DarkCrystal RAT - Hackers Selling Commercial Backdoor on Russian Hacking Forums

By Guru Baran

Published: 2022-05-10 · Archived: 2026-04-05 21:11:18 UTC

Security researchers at BlackBerry have recently reported a new RAT dubbed DarkCrystal RAT (also known as DCRat), and it's a specifically designed and actively maintained RAT.

A large number of cybercriminal groups are offering this RAT for dirt cheap prices. This means that it is widely accessible to both professional criminal groups and beginners as well.

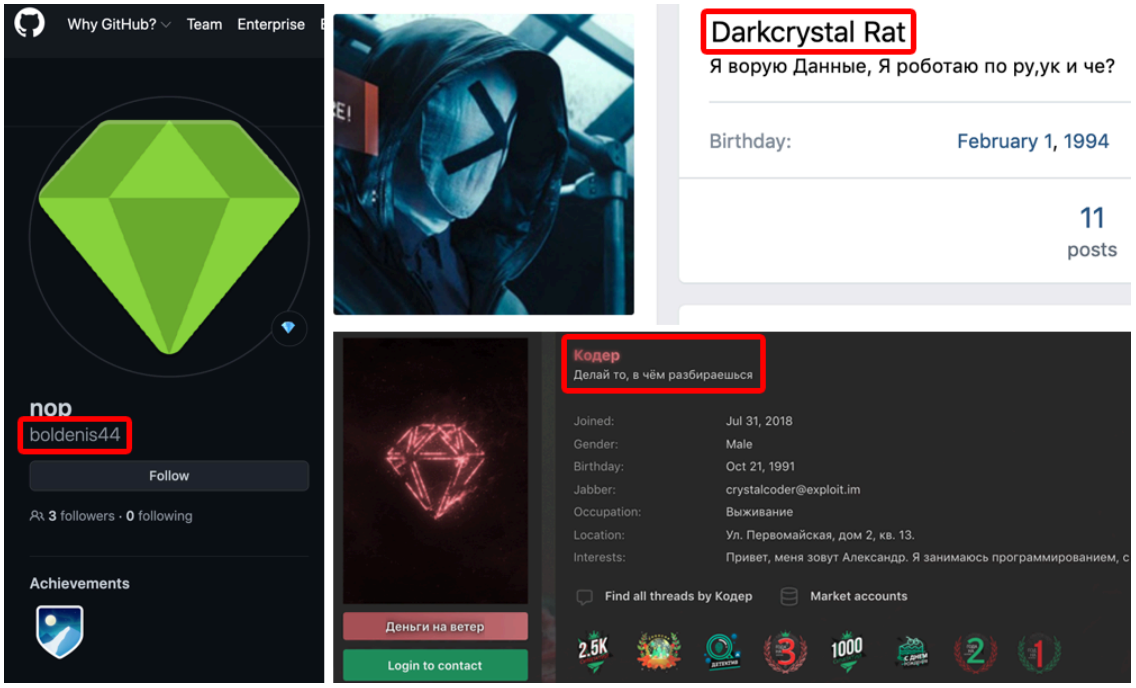
In spite of the fact that this remote access Trojan (RAT) appears to have been created by just one individual, it provides an impressively effective handmade tool for gaining access to systems on a low budget.

A two-month subscription to this backdoor would cost you about 500 Rubles which is less than 5 pounds or 6 dollars. When special promotions are running, the price can sometimes dip even lower.

It is evident that the author is not particularly motivated by profits, which makes the price range a curious feature.

DCRat was initially released in 2018, and it is a commercial Russian backdoor that is redesigned and relaunched a year later. A single person appears to be behind the development and maintenance of this threat using the pseudonyms presented below:-

- boldenis44
- crystalcoder
- Кодер



Components of DCRat

In total, the DCRat product contains three components, and here below we have mentioned all the three components of DCRat:-

- A stealer/client executable
- A single PHP page, serving as the command-and-control (C2) endpoint/interface
- An administrator tool

DCRat (aka DarkCrystal RAT)

DCRat is a full-featured backdoor that is written in .NET. With DCRat, third-parties can develop plugins to extend the functionality of the tool further, which can be completed by using a dedicated IDE called DCRat Studio, developed by affiliates.

The flexibility of DCRat's modular architecture and custom plug-in framework makes it exceptionally handy for use in a range of nefarious activities.

