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

Domain Name

- dcrat[.]ru
- crystalfiles[.]ru

MD5

- 15a1eb360159ae7906efb9562ee664cb
- 29fb61de3e11e1db3e65ca5fdef6e542
- 8a1764d0affe8740407b93040fc639d4
- 89bf0f7e9adf290c6d571eccf79206a9
- aa84f91edd922e7b3bb979e663c94f1a
- 569052631a6b80c1c6a336c10c978b02
- 9a2ea4da5eec75298f16ba444d3a98d6
- 0b4dbf61a98f3e34cdd3a1b08a6a4609
- bbc5441ecd131f5a98dff8be2ebc5294
- e8b39f250fb67e115e07e9eac5c99708

SHA-256

- 6014d44d8f7da00f03db051b3dcea9a03ec3837977118c69a4512ef558a6df2a

- 914cca033fc8ca52830a21b5dca55263cee1e74ab5571702906ee9c25aedafd7
- 812cd4b5e80bc4e83a2e01a6f3fb24346ecf57dcaf8ff6fc3e55a2a6b953da23
- b11ad1adfa96eacf5f18cf87785884947a6d35a1baebf4f20f16402b04d5109f
- 38274608d5a4b53ec22f8099f798ba46ce0ed41db65a33dfb3853f0dbf849f6f
- c41cd461470ff3c936e225cea37e5190cb06e3cd70a3d76ca8e5d3aceead5493
- 2293fe261d5c6f5f2a33004b11f068037677b7aa5a6f792031e31555f31f0d69
- e817802f166662a7df0b144571354d74b10e34d120f91ae9d84ca3ba925241c6
- 78684aea83b1a5c402a87ba0ce2e7ad5b0338462cc804e97369203ce53d29834
- d634cde09d1aa1320a1d4c589d35d306f8350129faf225b2bca394128c2c4442

SHA-1

- a229e40ceaa5d9f18d0e2fd9040caaa7330457f0
- 7101c467e214e39cebb281e98e8009b3f64ec411
- ea4e4925abf5d7d2e7488850efe8cecaaf8471ea
- 65f95791234ff93bc3e35f1d35d7a6664872dc56
- da46b9962a6c6cceef38c3e11b8b5bc9c1b536fa
- 4bc411b19536c90a6ea0917d7d93f3f6560ee6f0
- f4f790430556e36d418498cd2f3112d04dabf877
- 73587f1f5d040541b230513d22d696513dbd4cf9
- f90e309443dc760359e69102f366496a53c307d8
- 51bf6ab0baa3a4c6f45be46011baa8ccd7ceaf8f

Remediation

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