PureRAT = ResolverRAT = PureHVNC

By Erik Hjelmvik

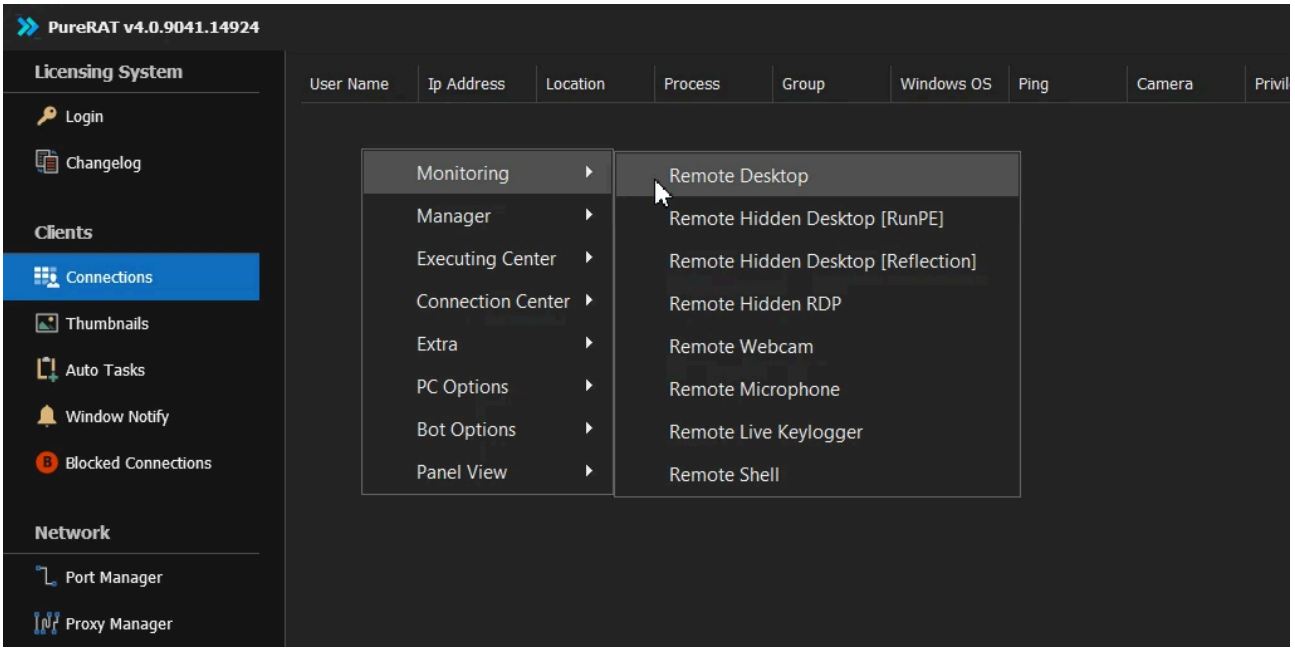
Published: 2025-08-12 · Archived: 2026-04-05 22:46:10 UTC

,

Tuesday, 12 August 2025 15:43:00 (UTC/GMT)

PureRAT is a Remote Access Trojan, which can be used by an attacker to remotely control someone else's PC. PureRAT provides the following features to an attacker:

- See the victims user interface
- Interact with the victim PC using mouse and keyboard
- View the webcam
- Listen to the microphone
- Record keystrokes
- Upload and download files
- Proxy network traffic through victim



What the PureRAT user interface looks like to the attacker

PureRAT is the exact same malware as what Morphisec and others call ResolverRAT. PureHVNC, on the other hand, is the predecessor to PureRAT. These three malware names are all used by threat intel companies and researchers when referring to the same malware family. We will call this malware family "PureRAT" in this blog post.