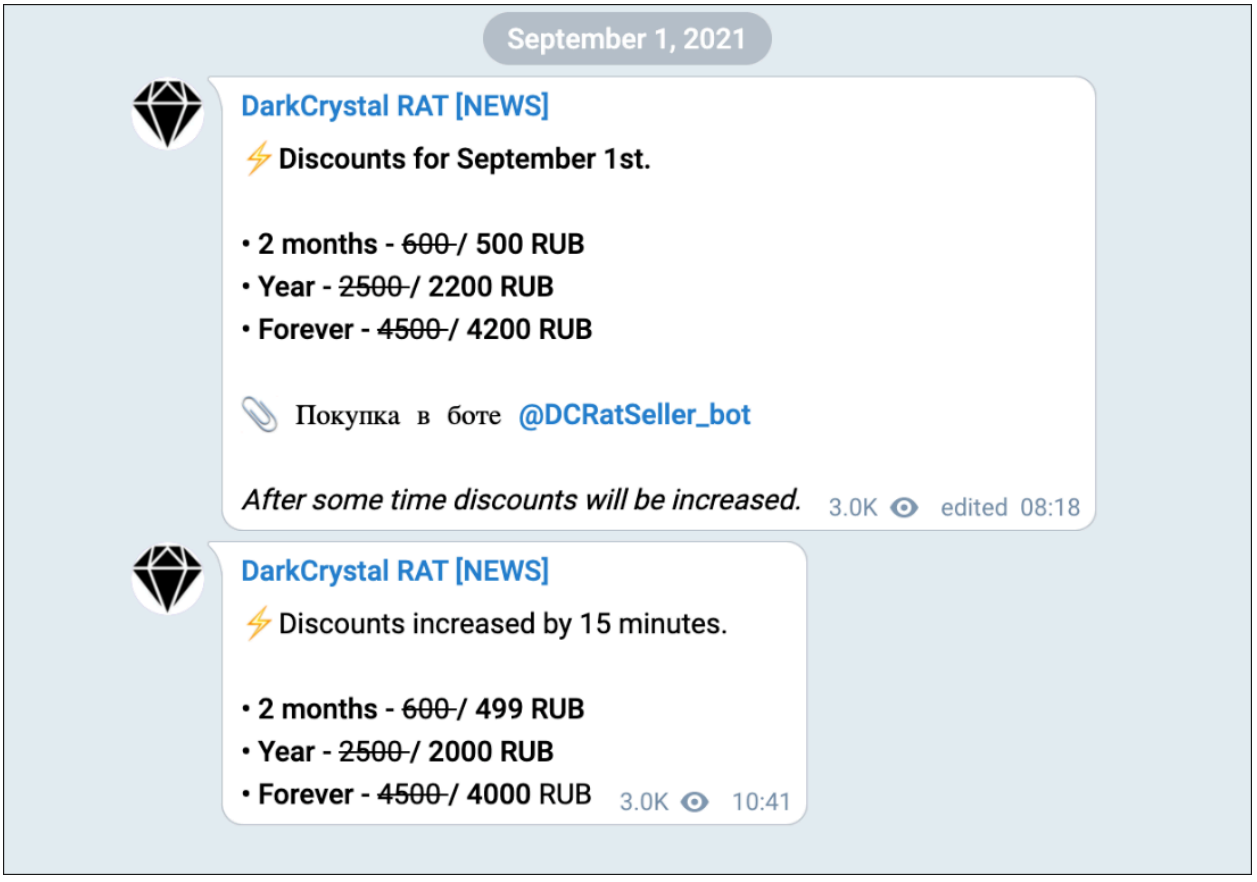
This includes the following things:-

- Surveillance
- Reconnaissance
- Information theft
- DDoS attacks
- Dynamic code execution

Price chart

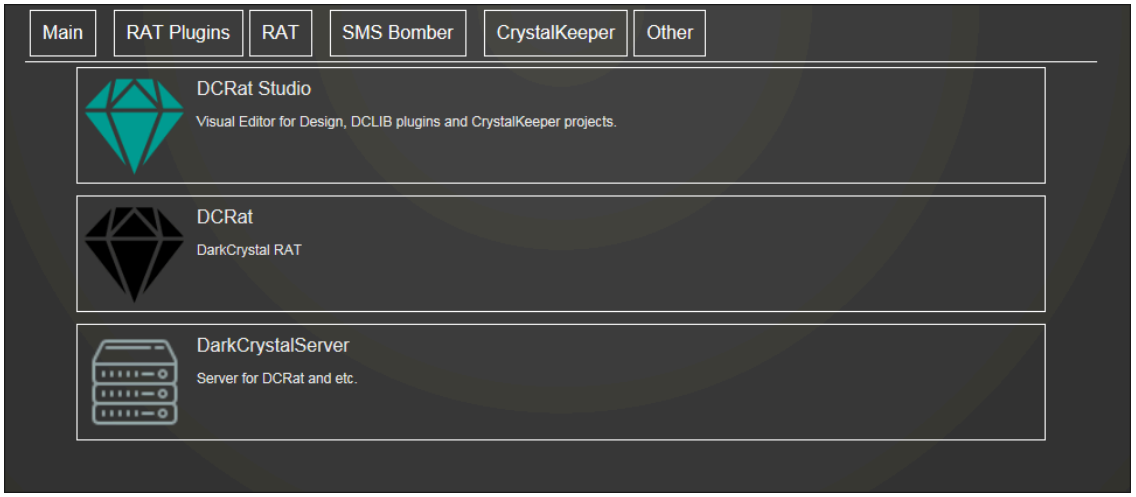
A two-month license for the trojan starts at 500 RUB ($5), which is the general price for the trojan's general use. While the further prices are mentioned below:-

- Two-month subscription: 500 RUB ($5)
- One year subscription: 2,200 RUB ($21)
- Lifetime subscription: 4,200 RUB ($40)



DCRat Offering

Mandiant conducted an analysis in May 2020 which traced RAT's host infrastructure on "files.dcrat[.]ru" but at present, the malware is hosted on a domain called "crystalfiles[.]ru" which is a different domain.



