

# XLoader's Latest Trick | New macOS Variant Disguised as Signed OfficeNote App

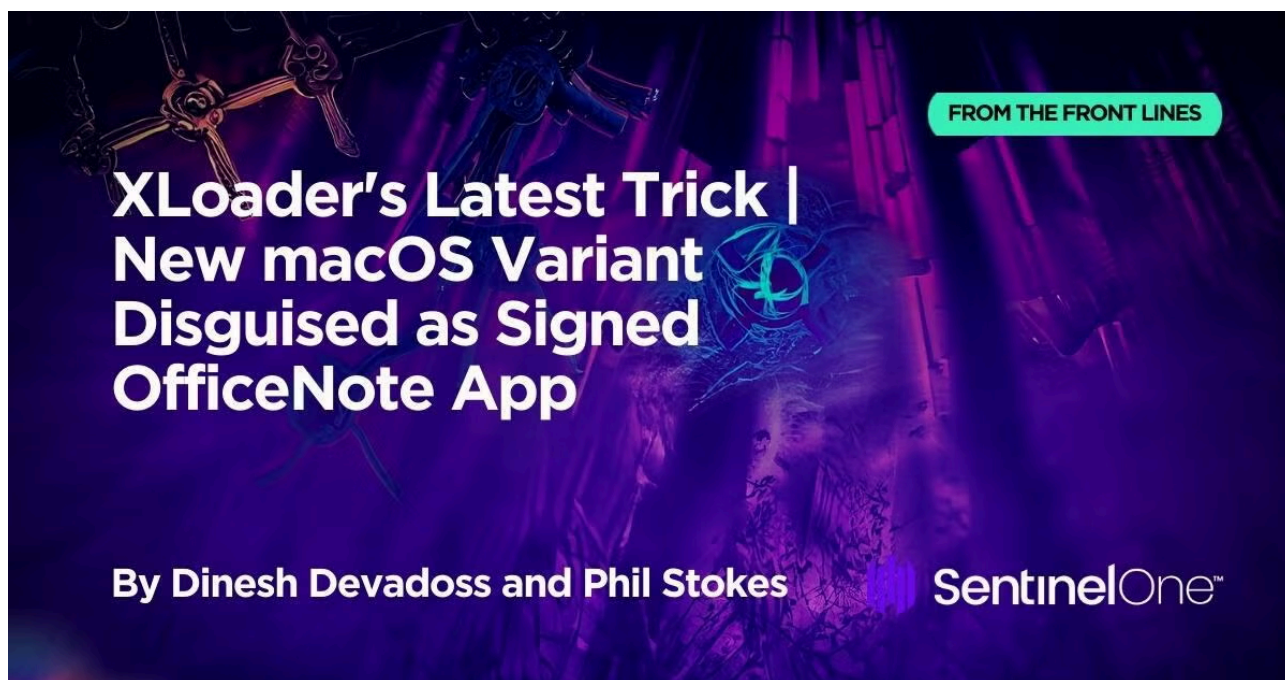
By Dinesh Devadoss & Phil Stokes

Published: 2023-08-21 · Archived: 2026-04-05 14:22:55 UTC

XLoader is a long-running malware-as-a-service infostealer and botnet that has been around in some form or another since 2015. Its [first macOS variant](#) was spotted in 2021 and was notable for being distributed as a Java program. As we noted at the time, the Java Runtime Environment hasn't shipped by default on macOS since the days of Snow Leopard, meaning the malware was limited in its targeting to environments where Java had been optionally installed.

Now, however, XLoader has returned in a new form and without the dependencies. Written natively in the C and Objective C programming languages and signed with an Apple developer signature, XLoader is now masquerading as an office productivity app called 'OfficeNote'.

