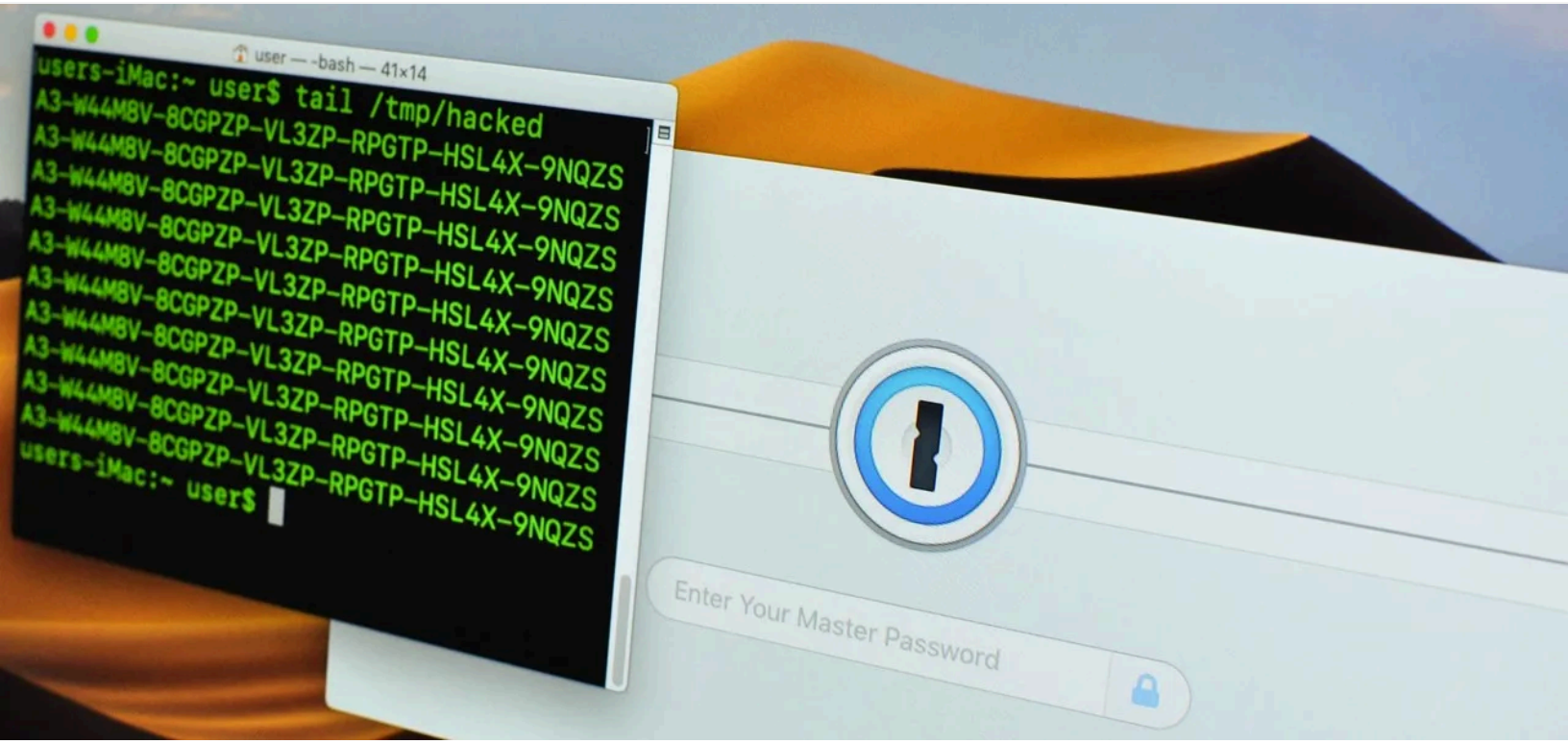


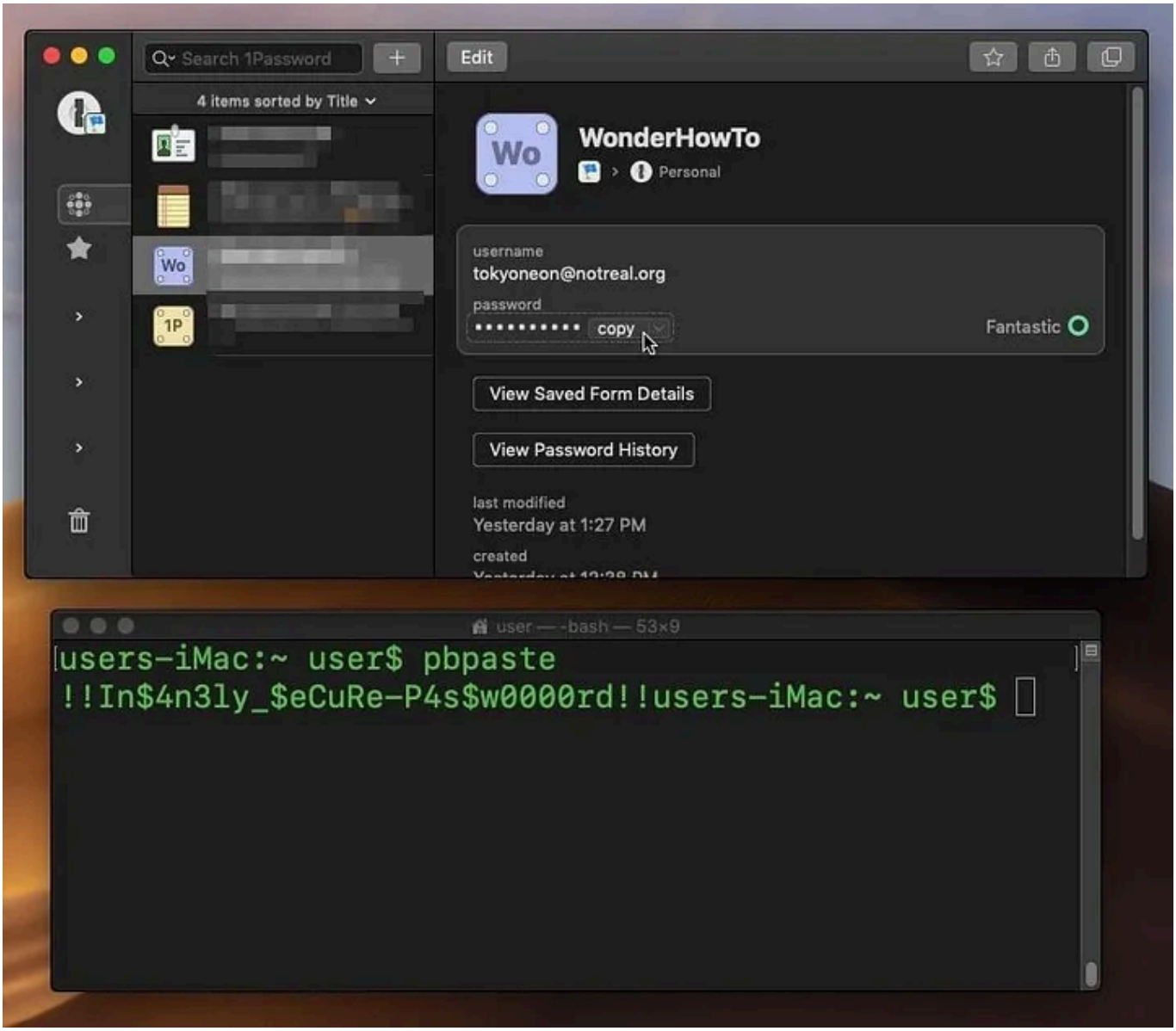
Member-only story

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

Null Byte · Follow
7 min read · Jun 11, 2019

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...