# CryptoShuffler Stole $150,000 by Replacing Bitcoin Wallet IDs in PC Clipboards

By Catalin Cimpanu

Published: 2017-11-01 · Archived: 2026-04-05 15:47:14 UTC


The operators of a malware strain identified as CryptoShuffler have made at least $150,000 worth of Bitcoin by using an extremely simple scheme.

Crooks infect users with their trojan, which then sits idly on users' computers and does nothing but watch the user's clipboard and replace any string that looks like a Bitcoin wallet with the attackers' address.

When the victim wants to make a payment and copy-pastes the wallet ID inside a payment field, if the user doesn't notice the new address, crooks would receive the payment.

## CryptoShuffler has been active since 2016

The trojan has been making the rounds for more than a year. Transactions to CryptoShuffler's Bitcoin wallet reached their peak in late 2016, but Kaspersky Lab detected a new campaign in June 2017.

"The malware described is a perfect example of a 'rational' gain," said Sergey Yunakovsky, Kaspersky Lab malware analyst. "The scheme of its operation is simple and effective: no access to pools, no network interaction, and no suspicious processor load."

CryptoShuffler's Bitcoin wallet currently holds 23.21 Bitcoin, worth over $150,000 at today's (record) Bitcoin price of $6,544.

## CryptoShuffler targets other cryptocurrencies as well

Besides Bitcoin, crooks also targeted wallets for other cryptocurrencies, such as Dogecoin, Litecoin, Dash, Ethereum, Monero, and Zcash.

The funds in the wallets for the other cryptocurrencies aren't pennies either, ranging from tens to thousands of US dollars.

CryptoShuffler is one of the most successful malware families targeting cryptocurrencies to date. For example, another malware author wasted months scanning for vulnerable IIS servers to install a Monero miner, only to make $63,000. Making over $150,000 for some code that watches the clipboard and replaces a string is quite the ROI (return on investment).

### CryptoShuffler MD5 hash:

```
 0ad946c351af8b53eac06c9b8526f8e4
095536CA531AE11A218789CF297E71ED
14461D5EA29B26BB88ABF79A36C1E449
1A05F51212DEA00C15B61E9C7B7E647B
1E785429526CC2621BAF8BB05ED17D86
2028383D63244013AA2F9366211E8682
25BF6A132AAE35A9D99E23794A41765F
39569EF2C295D1392C3BC53E70BCF158
50E52DBF0E78FCDDBC42657ED0661A3E
6EB7202BB156E6D90D4931054F9E3439
7AE273CD2243C4AFCC52FDA6BF1C2833
7EC256D0470B0755C952DB122C6BDD0B
80DF8640893E2D7CCD6F66FFF6216016
AA46F95F25C764A96F0FB3C75E1159F8
B7ADC8699CDC02D0AB2D1BB8BE1847F4
D45B0A257F8A0710C7B27980DE22616E
D9A2CD869152F24B1A5294A1C82B7E85
```

---