

PureRAT = ResolverRAT = PureHVNC

By Erik Hjelmvik

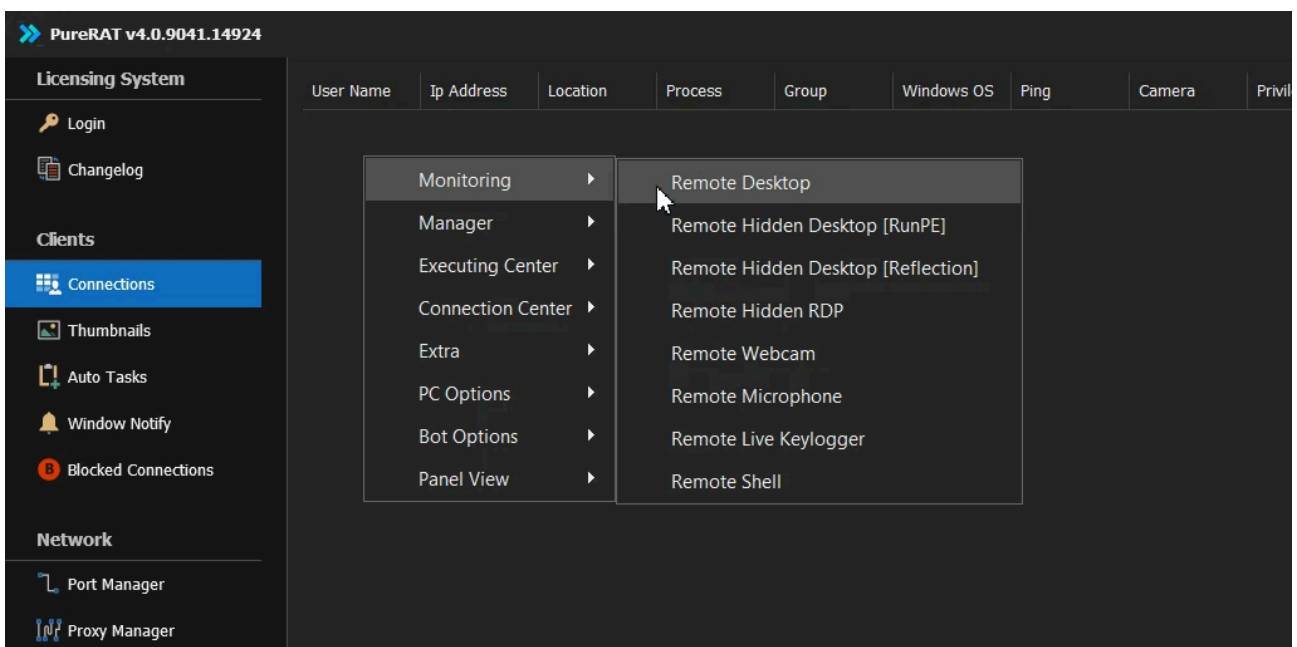
Published: 2025-08-12 · Archived: 2026-04-05 22:46:10 UTC

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 [Oxlibris](#) 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

Transcript: 192.168.100.8:49724 -> 45.74.10.38:56001 TCP ResolverRAT

Client : 192.168.100.8 TCP 49724
Server : 45.74.10.38 TCP 56001
Start Time : 2025-08-12 02:27:55.978751 UTC (04:27 GMT+02:00)
End Time : 2025-08-12 02:30:14.276488 UTC (04:30 GMT+02:00)
Duration : 00:02:18.2977370
Frames : 99
Protocol : ResolverRAT (certainty: 39,40)

Save Client Byte Stream
Save Server Byte Stream
PCAP

Flow Index 76 Display Frames 100 Encoding Time_Hex_ASCII Font Size 14

2025-08-12T02:27:56.0409550Z 0400 0000
2025-08-12T02:27:56.1323830Z 1603 0100 5a01 0000 5603 0168 9aa6 aba1Z...V..h????
dd8c b4bd 518e 24f7 fe76 4069 d16b f105 ?????Q??v@i?k?..
9ac9 d9bc 5efb 4af0 a8bb fa00 000e c00a ?????^J?????..
c009 c014 c013 0035 002f 000a 0100 001f ?..?..5./.....
000a 0008 0006 001d 0017 0018 000b 0002
0100 0023 0000 0017 0000 ff01 0001 00 ...#.....?.....

2025-08-12T02:27:56.2021350Z 1603 0107 b402 0000 5103 0168 9aa6 ac62?..Q..h????b
a7d8 9c18 2218 966b 8002 e43e 594b 2b22 ????.".?k?.?>YK+"
7ee8 ae1c 4313 ced2 1a9c a820 5404 0000 ~???.C.???.? T...
2922 2436 cc00 61c5 27f1 6aff cf4a d0fd)" \$6?.a?'?j??J??
d370 e057 f43c 796b 6090 8215 c014 0000 ?p?W?<yk`???.?..
0900 1700 00ff 0100 0100 0b00 04ec 0004?.....?..
e900 04e6 3082 04e2 3082 02ca a003 0201 ?..??.??.??.?..
0202 1000 d3ab c985 3957 bff2 3975 3f13????9W??9u?..
5d97 c930 0d06 092a 8648 86f7 0d01 010d]???.*?H??.....
0500 3012 3110 300e 0603 5504 030c 074f ..0.1.0...U....0
726e 6c63 6469 3020 170d 3235 3034 3036 rnlcdi0 ..250406
3136 3234 3137 5a18 0f399999123
3132 3335 3935 395a 3012 3110 300e 0603 123595920.1.0...
5504 030c 074f 726e 6c63 6469 3082 0222 U....Ornlcdi0?.."

Expires 9999-12-31 at 23:59:59 UTC

Find Match Case

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>

Source: <https://www.netresec.com/?page=Blog&month=2025-08&post=PureRAT-ResolverRAT-PureHVNC>