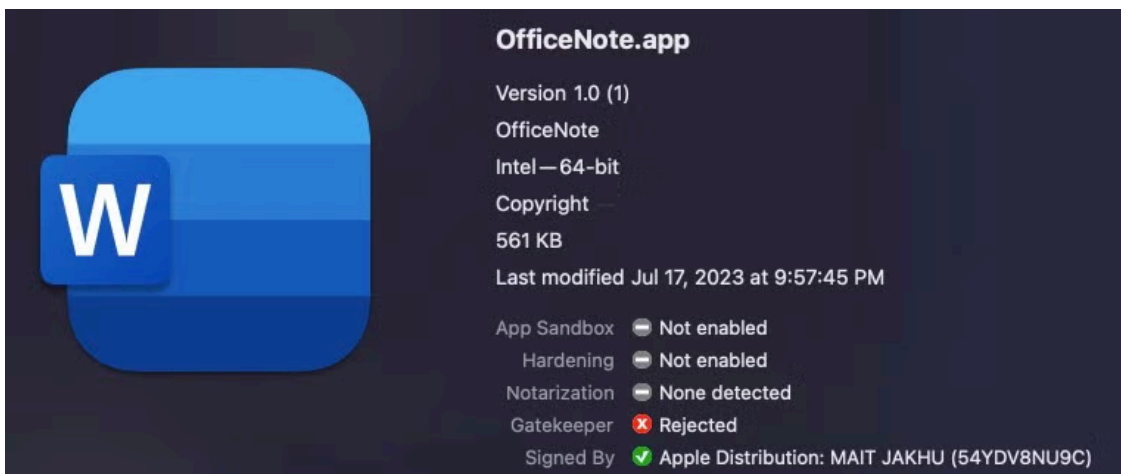
In this post, we examine how this new variant works and provide indicators for threat hunters and security teams. SentinelOne customers are automatically protected from this new variant of XLoader.



## XLoader Distribution

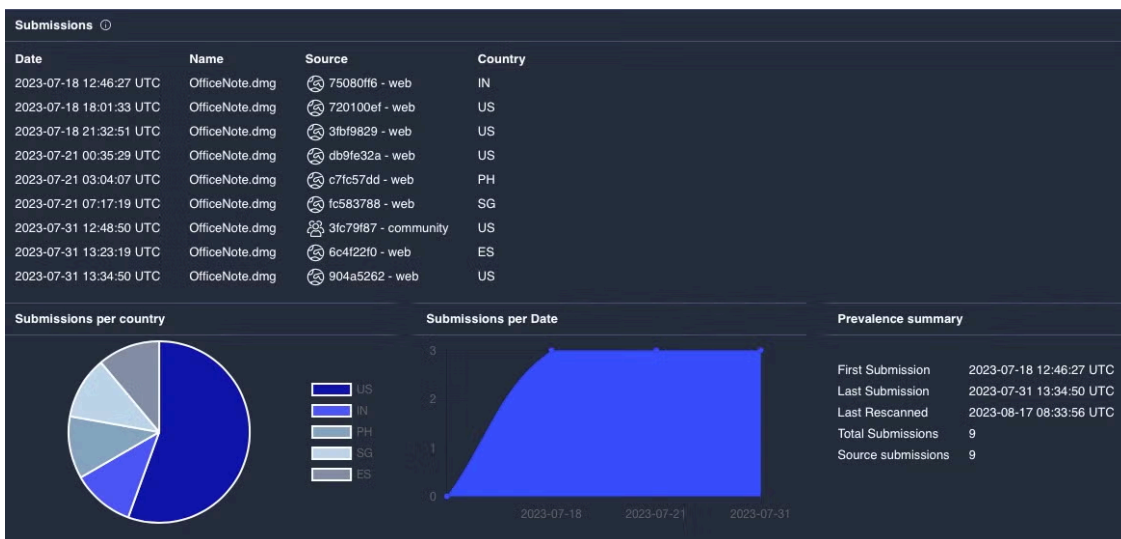
The new version of XLoader is bundled inside a standard Apple disk image with the name `OfficeNote.dmg`. The application contained within is signed with the developer signature `MAIT JAKHU (54YDV8NU9C)`.

The application was signed on 17 July, 2023; however, Apple has since revoked the signature. Despite that, our tests indicate that Apple’s malware blocking tool, [XProtect](#), does not have a signature to prevent execution of this malware at the time of writing.



OfficeNote’s revoked Apple Developer signature.

Multiple submissions of this sample have appeared on VirusTotal throughout July, indicating that the malware has been widely distributed in the wild.



