# DiamondFox (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:19:15 UTC

## DiamondFox

aka: Crystal, Gorynych, Gorynch

VTCollection

---

According to PCrisk, DiamondFox is highly modular malware offered as malware-as-a-service, and is for sale on various hacker forums. Therefore, cyber criminals who are willing to use DiamondFox do not necessarily require any technical knowledge to perform their attacks.

Once purchased, this malware can be used to log keystrokes, steal credentials (e.g., usernames, email addresses, passwords), hijack cryptocurrency wallets, perform distributed denial of service (DDoS) attacks, and to carry out other malicious tasks.

DiamondFox allows cyber criminals to choose which plug-ins to keep activated and see infection statistics in real-time.

**References**

**Yara Rules**

▶ [TLP:WHITE] win_diamondfox_auto (20180607 | autogenerated rule brought to you by yara-signator)

Download all Yara Rules

---