ANY.RUN on X: "🚨 ALERT: A new #SystemBC #RAT is targeting Linux-based platforms – #ExploreWithANYRUN The Linux variant of SystemBC proxy implant is potentially designed for internal corporate services. It is commonly used to target corporate networks, cloud servers, and even #IoT devices https://t.co/kP3F0GY46o" / X

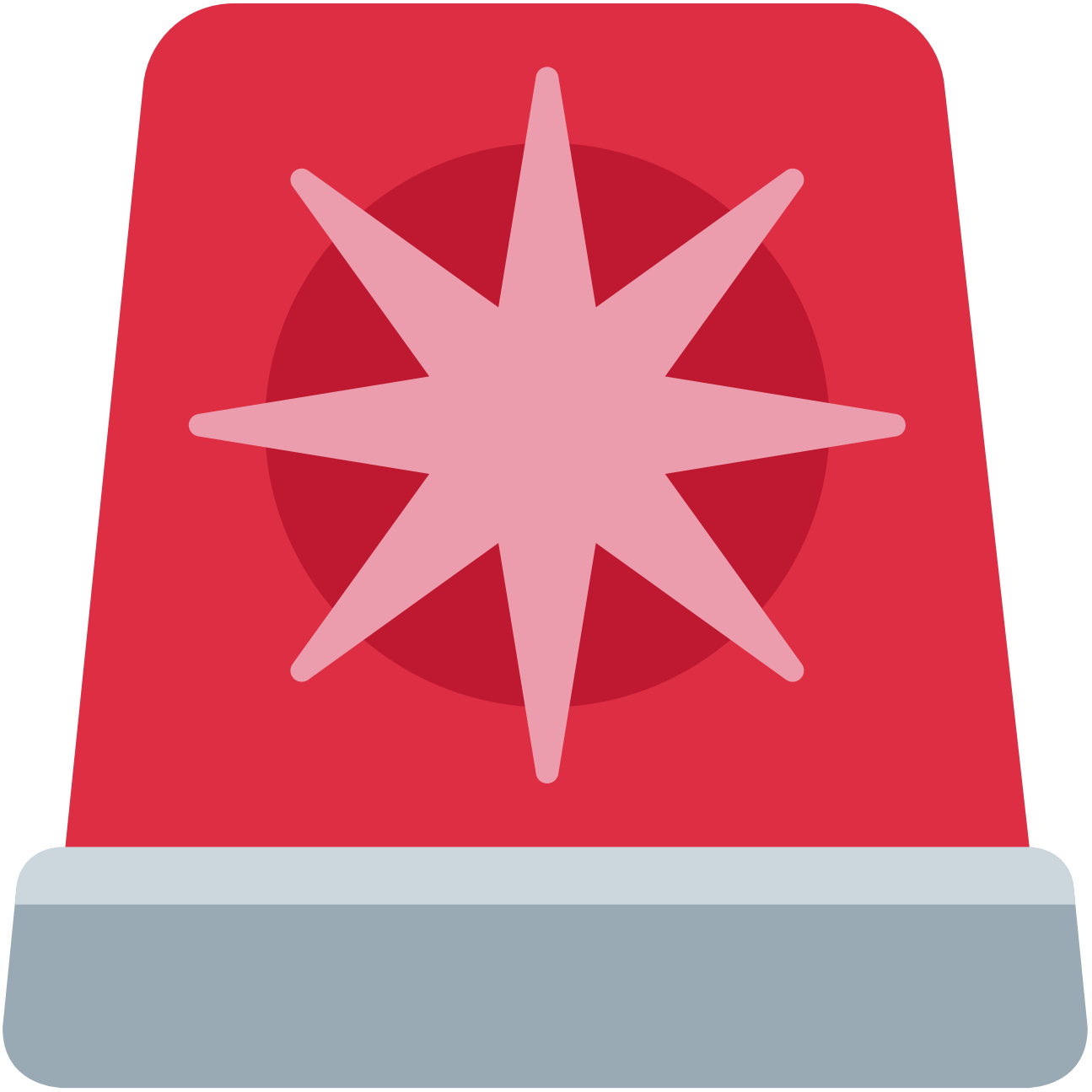
Published: 2025-01-28 · Archived: 2026-04-05 16:03:01 UTC