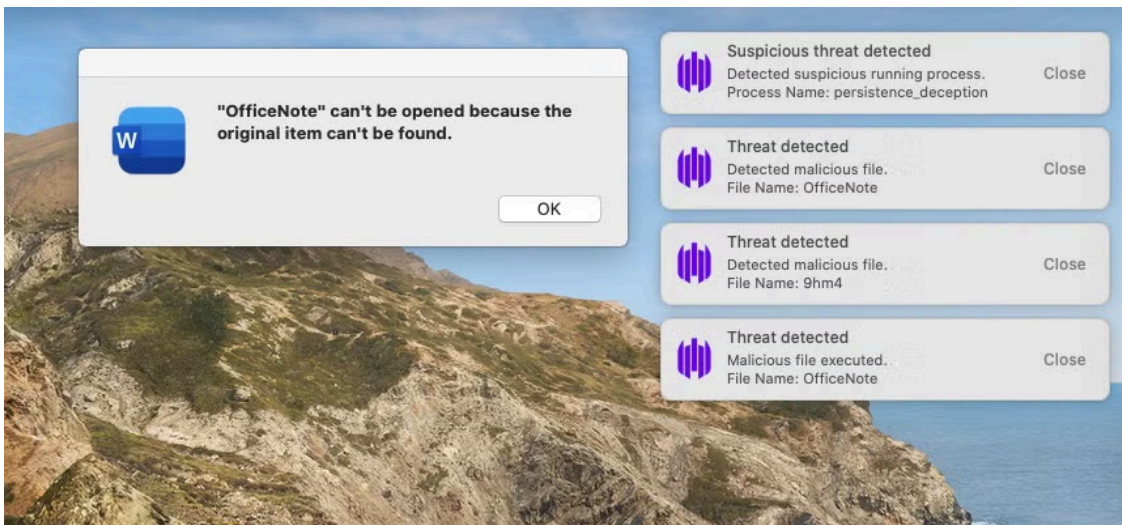
XLoader submissions to VirusTotal July 2023

Advertisements on crimeware forums offer the Mac version for rental at \$199/month or \$299/3 months.

Interestingly, this is relatively expensive compared to Windows variants of XLoader, which go for \$59/month and \$129/3 months.

## XLoader Dropper and Persistence Module

When executed, the OfficeNote application is hardcoded to throw an error message indicating that the application is non-functional. Meanwhile, the malware drops its payload and installs a persistence agent, behavior that is immediately detected by the SentinelOne agent.



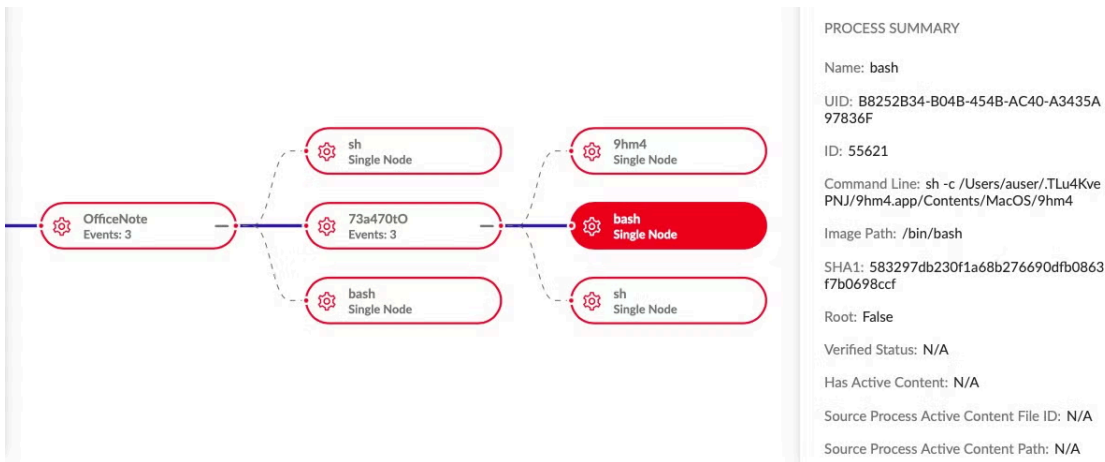
XLoader is immediately detected as a threat by the SentinelOne agent

