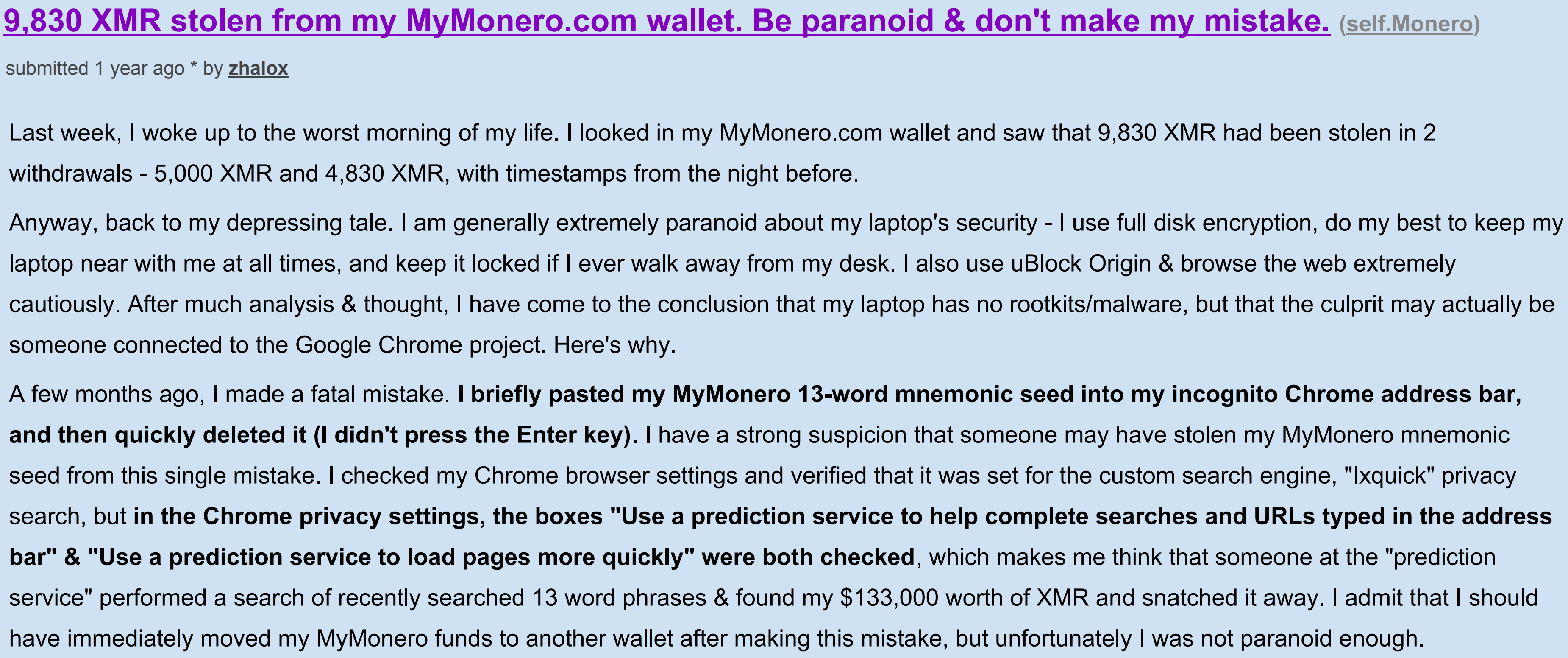
IsthmusCrypto
Seed Sieve

2018.03.02

https://www.reddit.com/r/Monero/comments/52sw9r/9830_xmr_stolen_from_my_mymonerocom_wallet_be/



9,830 XMR stolen from my MyMonero.com wallet. Be paranoid & don't make my mistake. (self.Monero)

submitted 1 year ago * by **zhalox**

Last week, I woke up to the worst morning of my life. I looked in my MyMonero.com wallet and saw that 9,830 XMR had been stolen in 2 withdrawals - 5,000 XMR and 4,830 XMR, with timestamps from the night before.

Anyway, back to my depressing tale. I am generally extremely paranoid about my laptop's security - I use full disk encryption, do my best to keep my laptop near with me at all times, and keep it locked if I ever walk away from my desk. I also use uBlock Origin & browse the web extremely cautiously. After much analysis & thought, I have come to the conclusion that my laptop has no rootkits/malware, but that the culprit may actually be someone connected to the Google Chrome project. Here's why.

