Ad Tracker on e-commerce site can flip the Bitcoin transaction mask

The study announced last week that cookies and other information collected by ad tracker on e-commerce sites can be used to flip an anonymous mask of Bitcoin transactions.

The study announced last week that cookies and other information collected by ad tracker on e-commerce sites can be used to flip an anonymous mask of Bitcoin transactions.

No matter how careful users hide their identity behind random Bitcoin addresses, when buying products, they cannot expect online buying sites where transactions can be kept confidential. and that anonymously.

Typically, these sites store each user's cookies or are willing to share information about buyers with advertising companies. These are done for financial purposes, allowing advertisers to bring ads to the right audience and increase the chances of clicking on them to increase revenue.

Ad tracker poses a risk for Bitcoin's anonymity

Information collected by e-commerce sites may include cookies on the user system to provide information about products, prices, shopping carts, emails, shipping addresses, etc.

Even if the page or ad tracker does not store so much information, an attacker or a state agency can aggregate information from many places. This information will help investigators find user profiles, assign suspicious Bitcoin addresses to real-life identities, online usernames, email addresses and many other data that e-commerce sites collected and transmitted to advertisers.

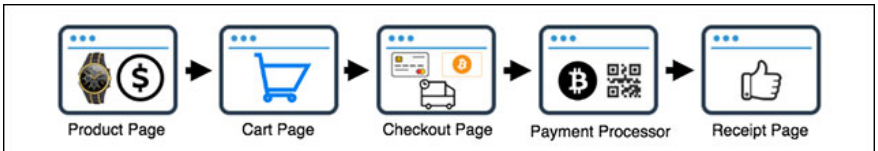

Fig. 2. **An illustration of a typical payment flow on a merchant site.** Each step of this flow presents opportunities for leaking transaction-relevant information to embedded third-party trackers.

Transaction process on e-commerce sites

In the best case, even if these pages store little information about users, customers who pay for products via Bitcoin and return to the page, pay via credit card or other methods, can also Assigned to small things like cookies.

Researcher investigates 130 Bitcoin-friendly online stores

The team from Princeton University analyzed 130 e-commerce sites from 21 countries that allow users to pay with BItcoin. They find out how these pages handle Bitcoin transactions and what information leaked during processing. And below are the results:

1. 53/130 leaked payment information to third parties, usually from the shopping cart page.
2. 49/130 single leakage PII.
3. 32/130 email address leak.
4. 27/130 and 25/130 leaking first and last names.
5. 15/130 leaked user names.
6. 13/130 leaked delivery address information.
7. 10/130 leaks leaking user phone numbers.
8. 25/130 leaks sensitive information leaks to third parties, even when monitoring protection is turned on.
9. 12/130 BItcoin address leaks.
10. 11/130 leaked Bitcoin prices for products.
11. 28/130 activity leaks added to the cart.
12. 107/130 gives the third party script access to information related to the transaction.
13. 125/130 gives the 3rd party script access to some models of PII.

All of this data is very important in resolving anonymous user identities, especially if it is gradually collected on the online advertiser server for months or years.