This error message is hardcoded using a [stack string technique](#), typical of previous versions of XLoader.

```
;- asm.str.0_Document_2:
0x10000171d c645c044 mov byte [s], 0x44 ; 'D' : 68
0x100001721 c645c16f mov byte [var_3fh], 0x6f ; 'o' : 111
0x100001725 c645c263 mov byte [var_3eh], 0x63 ; 'c' : 99
0x100001729 c645c375 mov byte [var_3dh], 0x75 ; 'u' : 117
0x10000172d c645c46d mov byte [var_3ch], 0x6d ; 'm' : 109
0x100001731 c645c565 mov byte [var_3bh], 0x65 ; 'e' : 101
0x100001735 c645c66e mov byte [var_3ah], 0x6e ; 'n' : 110
0x100001739 c645c774 mov byte [var_39h], 0x74 ; 't' : 116
0x10000173d 0f2945b0 movaps xmmword [var_50h], xmm0
0x100001741 0f2945a0 movaps xmmword [var_60h], xmm0
0x100001745 0f294590 movaps xmmword [var_70h], xmm0
0x100001749 0f294580 movaps xmmword [var_80h], xmm0
0x10000174d c6458020 mov byte [var_80h], 0x20 ; mach0_segment64_0
0x100001751 c6458163 mov byte [var_7fh], 0x63 ; 'c' : 99
0x100001755 c6458261 mov byte [var_7eh], 0x61 ; 'a' : 97
0x100001759 c645836e mov byte [var_7dh], 0x6e ; 'n' : 110
0x10000175d c6458427 mov byte [var_7ch], 0x27 ; '\' : 39
0x100001761 c6458574 mov byte [var_7bh], 0x74 ; 't' : 116
0x100001765 c6458620 mov byte [var_7ah], 0x20 ; mach0_segment64_0
0x100001769 c6458762 mov byte [var_79h], 0x62 ; 'b' : 98
0x10000176d c6458865 mov byte [var_78h], 0x65 ; 'e' : 101
0x100001771 c6458920 mov byte [var_77h], 0x20 ; mach0_segment64_0
0x100001775 c6458a6f mov byte [var_76h], 0x6f ; 'o' : 111
0x100001779 c6458b70 mov byte [var_75h], 0x70 ; 'p' : 112
0x10000177d c6458c65 mov byte [var_74h], 0x65 ; 'e' : 101
0x100001781 c6458d6e mov byte [var_73h], 0x6e ; 'n' : 110
0x100001785 c6458e65 mov byte [var_72h], 0x65 ; 'e' : 101
0x100001789 c6458f64 mov byte [var_71h], 0x64 ; 'd' : 100
```

Hardcoded error message constructed on the stack

At this point, however, the malware has already been busy dropping the payload and LaunchAgent. The payload is deposited in the user's home directory as `~/73a470t0` and executed. It creates a hidden directory and constructs a barebones minimal app within it, using a copy of itself for the main executable. Although the name of the payload is hardcoded into the dropper, the names of the hidden directory, app and executable are randomized on each execution.



Execution of OfficeNote and creation of a hidden application as seen in the SentinelOne console

Meanwhile, a LaunchAgent is also dropped in the User’s Library folder. This agent is similar to that used in the previous version of XLoader, providing a `start` value to the executable. This ensures that the binary can distinguish between its first run and subsequent runs.

```
LaunchAgents — vi com.TLu4KvePNJ.9hm4.plist — vi — vi com.TLu4KvePNJ.9hm4.plist — 97x29
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-
  1.0.dtd">
3 <plist version="1.0">
4 <dict>
5     <key>Label</key>
6     <string>com.TLu4KvePNJ.9hm4</string>
7     <key>ProgramArguments</key>
8     <array>
9         <string>/Users/auser/.TLu4KvePNJ/9hm4.app/Contents/MacOS/9hm4</string>
10        <string>start</string>
11    </array>
12    <key>RunAtLoad</key>
13    <true/>
14    <key>KeepAlive</key>
15    <false/>
16 </dict>
17 </plist>
```

XLoader LaunchAgent for persistence

## XLoader Payload Behavior

As in [previous versions](#), the malware attempts to steal secrets from the user’s clipboard via the Apple API `NSPasteboard` and `generalPasteboard`. It targets both Chrome and Firefox browsers, reading the `login.json` file located in `~/Library/Application Support/Firefox/Profiles` for Firefox and `~/Library/Application Support/Google/Chrome/Default/Login Data` for Chrome. As with [other infostealers](#) we’ve observed recently, Safari is not targeted.