A few months ago, I made a fatal mistake. **I briefly pasted my MyMonero 13-word mnemonic seed into my incognito Chrome address bar, and then quickly deleted it (I didn't press the Enter key)**. I have a strong suspicion that someone may have stolen my MyMonero mnemonic seed from this single mistake. I checked my Chrome browser settings and verified that it was set for the custom search engine, "Ixquick" privacy search, but **in the Chrome privacy settings, the boxes "Use a prediction service to help complete searches and URLs typed in the address bar" & "Use a prediction service to load pages more quickly" were both checked**, which makes me think that someone at the "prediction service" performed a search of recently searched 13 word phrases & found my $133,000 worth of XMR and snatched it away. I admit that I should have immediately moved my MyMonero funds to another wallet after making this mistake, but unfortunately I was not paranoid enough.

Regardless of whether THIS theft occurred as speculated,
Zhalox's post describes a juicy real attack vector

Grammarly Bug Let Snoops Read What You Wrote, Typos and All (Updated)

Andrew Cout 2/05/18 4:10pm

The **Grammarly browser extension for Chrome and Firefox contained a “high severity bug” that was leaking authentication tokens**, according to a bug report by Tavis Ormandy, a security researcher with Google’s Project Zero. **This meant that any website a Grammarly user visited could access the user’s “documents, history, logs, and all other data,” according to Ormandy.**

Grammarly provides **automated copyediting for virtually anything you type into a browser that has the extension enabled**, from blogs to tweets to emails to your attorney. This bug only affected the Grammarly Editor, according to the company

Grammarly has approximately 22 million users

Certainly, many of the 22 million Grammarly users have (accidentally or intentionally) exposed a seed to a website field

IsthmusCrypto Seed Sieve

- Extremely simple public-domain algorithm
- Designed to NOT interfere with indexing and learning on non-seed strings.
- Should be implemented device-side, before telemetry to any service
- Compares input string against seed mnemonic word lists (e.g. Bitcoin's BIP39)
- Count # of seed word hits, and total word count.
- Algorithm:

```
IF [SeedWords/WordCount > 0.3] AND [SeedWords > 6]

THEN replace seed words with name of seed list
```

pseudocode

```
algorithm SeedSieve(InputString, BIP39dictionary)  is
     InputWordSet = Uppercase InputString with special characters (not [a-Z]) turned into delimiters;
     NumSeedHits := number of BIP39dictionary elements that appear in InputWordSet;
     TotalWordcount := number of words in InputWordSet;
     SeedWordDensity := NumSeedHits/TotalWordcount;
     if (NumSeedHits>6) & (SeedWordDensity>0.3)  then
          SafeString := replace the seed words in InputString with the string “[BIP39]”;
     else
          SafeString := InputString;
     return SafeString
```

```
//Ex:
// SeedSieve(“Current-borne, wave-flung, tugged hugely by the whole might of ocean, the 10 jellyfish drift”,
//     {ABYSS, BORNE, DRIFT, HUGELY, JELLYFISH, LIGHT, MIGHT, OCEAN, SHINES, TIDAL, TUGGED, WAVE, WHOLE})
//     InputWordSet = {CURRENT,BORNE,WAVE,FLUNG,TUGGED,HUGELY,BY,THE,WHOLE,MIGHT,OF,OCEAN,THE,JELLYFISH,DRIFT}
//     NumSeedHits = 9;
//     TotalWordCount = 15;
//     SeedWordDensity = 9/15 = 0.6;
// returns:
//     SafeString = “Current-[BIP39], [BIP39]-flung, [BIP39] [BIP39] by the [BIP39] [BIP39] of [BIP39], the 10 [BIP39] [BIP39]”
```

Input String	#SEED	Ratio #SEED/all	Output String
The quick brown fox jumps over the lazy dog	6	0.6	The quick brown fox jumps over the lazy dog
Apple farm near upstate New York.	3	0.5	Apple farm near upstate New York
Lorem ipsum dolor sit amet, consectetur adipiscing	0	0	Lorem ipsum dolor sit amet, consectetur adipiscing
Lorem Ipsum is simply dummy text of the printing and typesetting industry.	2	0.1	Lorem Ipsum is simply dummy text of the printing and typesetting industry.
<< a 5000 word transcript >>	245	0.05	*<< string would be unchanged >>*
R4nd0m words physical collect false breast said blonde strife howl metal choice mirror pay	12	0.8	R4nd0m words [BIP39] [BIP39] [BIP39] [BIP39] [BIP39] [BIP39] [BIP39] [BIP39] [BIP39] [BIP39] [BIP39] [BIP39]
I think peach time depth I am safer hour hurl afternoon for adding words hurl canvas bite gone to the list harm lick	12	0.54	I think [BIP39] [BIP39] [BIP39] I am safer [BIP39] [BIP39] [BIP39] for adding words [BIP39] [BIP39] [BIP39] [BIP39] to the list [BIP39] [BIP39]
MyMonero.com list snake civilian salads doing maps ambush alumni geyser ramped hounded ridges adventure salads	13	0.8	MyMonero.com list [XMR] [XMR] [XMR] [XMR] [XMR] [XMR] [XMR] [XMR] [XMR] [XMR] [XMR] [XMR] [XMR]
Use CAPS insensitive search MoviE ~*~ SoNg LiMiT DAD !! QuESTiOn ?? HunGEr 1234 FrOnT AsK HuRrY PlaNeT LOLOL LauNcH EndLeSS	12	0.7	Use CAPS insensitive search [BIP39] ~*~ [BIP39] [BIP39] [BIP39] !! [BIP39] ?? [BIP39] 1234 [BIP39] [BIP39] [BIP39] [BIP39] LOLOL [BIP39] [BIP39]

