Severity

High

Analysis Summary

DCRat — a Russian backdoor, was initially introduced in 2018, but rebuilt and relaunched a year later. The DCRat backdoor appears to be the product of a single threat actor who goes online with the pseudonyms of “boldenis44,” “crystalcoder,” and Кодер (“Coder”).

DCRat is one of the cheapest commercial RATs. For a two-month membership, the price starts at 500 RUB (less than 5 GBP/US$6), and it periodically drops even cheaper during special offers. This is written in .NET and features a modular structure, allowing affiliates to create their own plugins using DCRat Studio, a dedicated integrated development environment (IDE).

The malware’s modular architecture allows it to be extended for a variety of nefarious objectives, including surveillance, reconnaissance, data theft, DDoS attacks, and arbitrary code execution.

The DCRat consists of three parts:

- A stealer/client executable
- The command-and-control (C2) endpoint/ interface is a single PHP page
- An administrator tool

The malware is still in development, the author announces any news and updates through a dedicated Telegram channel with about 3k users updated with any news and changes.

Impact

- Unauthorized Remote Access
- Keylogging
- Information Theft
- Password Theft

Indicators of Compromise

MD5

- 48f2b82b6457a1236a57e3d6a2919368

SHA-256

- 4755b33855dc2b701833bebb32d8548deeae802c9b0c044691236e4734755d68

SHA-1

- 0105771d9226ebe1eaaf34d30b70707402a70ed1

Remediation

- Block the threat indicators at their respective controls.
- Search for IOCs in your environment.