

Member-only story

Hacking macOS: How to Dump 1Password, KeePassX & LastPass Passwords in Plaintext



Null Byte · Follow

7 min read · Jun 11, 2019



1K

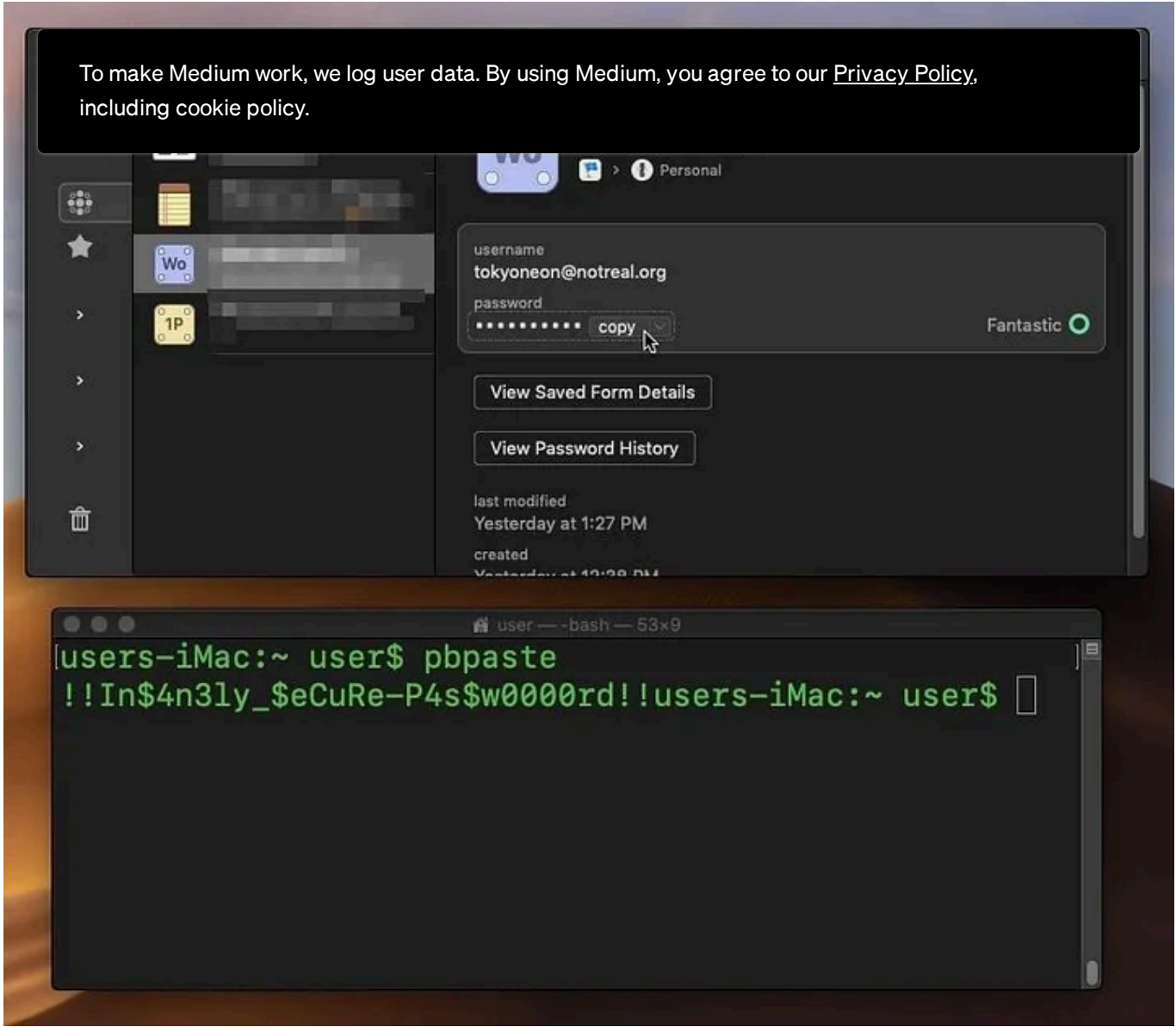


4



KeePassX, 1Password, and LastPass are effective against keyloggers, phishing, and database breaches, but passwords managers rely on the operating system’s clipboard to securely move credentials from the password vault to the web browser. It’s within these few seconds that an attacker can dump the clipboard contents and exfiltrate passwords.

Two scenarios come to mind with a clipboard-dumping attack geared toward password managers, and both utilize the pbpaste command found in all versions of macOS. Pbpaste will take any data found in the clipboard (including passwords) and write it to the standard output. Any macOS user can try this by first copying a password to the clipboard then immediately typing **pbpaste** into a terminal.



It doesn't require special privileges to execute pbpaste, and the clipboard can be written to any file, as shown below.


```
~$ pbpaste >>/tmp/clipboard.txt
```


Option 1: Dump the Clipboard Locally


Scenario: The attacker has established a [persistent backdoor](#) and wants to gather passwords stored in...

Create an account to read the full story.

The author made this story available to Medium members only.
If you're new to Medium, create a new account to read this story on us.

 Sign up with Google

 Sign up with Facebook

 Sign up with email

Already have an account? [Sign in](#)



To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.



Written by Null Byte

3.2K Followers

The aspiring white-hat hacker/security awareness playground

Follow



More from Null Byte



Null Byte

How to Find Vulnerable Webcams Across the Globe Using Shodan
Search engines index websites on the web so you can find them more efficiently, and the...

★ Aug 7, 2019 🖱️ 111 💬 1 📌⁺



Null Byte

How to Hack Open Hotel, Airplane & Coffee Shop Wi-Fi with MAC...
After finding and monitoring nearby wireless access points and devices connected to the...

★ Mar 16, 2018 🖱️ 123 📌⁺

Null Byte

How to Set Up an SSH Server with Tor to Hide It from Shodan &...
Keep your SSH service out of Shodan's database before hackers find new ways to...

★ May 23, 2019 🖱️ 685 📌⁺

Null Byte


Top 10 Browser Extensions for Hackers & OSINT Researchers
Extensions can unlock some pretty spectacular tools for hackers and OSINT...

★ Jun 28, 2019 🖱️ 1K 💬 3 📌⁺

See all from Null Byte

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.


Recommended from Medium

 Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling...

 Jun 18  1.6K  53 

 Navindu Chamodya in Bug Zero

The Dark Web and Cybercrime

Introduction

May 13  1 

Lists

General Coding Knowledge

20 stories · 1693 saves

Coding & Development


11 stories · 881 saves

ChatGPT prompts

50 stories · 2166 saves

AI Regulation


6 stories · 601 saves

 Satyam Pathania in OSINT Team

Hack Any Mobile Phone Remotely

Ethically — but note — this used to work great with phone under android 10

 Oct 11  243  3 

 Alexander Nguyen in Level Up Coding

The resume that got a software engineer a \$300,000 job at Google.

1-page. Well-formatted.

 Jun 1  25K  483 



The Tools You Should Never Run in...

Hey there! If you’re managing Linux systems in production, you know things can go from...

★ Oct 10 🖱️ 987 💬 21



Network Scans Like a Pro for Free...

Welcome to this step-by-step tutorial on NMap Viewer, a free, self-hosted network...

★ Oct 5 🖱️ 159 💬 3



See more recommendations