I. INTRODUCTION

DCRat, also known as Dark Crystal Rat, is a commercial backdoor that is predominantly sold on underground forums. It has been around since 2018 and operates as a modular remote access trojan (RAT) offered as a Malware-as-a-Service (MaaS). The malware is designed to provide threat actors unauthorized access to systems by circumventing security measures.

In terms of pricing, DCRat is sold for approximately $7 for a two-month subscription. Its one-month license goes for a mere $5, while a lifetime use license costs $40. Despite its low cost, DCRat is a versatile and dangerous cybersecurity threat.

In 2022, DCRat's developer announced on their GitHub page that the it would be discontinued, along with a link to its successor and a claim the new source code would remain private and not sold.

II. DCRAT FEATURES

DCRat is a modular remote access trojan (RAT) with a range of features that make it a versatile tool.

The DCRat product itself consists of three components: a stealer/client executable, a single PHP page serving as the C2 endpoint/interface, and an administrator tool. It uses a modular framework that deploys separate executables for each module, most of which are compiled .net binaries programmed in C#.

DCRat is capable of a range of nefarious uses, including surveillance, reconnaissance, information theft, Distributed Denial of Service (DDoS) attacks, and dynamic code execution in a variety of different languages. It can also steal credentials used to login to social media accounts, specifically Telegram and Discord. DCRat has been detected targeting Windows systems, with a specific focus on bypassing security safeguards.

As of 2023, DCRat has been updated with several new capabilities and features:

- **CryptoStealer** Module: This module allows attackers to access users' cryptocurrency wallets
- **Dynamic Code Execution**: DCRat can execute code in multiple programming languages
- **Crypto-Mining**: Instances of DCRat deploying crypto-mining software on victim endpoints have been documented
- **Delivery Methods**: DCRat has been disseminated through enticing adult content-themed baits, infected files, and network propagation
- **Evasion Techniques**: DCRat has been observed to evade sandbox environments that use fake internet to spoof internet connection for malware analysis
- **Persistence**: DCRat has been found to exploit a zero-day vulnerability in the Microsoft support diagnostic tool (MSDT), CVE-2022-30190 (Follina), to maintain persistence on the infected machine

As of 2023, DCRat has the following key features (**full list**):

- Information Theft
- Surveillance and Control
- Disruptive Attack Capabilities
- Modularity and Customization
- System Interaction
- Administration and Control
- Deployment and Distribution
- Stealth and Evasion

A. *Information Theft*

- **Information Theft**: DCRat can steal sensitive data from victimized systems, including capturing screenshots, harvesting clipboard data
- **Keylogging**: It can log keystrokes to capture sensitive information like passwords
- **Stealing Browser Data**: DCRat can extract session cookies, auto-fill credentials, personal information, and credit card details from browsers
- **Clipboard Data Harvesting**: It can copy and steal the contents of the user's clipboard
- **Credential Theft**: The malware can steal credentials from popular FTP applications and social media accounts, particularly targeting Telegram and Discord

B. *Surveillance and Control*

- **Screenshots**: It can take screenshots to monitor user activity
- **System Information Collection**: DCRat collects system information such as CPU and GPU stats, hostname, usernames, language preferences, and installed applications

C. *Disruptive Attack Capabilities*

- **DDoS Attacks**: DCRat can launch Distributed Denial of Service (DDoS) attacks against selected targets
- **Dynamic Code Execution**: It offers the ability to execute code dynamically in multiple programming languages

D. *Modularity and Customization*

- **Modular Architecture**: DCRat uses a modular framework, deploying separate executables for each module, most of which are compiled .NET binaries programmed in C#
- **Plugin Framework**: It has a plugin development framework that allows for the creation of new modules, enhancing its capabilities

E. *System Interaction*

- **Persistence**: DCRat can persist on compromised hosts using techniques such as creating scheduled tasks, Registry Run Keys, and Winlogon Autostart Registry Keys
- **Crypto-Mining**: There have been instances where DCRat deployed crypto-mining software on victim endpoints

F. *Administration and Control*

- **C2 Administration**: The malware includes a command-and-control (C2) administration interface that allows attackers to upload modules, execute commands remotely, and exfiltrate data
- **Stealer/Client Executable**: It consists of a .NET executable designed to exploit Windows systems

G. *Deployment and Distribution*

- **Malware-as-a-Service (MaaS)**: DCRat operates as a MaaS, allowing it to be purchased and used by various threat actors
- **Low-Cost Licenses**: It is sold for approximately $7 for a two-month subscription, with other pricing options available for longer-term use

H. *Stealth and Evasion*

- **Concealment**: DCRat employs techniques to stay undetectable, such as hiding its presence and disguising its network traffic
- **Anti-Detection Features**: Plugins are available that can resist running in a virtual machine, disable Windows Defender, and disable webcam lights on certain models
- **Persistence Mechanisms**: It can use techniques like creating scheduled tasks, Registry Run Keys (incl. Winlogon Autostart) to maintain its hold on the system

III. DCRat Deployment

DCRat operates as a Malware-as-a-Service (MaaS). DCRat is deployed via first-stage attacks employing a wide array of tactics, including malspam, phishing, spear-phishing, and pirated (or “cracked”) commercial software such as rogue updaters and anti-virus products.