XLoader uses a variety of dummy network calls to disguise the real C2. We observed 169 DNS name resolutions and 203 HTTP requests. Among the many contacted hosts the malware reaches out to are the following suspicious or malicious IP addresses.

```
23[.]227.38[.]74
62[.]72.14[.]220
```

66[.]29.151[.]121  
104[.]21.26[.]182  
104[.]21.32[.]235  
104[.]21.34[.]62  
137[.]220.225[.]17  
142[.]251.163[.]121

XLoader also attempts to evade analysis both manually and by automated solutions. Both the dropper and payload binaries attempt to prevent debuggers attaching with ptrace's `PT_DENY_ATTACH` ( `0x1f` ).

```
push rbp ; [00] -r-x section size 296153 named 0.__TEXT.__text
mov rbp, rsp
push r14
push rbx
mov rbx, rsi ; argv
mov r14d, edi ; argc
mov edi, 0x1f ; 31 ; __ptrace_request request
xor edx, edx ; void*addr
xor esi, esi ; pid_t pid
xor ecx, ecx ; void*data
call sym.imp.ptrace ; long ptrace(__ptrace_request request, pid_t pid, void*addr, void*data)
; long ptrace(?, -1, ?, ?)
mov edi, 2 ; int64_t arg1
mov esi, 1
```

XLoader attempts to prevent analysts reverse engineering the malware

On execution, the malware executes `sleep` commands to delay behavior in the hope of fooling automated analysis tools. The binaries are stripped and exhibit high entropy in an attempt to similarly thwart static analysis.

```
[0x100001920]> it; i5 entropy
md5 c68e9ab57bff9de72414c83d612636dc
sha1 26fd638334c9c1bd111c528745c10d00aa77249d
sha256 adda1b2139b7bbec7f051ecb58d1015d9ac8d5552987374ec48c6598acf54de8
[Sections]
nth paddr size vaddr vsize perm entropy type name
-----
0 0x00001400 0x1db3e 0x100001400 0x1db3e -r-x 7.12157708 REGULAR 0.__TEXT.__text
1 0x0001ef3e 0x6 0x10001ef3e 0x6 -r-x 1.79248125 SYMBOL_STUBS 1.__TEXT.__stubs
2 0x0001ef44 0x1a 0x10001ef44 0x1a -r-x 3.11508276 REGULAR 2.__TEXT.__stub_helper
3 0x0001ef60 0x40 0x10001ef60 0x40 -r-x 0.00000000 REGULAR 3.__TEXT.__const
4 0x0001efa0 0x48 0x10001efa0 0x48 -r-x 1.51041723 REGULAR 4.__TEXT.__unwind_info
5 0x0001f000 0x10 0x10001f000 0x10 -rw- 0.00000000 NONLAZY_POINTERS 5.__DATA.__nl_symbol_ptr
6 0x0001f010 0x8 0x10001f010 0x8 -rw- 1.75000000 LAZY_SYMBOL_POINTERS 6.__DATA.__la_symbol_ptr
```

The XLoader binaries exhibit high entropy in the `__text` section

## Conclusion

XLoader continues to present a threat to macOS users and businesses. This latest iteration masquerading as an office productivity application shows that the targets of interest are clearly users in a working environment. The malware attempts to steal browser and clipboard secrets that could be used or sold to other threat actors for further compromise.

IT and security teams are advised to deploy a trusted third party security solution to prevent and detect malware such as XLoader. To see how SentinelOne can help protect the macOS devices in your fleet, [contact us](#) or [request a free demo](#).

## Indicators of Compromise

SHA1	Description
26fd638334c9c1bd111c528745c10d00aa77249d	Mach-O Payload
47cacf7497c92aab6cded8e59d2104215d8fab86	Mach-O Dropper
5946452d1537cf2a0e28c77fa278554ce631223c	Disk Image
958147ab54ee433ac57809b0e8fd94f811d523ba	Mach-O Payload

### FilePaths

~/73a470t0

### Developer ID

MAIT JAKHU (54YDV8NU9C)

### Network Communications

23[.]227.38[.]74  
62[.]72.14[.]220  
66[.]29.151[.]121  
104[.]21.26[.]182  
104[.]21.32[.]235  
104[.]21.34[.]62  
137[.]220.225[.]17  
142[.]251.163[.]121

www[.]activ-ketodietakjsy620[.]cloud  
www[.]akrsnamchi[.]com  
www[.]brioche-amsterdam[.]com  
www[.]corkagenexus[.]com  
www[.]growind[.]info  
www[.]hatch[.]computer  
www[.]kiavisa[.]com  
www[.]lushespets[.]com  
www[.]mommachic[.]com  
www[.]nationalrecoveryllc[.]com  
www[.]pinksugarpopmontana[.]com  
www[.]qhsbobfv[.]top  
www[.]qq9122[.]com  
www[.]raveready[.]shop  
www[.]spv88[.]online  
www[.]switchmerge[.]com

Source: <https://www.sentinelone.com/blog/xloaders-latest-trick-new-macos-variant-disguised-as-signed-officenote-app/>