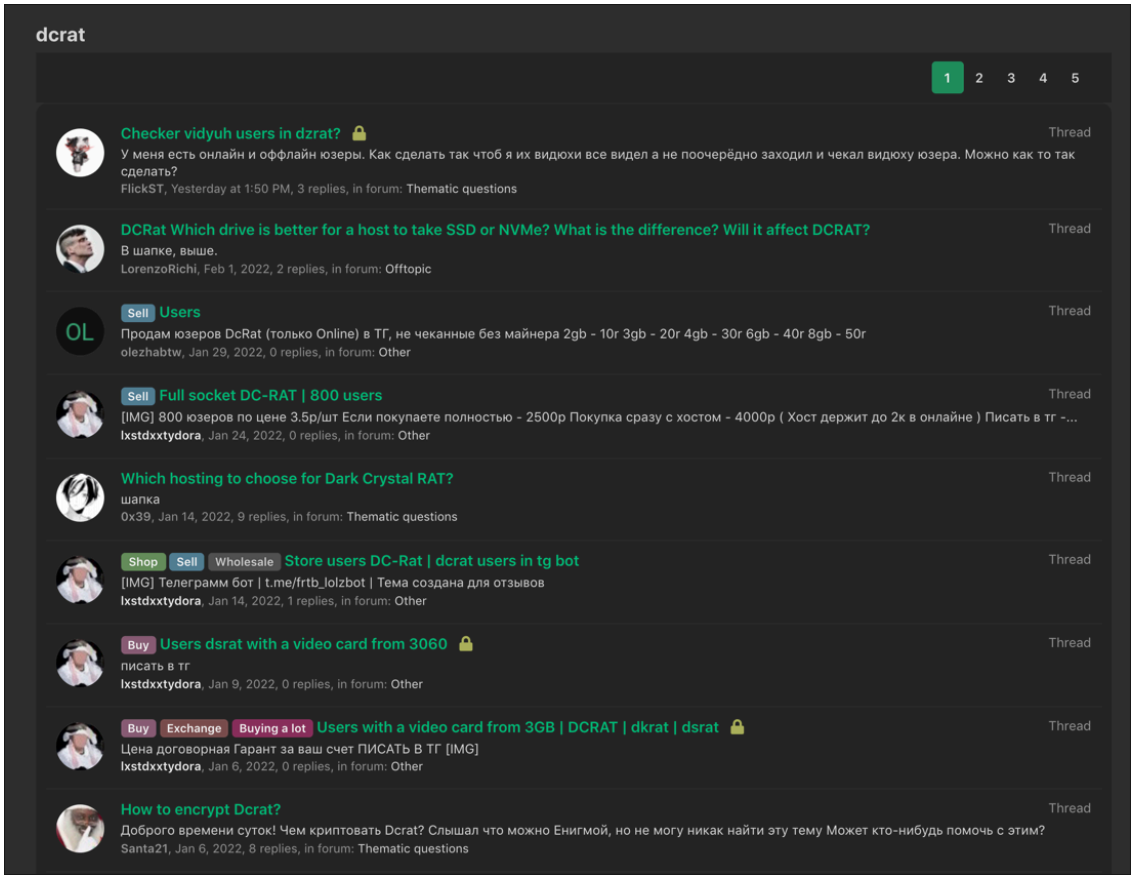
There is no real complex interface on the crystalfiles website and the website is intended to serve as a download point only. Further, clients and potential clients will find no other information or resources on the site.

Among the vectors that DCRat uses to spread throughout a host are:-

- Cobalt Strike Beacons
- Prometheus TDS (A subscription-based crimeware-as-a-service (CaaS) solution.)

Moreover, the further capabilities of this RAT include:-

- Capturing screenshots
- Recording keystrokes
- Stealing content from the clipboard
- Stealing data from Telegram & web browsers



Apart from this, it is the Russian hacking forum lolz[.]guru through which all DCRat marketing and sales activity is carried out. In addition, there are some pre-sales queries that are handled by this same portal.

You can follow us on Linkedin, Twitter, Facebook for daily Cybersecurity and hacking news updates.

Source: https://cybersecuritynews.com/darkcrystal-rat/