**What is the 2easy dark web marketplace?**

Market of stolen data?



**EXECUTIVE SUMMARY:**

The 2easy dark web market has gained fame for its role in marketing and exchange of stolen data. Users of the site recover stolen data from 600,000 devices that have been corrupted by malicious computer-stealing software.

**What is 2easy?**

The 2easy platform debuted in 2018 and has since shown rapid growth. In 2021, the platform sold data from 28,000 infected devices. 2easy was considered the youngest player on this particular black web with information theft space.

Since then, analysis shows that ‘high-level’ offerings on the site increased interest among cyber criminals. The hackers want to see which network they can access next.

**How it works**

Data logs are archived data stolen from web browsers that are vulnerable to malware or malware. Logs usually contain account credentials, cookies, and stored credit card information.

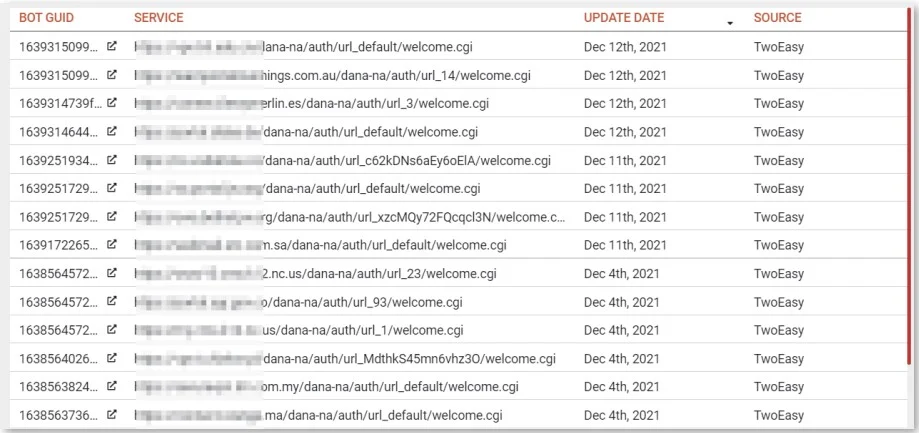
2easy platform is fully automatic, allowing people to create accounts, add money to wallets and participate in purchases without direct contact with merchants. Hackers can buy logs for as little as $ 5.00 per item. This is about 5X less than what a typical competitor offers and is three times the average cost of bot logs in an underground market.

2easy logs always provide valid information that provides network access to many organizations. In addition to the cost benefits of hackers, they can also check various performance information by purchasing services they may not offer. The only culprit in this case is the intruder.

**Why 2easy is important**

Certificate-filled logs represent departmental keys and those departments can lead directly to your online accounts, giving hackers access to financial information or corporate networks. Although the logs are sold for as little as $ 5.00 per item, the damage done to your organization can cost millions of dollars.

In June 2021, an Electronic Arts attack occurred as a result of cybercriminals who bought stolen cookies online and then equipped them to gain access to the EA Slack channel. Upon reaching the Slack station, the attackers tricked the EA employee into giving them a multi-item verification token. Another history.



**More details**

Items purchased on the 2easy platform are packaged as archive files containing stolen logs from selected bots. The specific type of content depends on a malicious computer program to steal previously used information and associated capabilities. Each type of malware program focuses on something a little different.

In 50% of cases, retailers are relying on RedLine as a computer program of their choice. RedLine can scan passwords, cookies, credit cards, FTP information and more. Of the 18 active vendors on site, five use RedLine alone. The other four use RedLine in conjunction with other types of malware.

**Conclusion**

2easy supports an ecosystem that exploits logs to help hackers gain access to secret and otherwise inaccessible areas. These types of intrusions can lead to ransomware attacks and other types of malware attacks. Measures to prevent access-based attacks include the use of multiple authentication, regular password exchange, and the use of zero trust principles.