Post

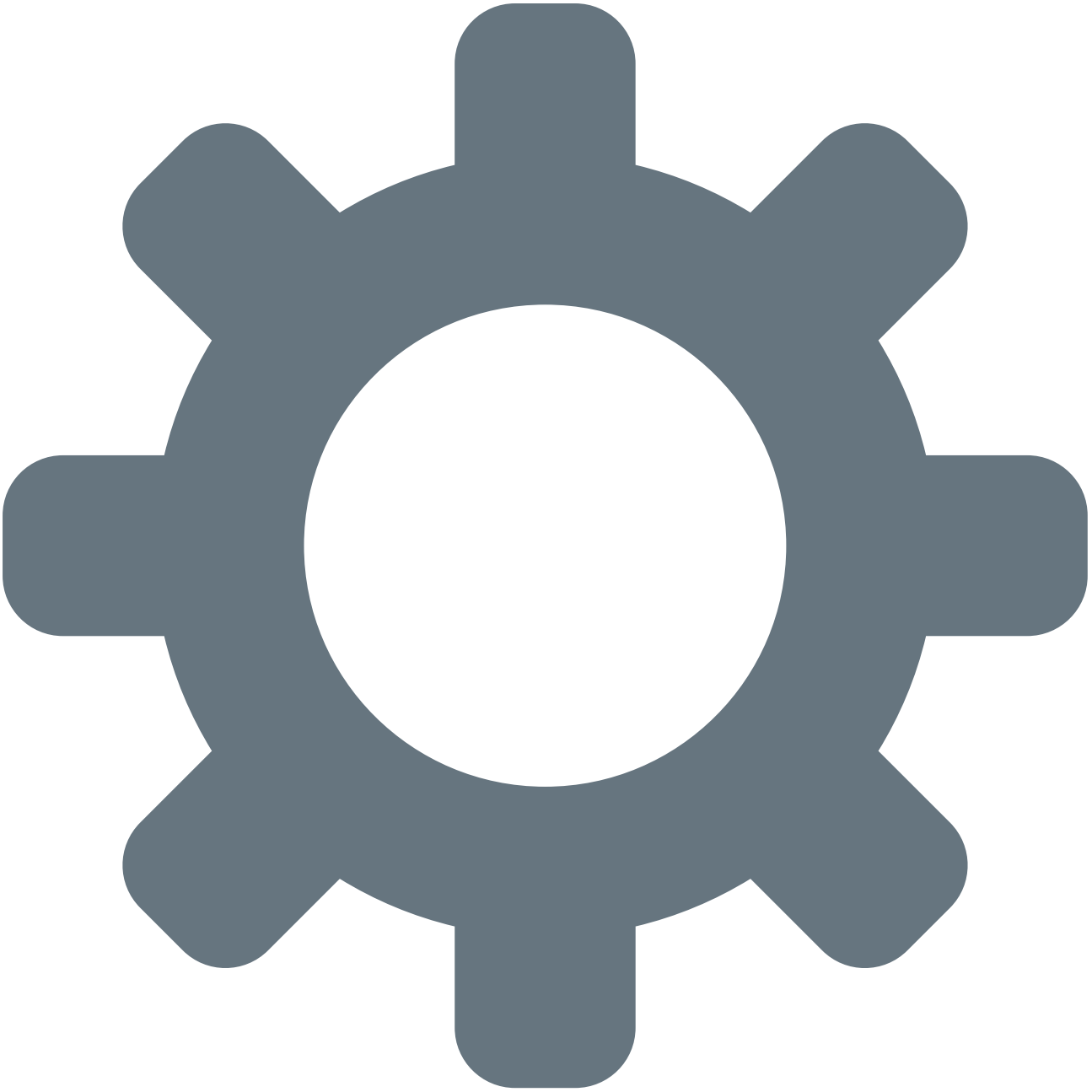
Conversation

ANY.RUN

@anyrun_app

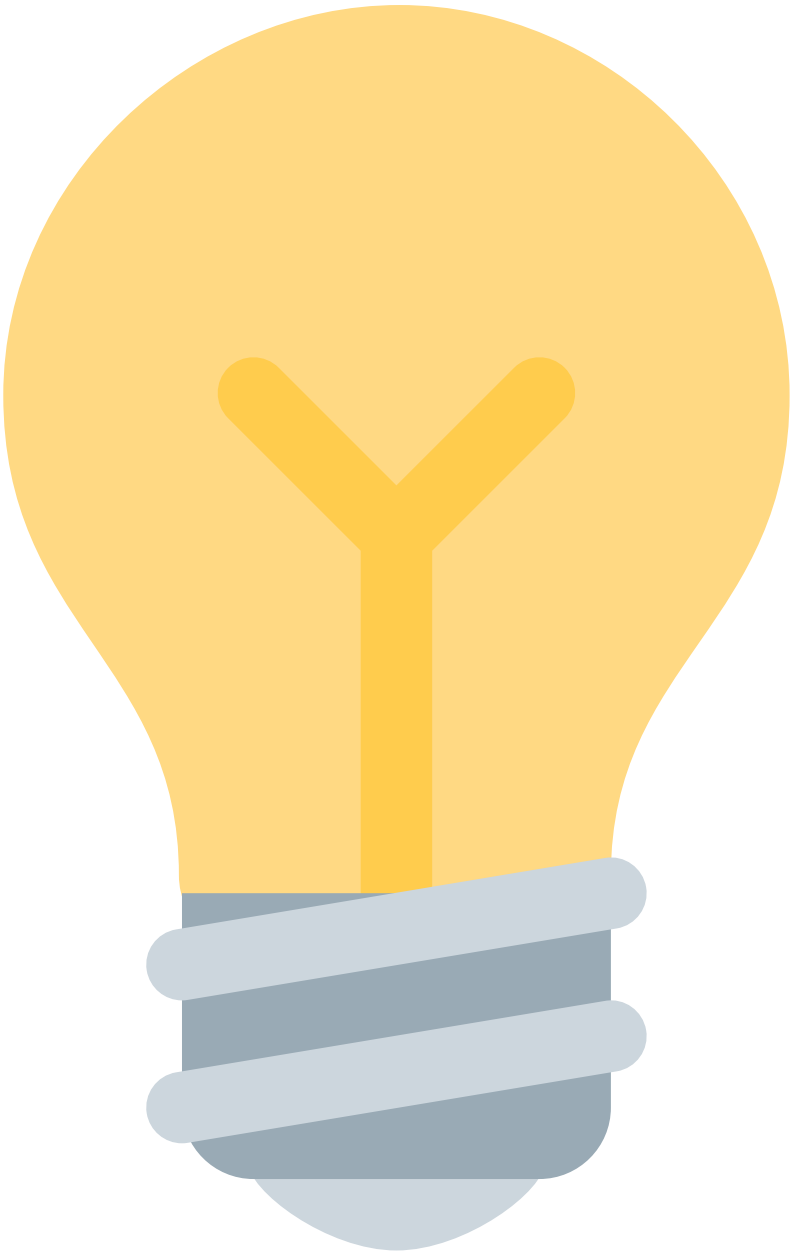


ALERT: A new #SystemBC #RAT is targeting Linux-based platforms – #ExploreWithANYRUN The Linux variant of SystemBC proxy implant is potentially designed for internal corporate services. It is commonly used to target corporate networks, cloud servers, and even #IoT devices



A proxy implant within a victim's infrastructure is a crucial tool for attackers, allowing for lateral movement and pivoting without deploying additional detectable tools, further evading detection on the host

This version is more stealthy and far more dangerous. Samples do not have clear family detection by security vendors



This Remote Access #Trojan is designed to maintain encrypted communication with #C2 servers, using the same custom protocol, ensuring connection to a unified infrastructure of both Windows and Linux implants.

