ThreatCure

Cyber Threat Advisory

DarkCrystal RAT

Threat Actor Malware

Description

DarkCrystal RAT (DCRat)

CATEGORY

Malware

SEVERITY

High

Platforms

Windows, Linux

IMPACT

- Unapproved system access
- Capturing keystrokes
- Theft of confidential data
- Stealing user credentials

DCRat, also known as DarkCrystal RAT, is a Russian backdoor malware that first emerged in 2018 and was later rebuilt and relaunched in 2019. Created by a single threat actor using aliases like "boldenis44" and "crystalcoder," DCRat is among the most affordable commercial Remote Access Trojans (RATs), with prices starting at 500 RUB (less than $6). Written in .NET, the malware's modular architecture enables affiliates to develop custom plugins using its dedicated integrated development environment, DCRat Studio. This modularity supports a range of malicious activities, including data theft, surveillance, DDoS attacks, and executing arbitrary code. DCRat comprises three components: a client executable for stealing data, a PHP-based command-and-control (C2) interface, and an administrator tool. The malware's author communicates updates through a Telegram channel with approximately 3,000 subscribers.

To mitigate risks posed by DCRat and similar malware, maintaining up-to-date software, implementing multi-factor authentication, and exercising caution with emails and attachments are critical. Regular backups, antivirus software, and awareness of infection signs, such as unusual system behavior or slow performance, are also essential. In the event of suspected infection, isolating the affected system and seeking professional help are necessary steps to prevent further damage and ensure proper remediation.

Indicator of Compromise

SHA-256

- 46cf8f5e46c3dbdd32c5f300f6fd395a7f12c0ec611de9e518bf7312f187590c
- 765a4d3d78bfe581a988e5a2934671b045e989afd02b995000325c347b16fa5e
- d169e5e99edef6f5c3619faee33bddd20978f514bdc3448b8655fd06ea5f5984
- 0a0eebfca8553e921339c90b0060ceb6adcbc5f747696b1abecd376f50283911
- 91a5d06a6ddc1dbc0d573871082b21c0ef5d260987d760bff9b1d19966d0c32d
- 46f77240e4a469bf38e0600e95edf6de249ede13f5a41de3702af584a69b7761

MD5

- 02d4afb627db486201d4700854e390d9
- 79893ef0d65e23527017d1f9feaf0331
- 183cb9283d9c8f6282283bd39f49d33c
- dabf40b2ed8d96638f713f6373ef64cb
- d49f9a9a6f4d5c60ae2c35aafe7d105a
- bae83c597a9f76e1a42b833f108c8c9a

Remediation

- Keep all software and systems updated.
- Use multi-factor authentication (MFA).
- Regularly back up critical data.
- Install and maintain antivirus/antimalware tools.
- Avoid opening suspicious emails or attachments.
- Monitor systems for unusual activity.
- Isolate infected devices immediately.
- Seek professional assistance for cleanup and recovery

ThreatCure

Cyber Threat Advisory

Secure your byte world

DarkCrystal RAT

Threat Actor Malware

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE