

Forum:[Hack Forums](#)

Thread: [New "Cavalry Werewolf" Attack Hits Russian Agencies with FoalShell and StallionRAT](#)

Stanley - October 12, 2025, 8:55 pm

New "Cavalry Werewolf" Attack Hits Russian Agencies with FoalShell and StallionRAT

A threat actor that's known to share overlaps with a hacking group called YoroTrooper has been observed targeting the Russian public sector with malware families such as FoalShell and StallionRAT.

Cybersecurity vendor BI.ZONE is tracking the activity under the moniker Cavalry Werewolf. It's also assessed to have commonalities with clusters tracked as SturgeonPhisher, Silent Lynx, Comrade Saiga,

<https://thehackernews.com/2025/10/new-cavalry-werewolf-attack-hits.html>

Oh_Well - October 13, 2025, 1:28 am

Interesting twist.. They show how fragmented the cyber landscape has become. Espionage-grade tools wrapped in stealth and persistence.

Vectura - October 13, 2025, 5:05 am

That's an interesting twist, most often we hear about Russian-linked actors going after others, not the other way around. The Cavalry Werewolf campaign seems like a reminder that cyber espionage is far from one-sided. The fact that it overlaps with groups like YoroTrooper and uses multiple RATs like FoalShell and StallionRAT suggests a well-coordinated and evolving operation. It'll be worth watching how Russia responds to this, especially if government agencies were directly impacted.

plops - October 13, 2025, 6:46 am

Definitely a reminder that it doesn't just come from one side. I think we just don't get to see the other sides news always.

Aeowulf - October 13, 2025, 4:02 pm

Love to see it. Its about time some nasty stuff goes that way.

leste - October 30, 2025, 5:23 pm

Overlaps with YoroTrooper show these threat groups are collaborating.

B3A - October 31, 2025, 1:24 am

(Oct 13, 2025 06:46 AM)plops Wrote: [\[CITE\]](#) Definitely a reminder that it doesn't just come from one side. I think we just don't get to see the other sides news always.

Nothing comes one sided. You have to do something to get them access