

Financial Fraud-Focused Cybercrime Marketplace 'Styx' Emerges

A recently identified dark web portal offers illegal services related to financial fraud, identity theft, and money laundering, cybersecurity company Resecurity warns.

Dubbed Styx Marketplace, the portal offers data dumps, cash-out services, fake and stolen IDs, SIM cards, multi-factor authentication bypass solutions, banking malware, and other types of illegal services.

Initially mentioned on the dark web in early 2022, the marketplace opened in January 2023, following an escrow module for brokering transactions between cybercriminals.

Registered users are provided with access to the various illicit services available on the portal. A Trusted Sellers section also exists, likely for vendors that have been vetted by the Styx administrators.

"Some of the service descriptions are limited – the marketplace connects actors via Telegram contacts and various automated bots as a security measure," Resecurity explains.

Users interested in purchasing services are first required to fund their Styx wallet in cryptocurrency, with available options including Bitcoin (BTC), Ethereum (ETH), and Tether (USDT).

Resecurity also linked Styx to tools for online-banking theft, anti-fraud bypasses, and identity spoofers, including some marketed via Telegram channels. Some of these tools are

optimized for mobile devices.

The focus of Styx, however, remains the selling of compromised online banking credentials, stolen credit card data, and cryptocurrency and ecommerce accounts. The marketplace also facilitates 'digital bank' and VCC (virtual credit card) fraud.

Some of the Styx vendors sell personally identifiable information (PII), including stolen Social Security numbers (SSNs). One vendor sells large volumes of SSNs and ID-related data of victims in the US, Canada, the Netherlands, the UK, and other countries, along with stolen business data.

Fake IDs and document forgery represent another significant product offering available on Styx. One vendor, who uses the handle 'Podorozhnik', is well known on the dark web and widely used by cybercriminals.

Styx also houses multiple vendors offering money laundering, such as cash-out services from stolen banking, cryptocurrency exchange, ecommerce, and VCC accounts.

Other vendors on Styx provide telephone and email flood services, tutorials on how to perform cybercrime and fraud, and other types of fraud services.

Related: Cybercrime Marketplace Leaks Over 2.1 Million Payment Cards

Related: Authorities Seize Online Marketplace for Stolen Credentials

Related: Success of Genesis Market Takedown Attempt Called Into Question

Financial Fraud-Focused Cybercrime Marketplace 'Styx' Emerges