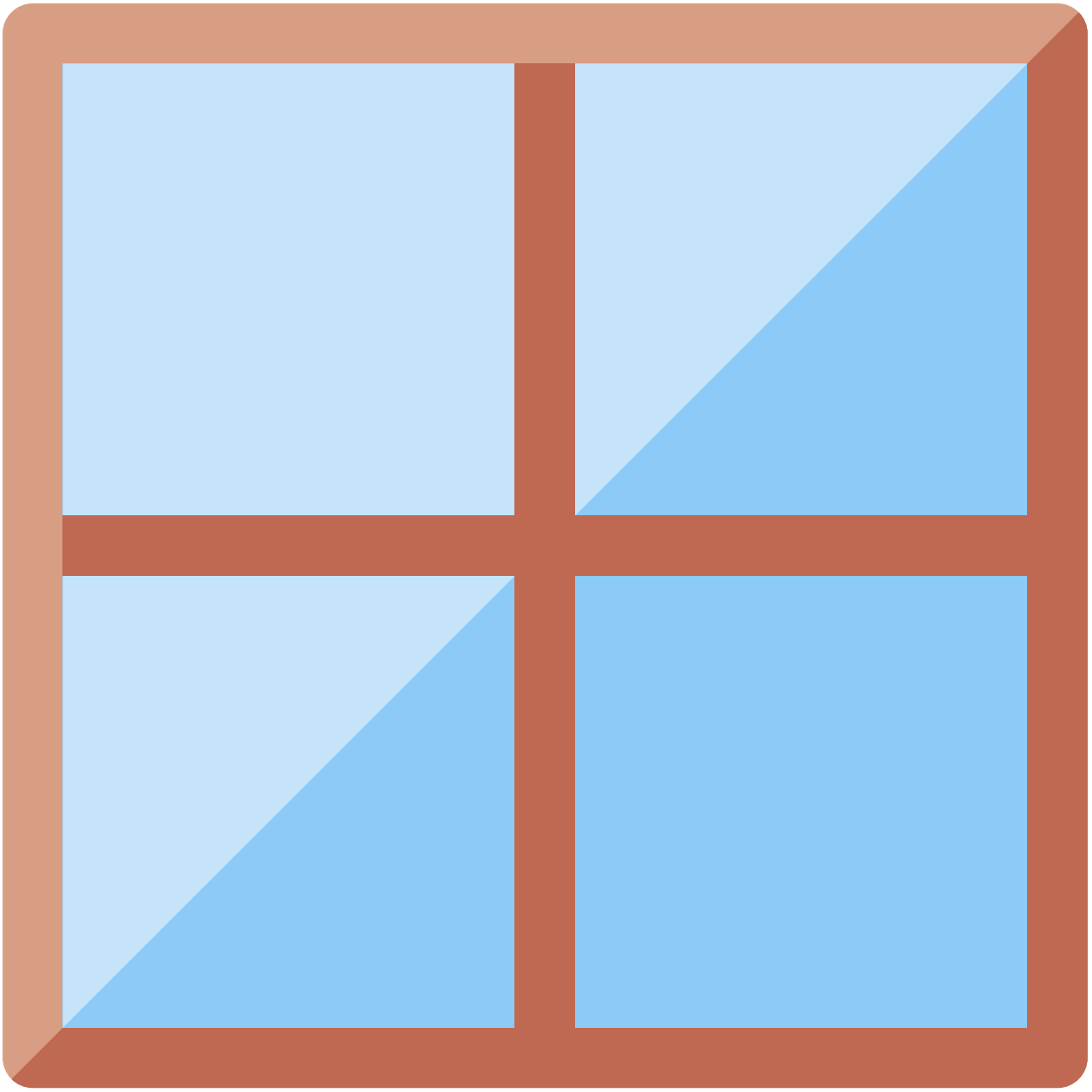
To respond effectively, use #ANYRUN's Linux VM and quickly detect #malicious communication with in-depth network traffic insights, powered by advanced #Suricata rules made by our experts Take a look at the Linux version analysis: app.any.run/tasks/63a3a89a #IOCs: cluster[.]amazonaws[.]work

0e1b714ff0ea13e64b302c48cb12c9bf 3d544d6b9086da758f17149cf1ac2e81

8601c30e1c5ba28541c8b164a879bfcb a1cc04b62c048cdbb25d027ab5dea111

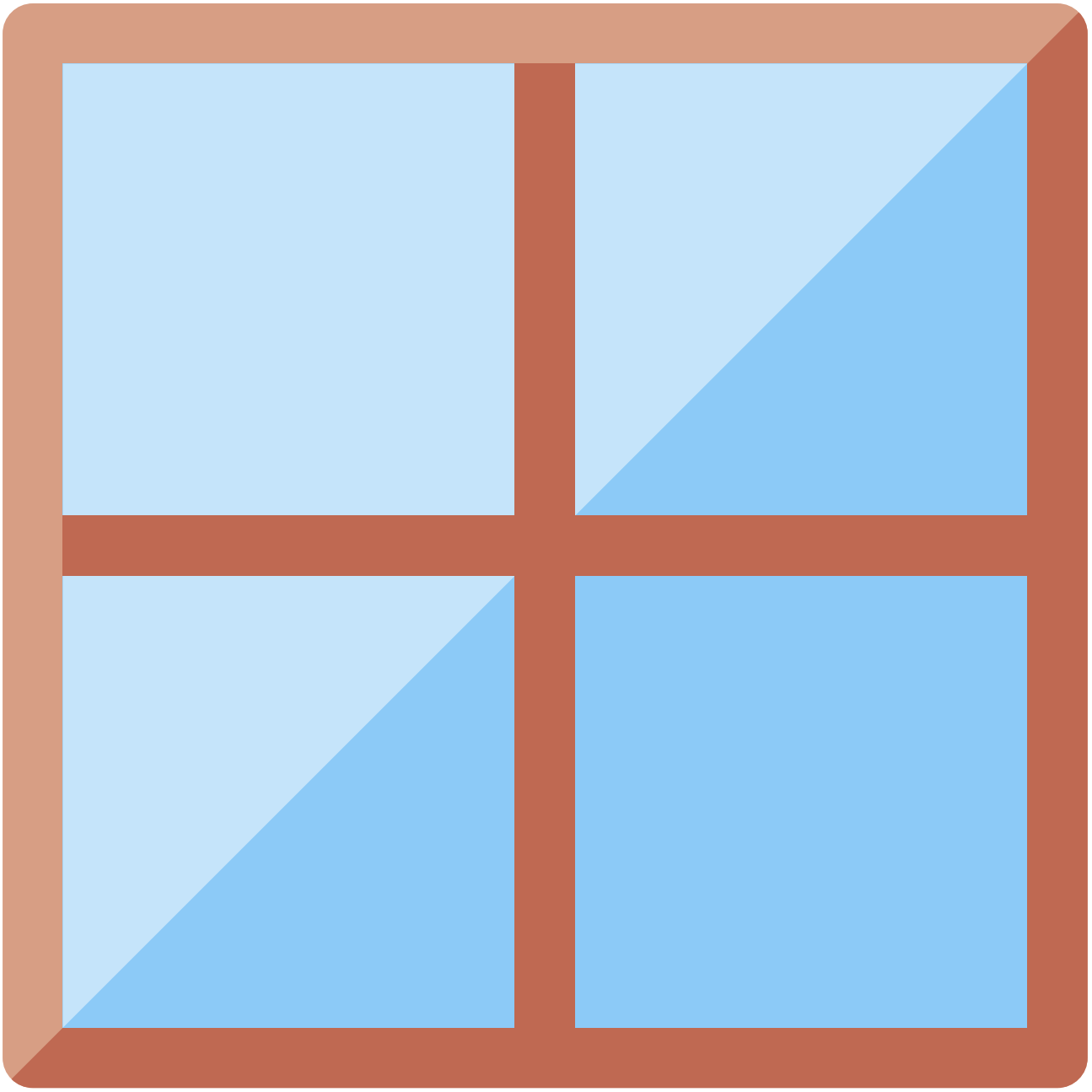
Decrypted traffic and configuration analysis of SystemBC: Linux vs. Windows

Linux traffic: gchq.github.io/CyberChef/#rec



Windows traffic: gchq.github.io/CyberChef/#rec

Linux config: gchq.github.io/CyberChef/#rec



Windows config: gchq.github.io/CyberChef/#rec More samples analyzed in #ANYRUN Interactive Sandbox: app.any.run/tasks/e8a9d10a app.any.run/tasks/0b30b2ee app.any.run/tasks/70c277f6

Use this TI Lookup search query to find more sandbox sessions and improve the precision and efficiency of your organization's security response: intelligence.any.run/analysis/looku Analyze latest malware and #phishing threats

with #ANYRUN

11:51 AM · Jan 28, 2025

12.3K

Views

Sign up now to get your own personalized timeline!

Registrera dig med GoogleRegistrera dig med GoogleÖppnas på en ny flik

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Source: https://x.com/anyrun_app/status/1884207667058463188