What Is The Venom RAT? A Detailed Explanation of this remote access tool | Threat Intelligence | CloudSEK

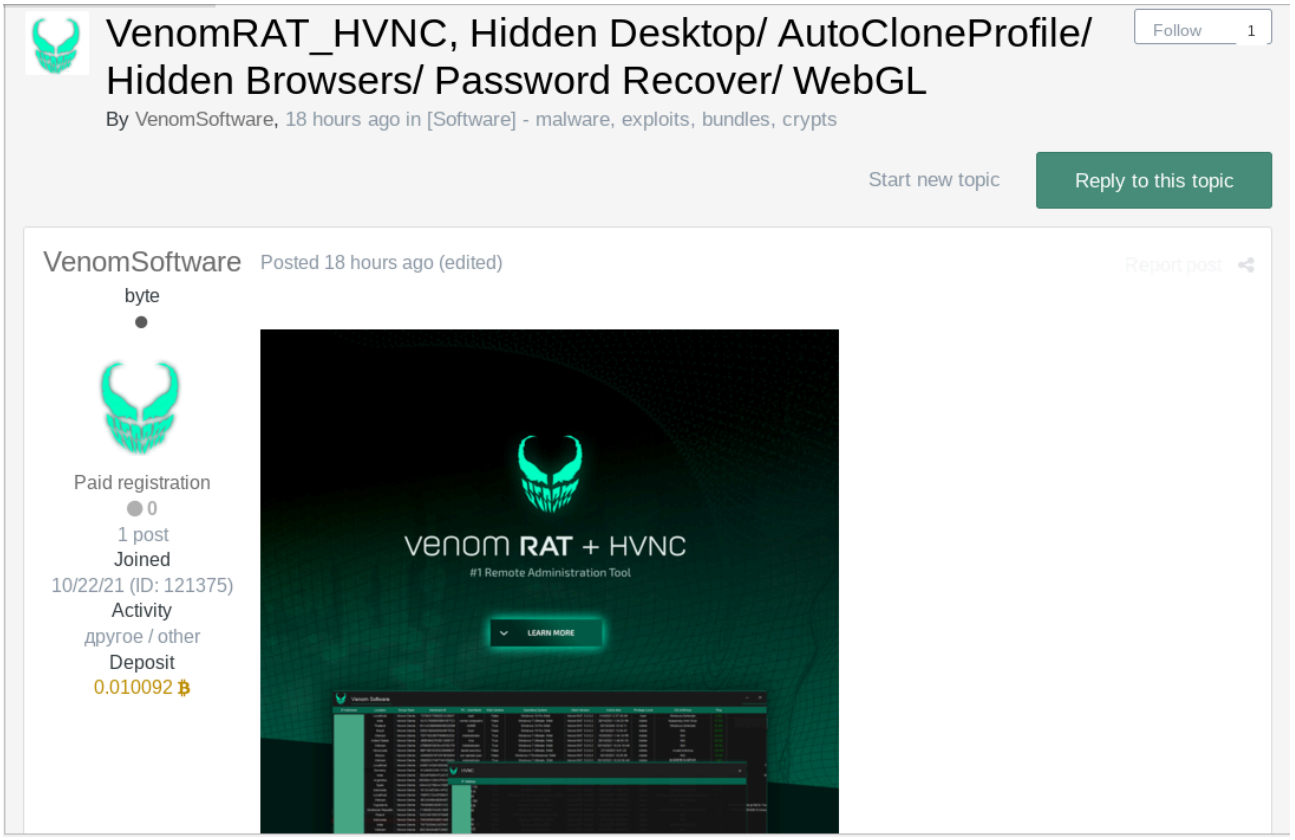
Archived: 2026-04-05 19:55:08 UTC

Executive Summary

- CloudSEK's flagship digital risk monitoring platform XVigil discovered a post, on a cybercrime forum, advertising VenomRAT.
- VenomRAT is a remote access tool discovered by 2020, and it is used by threat actors to control the infected systems remotely.

Category	Adversary Intelligence
Affected Industries	Multiple
Affected Region	Global
Source*	C2
TLP#	**Green**
Reference	*https://en.wikipedia.org/wiki/Intelligence_source_and_information_reliability #https://en.wikipedia.org/wiki/Traffic_Light_Protocol

[caption id="attachment_18224" align="aligncenter" width="1090"]



VenomRAT - Threat actor’s post on the cybercrime forum[/caption]

Analysis and Attribution

Information from the Post

The threat actor has listed two versions of the RAT, the second version of the RAT includes HVNC (Hidden Virtual Network Connection).

1. Features of the RAT include:

- Connect with the system remotely.
- Get the system information
- Remote Shell
- TCP Connection
- Reverse Proxy
- Registry Editor
- UAC (User Access Control) Exploit
- Disable WD (Windows Defender)
- Format All Drivers
- Change client name
- Enable install
- Anti kill
- Hide file

- Hide folder
- Persist on the system as startup / persistence
- Change registry name
- Encrypted connection
- Enable keylogger Offline/Online

2. VenomRAT with HVNC

- HVNC Features, Included all the features of the Venom RAT
- HVNC Clone Profile
- Hidden Desktop
- Hidden Browsers
- Support WebGL
- Hidden Chrome, Firefox, Edge, Brave
- Hidden Explorer
- Hidden Powershell
- Hidden Startup
- Reverse Connection
- Remote Download+ Execute

This RAT was discovered by 2020, and based on open-source research this RAT is built on top of QuasarRAT which is an open-source legit tool used as a Remote Access Tool.

Source Rating

- The threat actor joined in October 2021 and has a deposit on the forum 0.010092 BTC.
- The main activity of the threat actor is related to advertising for VenomRAT.

Hence,

- The reliability of the actor can be rated **Fairly reliable** (C).
- The credibility of the advertisement can be rated **Probably true** (2).
- Giving overall source credibility of **C2.**

Impact & Mitigation

Impact	Mitigation
• This type of malware gives the attackers the ability to control the victim machine and wreak havoc in the system.	• Avoid downloading suspicious documents from unknown sources. • Avoid clicking on suspicious links. • Enable the visibility of files extensions, and have a vigil eye on the file

	extensions. • Update the system and all the applications to the latest patches and updates. • Ensure the usage of MFA. • Use up-to-date antivirus and anomaly detection tools. • Use updated EDR solutions that help in monitoring the network.