People ARE going to lose money this way

Note to business owners & software developers:

If a user pastes a seed into a website form etc, that is their OpSec failure. However, customers are going to [rightly or wrongly] blame you and your business/application/extension/etc if

- A hacker, employee, or third-party partner searches your database and steals your users' life savings
- A hacker exploits weaknesses your app/extension data collection/transmission/storage to collect users' seeds

Services not designed with security in mind may still end up transmitting and storing sensitive financial information, without any appropriate precautions. Every day, seeds are stashed on clipboards, pasted into URL bars, saved as email drafts, sent in messages to others or self, etc....

For an honest business, <u>there is nothing to gain from leaving seed info in your data stream and or data storage</u>. However, there is a lot for you (and your customers) to lose...

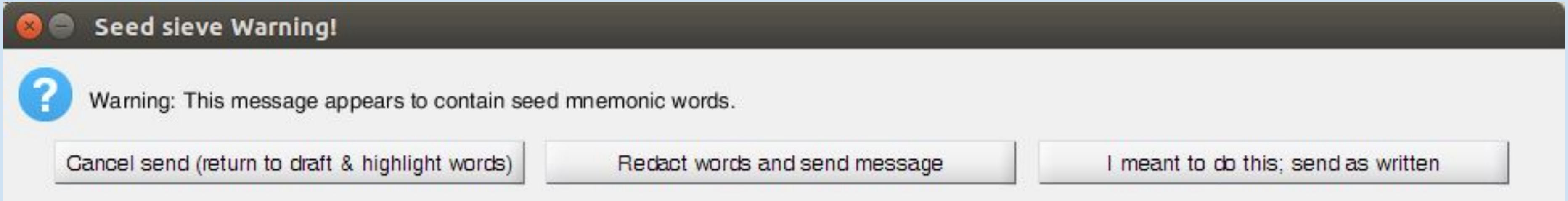
Minimize your liability. Device-side filter your telemetry data. Remember datensparsamkeit.

Notes

- If you are doing market analysis, learning, etc from your data, then the Seed Sieve should actually improve model performance! Why? Seed words (“apple”, “boat” ...) are red herrings for message content and will confuse the algorithms! By replacing seed words with list tags (e.g. [BIP39]), you can accurately classify these messages as cryptocurrency-related.

- In the near future, seed information may be classified as personal financial data, and there may be legal consequences for transmitting financial information insecurely. Any seed that has been even possibly exposed is never secure again, and danger from mistakes made today cannot be undone tomorrow.

- Does not have to be used only for redaction. An email client or chat client might run all messages through the sieve and, if a message tests positive, present warning:


Seed sieve Warning!
Cancel send (return to draft & highlight words)
Redact words and send message
I meant to do this; send as written

Warning: This message appears to contain seed mnemonic words.

Notes

- Couple with OCR to scan and\or redact legible seeds in images, movies
    - This should be implemented by social media sites to protect their users! Warning and/or auto-redact, with the option to override (for example, for wallet tutorial videos where a visible seed is intentional).
    - Like a privacy version of Word Lens https://www.youtube.com/watch?v=h2OfQdYrHRs
    - I would also like to see screenshot apps include this. It would be great if Android OS flashed a warning when users try to take a screenshot of their Bitcoin wallet seed for backup.

- Use this for:
    - Crash reports
    - Beta testing data
    - Predictive fields
    - Log files
    - Data visible to (/stored for) customer support
    - Data visible to (/stored for) technical support
    - Etc

- Are there any standard libraries for tools to clean field inputs? Can just be added to those?

- How can this be distributed to best encourage adoption? What coding languages?