Indicators of PureRAT

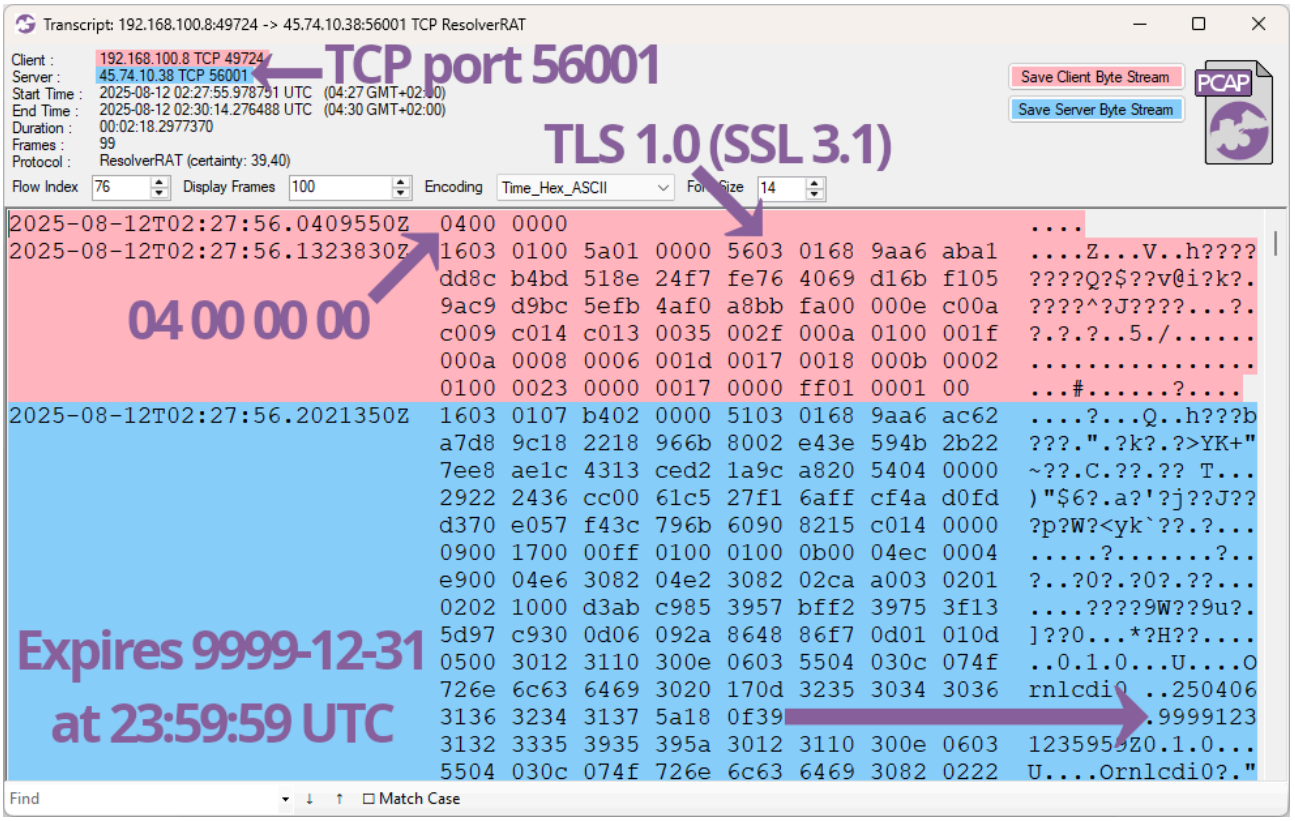
Malware analysts might recognize PureRAT through properties like these ones:

- Loader is a .NET executable obfuscated with Eazfuscator.NET
- Payload is AES-256 encrypted in CBC mode
- Payload is gzip compressed
- Extracted PureRAT payload is a DLL
- PureRAT DLL is packed with .NET Reactor
- A handler is registered for the ResourceResolve event to inject a malicious .NET assembly

See analysis by eSentire, Morphisec, Kaspersky, Fortinet and 0xlibris for more reverse engineering details on PureRAT and related software from the PureCoder developer(s).

Another way to identify the malware is to run it in a sandbox and inspect the network traffic. The following characteristics are typical indicators of PureRAT:

- C2 TCP port is often 56001, 56002 or 56003
- Client (bot) first sends 04 00 00 00 (in hex), followed by a TLS handshake
- Client and server run TLS 1.0
- X.509 cert is self signed
- X.509 cert expires 9999-12-31 23:59:59 UTC



As you can see in the flow transcript above, CapLoader currently identifies this traffic as “ResolverRAT”. This detection will most likely be changed to “PureRAT” in future versions of CapLoader.

IOC List

Here are some IP:port tuples for C2 servers used by recent samples of PureRAT:

- 193.26.115.125:8883
- purebase.ddns[.]net:8883
- 45.74.10.38:56001
- 139.99.83.25:56001

Posted by Erik Hjelmvik on Tuesday, 12 August 2025 15:43:00 (UTC/GMT)

Tags: #PureCoder

Short URL: https://netresec.com/?b=2589522