Once installed, the DCRat C2 administration allows attackers to upload modules to the infected host, execute commands remotely, and exfiltrate data. DCRat uses a modular framework that deploys separate executables for each module, most of which are compiled .net binaries programmed in C#. The malware is capable of stealing information from browsers, such as session cookies, auto-fill credentials, personal information, and credit card details. It can also monitor the infected host by logging and exfiltrating keystrokes and screenshots.

DCRat establishes a connection between the victim's device and the attacker's device through a command-and-control (C2) server. Once the malware is installed on the victim's device, it connects back to the C2 server controlled by the attacker. This server can send commands to the compromised device, allowing the attacker to access and modify data, steal sensitive information, and ensure persistence by reconnecting to the C2 server even after reboots or attempts to remove the malware.

The most common lures used to distribute DCRat include:

- **Adult Content-Themed Lures and Fake OnlyFans**: DCRat has been distributed using explicit lures related to OnlyFans pages and other adult content. Victims are tricked into downloading malicious files, often ZIP archives, which contain the malware
- **Phishing and Malspam**: DCRat is also spread through phishing emails and malspam campaigns, where victims receive emails with malicious attachments or links that, when opened, install the malware
- **Network Propagation**: The malware can spread through network propagation, exploiting vulnerabilities or using other methods to move laterally within a network and infect multiple devices

IV. DCRat Evade techniques

DCRat employ several techniques to evade detection:

- **Process Infiltration**: DCRat rarely produces malicious activity in its current process. Instead, it prefers to create large process trees and infiltrate a harmless process at some point
- **Persistence Algorithm**: DCRat can execute a persistence algorithm to retain control over the system. For instance, it can copy itself to a random running process and to the root directory. It can also create shortcuts to these copies in the user's Startup folder and add registry values that point to these shortcuts
- **Delay Execution**: DCRat can delay execution for a period of time after the infection, which can help it evade immediate detection
- **Obfuscation**: DCRat's payload has been protected with Enigma Protector to prevent analysis
- **Use of SSL/TLS Certificates**: DCRat, like many other malware families, uses self-signed SSL/TLS certificates, which can help it blend in with normal encrypted traffic and evade detection

V. DCRat Effectiveness

DCRat is known for its cost-effectiveness, versatility, and continuous updates, which make it a significant cybersecurity threat. DCRat allows threat actors to take control over an infected machine and steal sensitive information such as clipboard contents and personal credentials from apps. DCRat is developed and maintained by a single user who actively markets their product on several underground forums as well as a Telegram channel. This is unlike most other RATs, which are typically the work of sophisticated and well-resourced cyber-criminal groups.

DCRat differs from other RATs in several ways. It can also function as a loader, dropping other types of malware on the infected computer. DCRat uses three distinct techniques for persistence on the compromised host: creating a scheduled task, creating a Registry Run Key, and creating a Winlogon Autostart Registry Key. It also uses the W32tm "stripchart" command as a delay tactic for its execution and beaconing, which is not commonly used by other RATs.

In terms of effectiveness, DCRat is surprisingly effective despite its low cost. The malware is under active development, with new capabilities being added regularly. It is also capable of evading detection by security software, making it a potent cybersecurity threat.

The most common features of other remote access trojans include the ability to establish complete to partial control over infected computers, the capability to spawn a child process, and the use of the Task Scheduler to ensure persistence within the compromised system. They can also exfiltrate sensitive information, establishing connections with command and control (C2) servers. Some RATs, like njRAT, operate on the .NET framework and enable hackers to remotely control a victim's PC, giving them access to the webcam, keystrokes, and passwords stored in web browsers and desktop apps.

VI. DCRat Detection

A. *Common IoC's features*

The most common indicators of compromise (IOCs) for DCRat attacks relate to the following features:

- Monitoring the infected host by logging and exfiltrating keystrokes and screenshots
- Stealing information from browsers, such as session cookies, auto-fill credentials, personal information, and credit card details, including popular FTP applications
- The ability to record the victim's keystrokes, which can be used to steal passwords and other sensitive information
- The ability to collect information about the system (CPU and GPU stats, etc.)

B. *Network IoC's features*

The most common indicators of compromise (IOCs) for DCRat attacks relate to the following networks features:

- **Network Traffic**: DCRat communicates with its Command & Control (C2) server to exfiltrate data and receive commands. This communication can be detected as unusual network traffic
- **Data Collection**: DCRat collects sensitive information from compromised hosts, such as server type, username, and GPU info, which can be detected by monitoring for unusual data access or movement
- **Persistence Mechanisms**: DCRat uses several techniques for persistence, including creating a scheduled task, creating a Registry Run Key, and creating a Winlogon Autostart Registry Key. These entries can be detected by monitoring for changes in the system's scheduled tasks, registry, and startup processes
- **DDoS Attacks**: DCRat can orchestrate Distributed Denial of Service (DDoS) attacks against targeted websites. This can be detected by monitoring for unusual network traffic patterns or an increase in requests to a specific website
- **Dynamic Code Execution**: DCRat has the ability to execute code in multiple programming languages. This can be detected by monitoring for unusual code execution or process behavior
- **Information Theft**: DCRat can facilitate the theft of sensitive data from victim devices, including capturing screenshots and harvesting credentials. This can be detected by monitoring for unusual data access
- **Crypto-Mining**: Instances of DCRat deploying crypto-mining software on victim endpoints have been documented. This can be detected by monitoring for unusual CPU usage or network traffic