOS in my post before what I mean is that it's a lot harder to do things like manipulate a process, inject memory, etc.

Even logging keys is harder because you need Accessibility perms, and syscalls can't override (or I haven't found it yet).

I did however figure out how to do screenshots (partially, still in progress) without priv escalation or permission requests.

Stanley - March 16, 2026, 8:49 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Hackers - April 14, 2026, 8:29 am

I should come back to Mac and play around more, I had fun with this one.