ChaosRAT

Target Bio

Names/Alias: chaosRAT
Source Code: Go (58%), HTML (23%), JavaScript (19%)
Purpose: To allow attackers to execute commands, steal data and control machines remotely
First Activity: November 2022
Targets: ChaosRAT targets Windows and Linux systems through a multi-stage infection process.
Most Recent Development: The most recent variants of chaosRAT have been in use as of June 2025

BLUF

ChaosRAT is a cross-platform, open-source remote administration tool (RAT) turned malware modified for cyber espionage, data exfiltration, remote system control and other malicious operations. With the ability to compromise multiple OS's, ChaosRAT poses a serious threat capable of endangering organizations across almost every sector.

Background

Originally developed as a remote administration tool in 2017, ChaosRAT has since been weaponized to enable unauthorized remote access, data exfiltration, and payload execution on compromised hosts [1][2][6][7]. Attackers frequently leverage the '/etc/crontab' directory - part of the Linux scheduling system that automatically runs tasks at set intervals – to gain persistence and maintain long-term access [1][2][3][6]. Once inside, ChaosRAT is exceptionally difficult to detect. Its high degree of customizability further enhances its resilience, allowing operators to adapt the tool to evade evolving detection methods across targeted devices and servers [1][2].

Summary (General Overview)

ChaosRAT typically gains its initial foothold through phishing emails containing malicious links or attachments. Once a victim interacts with them, the malware deploys a lightweight script that modifies a commonly exploited task manager via the /etc/crontab file to establish persistence [1][2][5][6]. With persistence in place, attackers can continue delivering malicious payloads without further manual interaction. After full deployment, ChaosRAT activates multiple layers of obfuscation, such as encoded strings and dynamic API resolution, to evade detection, while also performing environmental awareness checks, including virtual environment detection, to ensure execution only occurs under favorable conditions [3][4][5]. Another key advantage of ChaosRAT is its built-in communication channel with its command-and-control (C2) server, sending JSON-formatted updates approximately every 30 seconds that include system details like operating system information, IP and MAC addresses, and system architecture. This continuous flow of reconnaissance data enables attackers to maintain awareness of the compromised environment and remotely execute malicious commands as needed [2][7].

Details & References

Analysis Summary

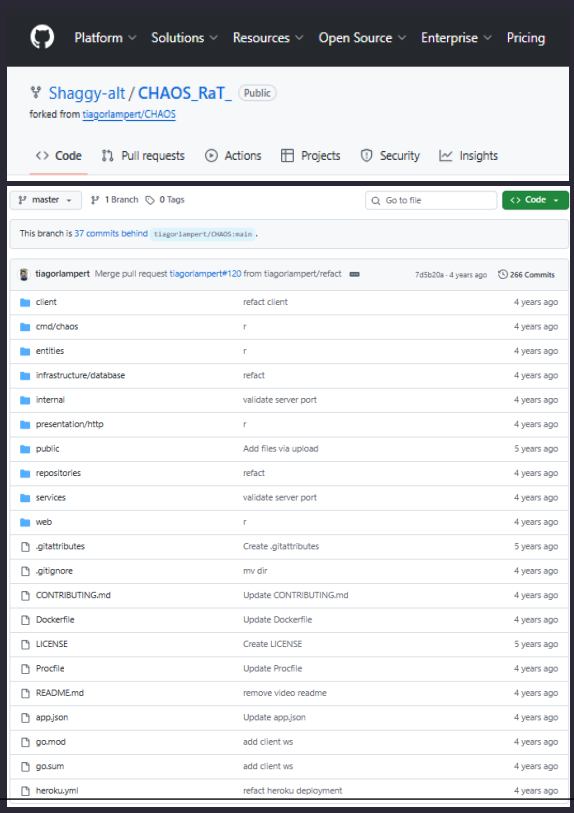
ChaosRAT's ability to remotely execute commands, extract files, perform reconnaissance, etc. makes it a valuable tool for malicious actors. ChaosRATs high adaptability, low detection rate, and multi-function capability it grants attackers makes it stand out from other RAT's, making it a highly effective and dangerous tool in the hands of attackers [1][2][3].

The tools cross compatibility across multiple operating systems, deriving from the tools source code in Go, adds a high degree of versatility to the tool, in addition to its ability to persist on a targets systems [1][2][5][7]. These features, combined with the high degree of customizability stated above, make the tool incredibly useful to threat actors. As a result, the popularity of this tool is likely to continue increasing and will continue receiving newer, more dangerous versions that give attackers more tools and capabilities than previous models.

Adding to the strengths of ChaosRAT listed, the greatest strength of ChaosRAT is the free and open-source nature, which grants ease-of-access and a low-risk high reward incentive surrounding the tool. This means that the cost barrier to entry is non-existent, giving potential attackers of widely varying skill and experience levels access.

Because the primary delivery method of chaosRAT is phishing emails, the best way to combat it is going to be advanced email filtering and proper employee training. [1][2][3][5] Phishing identification (the ability to identifying which emails are real or phishing) is a skill that every organization should emphasize, as this will be the most effective mitigation tool. Other technical preventions can and should also be taken; For example: Implementing endpoint detection and response (EDR), continuously monitoring network traffic, restricting administrative privileges, and patching vulnerabilities quickly are all great security practices that will protect systems against chaosRAT [1][2][3][5][6][7].

ChaosRAT GitHub Repository



Source: GitHub - Shaggy-alt/CHAOS_RaT_ : :fire: CHAOS is a

References

[1] Chaos RAT Malware Targets Windows and Linux via Fake Network Tool Downloads

[2] From open-source to open threat: Tracking Chaos RAT's evolution

[3] Chaos RAT MalwarVariant Distributed via Fake Linux Network Tools | Black Hat Ethical Hacking

[4] Chaos RAT Malware Targets Linux Systems: Tactics and Defense

[5] Threat Advisory – hivepro

[6] https://cybersecuritynews.com/new-variants-of-chaos-rat-attacking-windows-and-linux-systems/

[7] https://hunt.io/malware-families/chaos-rat