

Executive Situation Report | Global Botnet Escalating Attacks Against U.S. Remote Desktop Infrastructure

Key Judgments & Evidence

1. A global botnet has been activated to target RDP infrastructure in the United States.

- Since 8 October, GreyNoise has tracked a coordinated botnet operation initially involving over 100,000 unique IP addresses attacking U.S. RDP infrastructure
- The botnet leveraged RDP timing vulnerabilities to infer usernames, likely for follow-on compromise.
- Coordinated timing patterns, similar client fingerprints, and shared attack vectors suggest the activity likely originated from a centrally-controlled botnet.

2. Attacks are rapidly escalating, demanding urgent attention from security teams.

- On 14 October, the botnet grew to over 300,000 IPs — tripling its original size in four days.

3. Static defense measures will be ineffective at mitigating this threat.

- New IPs have been continuously activated, rendering static blocklists and traditional firewall rules insufficient.

Top 3
Source
Countries:

BRAZIL
ARGENTINA
MEXICO

Top
Target
Country:

UNITED STATES

Strategic Threat Context

ESPIONAGE:

In October 2024, Google Threat Intelligence observed a Russia-nexus espionage actor (UNC5837) distribute signed .rdp attachments to establish remote desktop sessions that allowed exfiltration of files and clipboard data.

RANSOMWARE:

According to CISA, the Snatch ransomware gang has been observed brute-forcing exposed RDP services to gain administrator credentials for network compromise.

GLOBAL EXPLOITATION:

The BlueKeep (CVE-2019-0708) remote code execution vulnerability in RDP is a “wormable” flaw that pre-authentication attackers could use to propagate across networks globally.

Recommended Actions

- Use GreyNoise Block (template name: *Oct-2025 RDP Botnet Campaign*) to dynamically block all IPs involved in this campaign.
- Check logs for unusual RDP probing.
- Monitor GreyNoise's RDP tags:
 - [Microsoft RD Web Access Anonymous Authentication Timing Attack Scanner](#)
 - [Microsoft RDP Web Client Login Enumeration Check](#)

Implications

- Infrastructure turnover:** The threat actor(s) is rapidly deploying new IPs to target RDP in the U.S., rendering static defenses insufficient.
- Attack volume:** Given recent developments, the volume of attacks is likely to increase in the near future.
- U.S. endpoints most targeted:** Most observed probes were directed at U.S.-hosted assets, suggesting focus on U.S. networks.

Threat Actor Activity

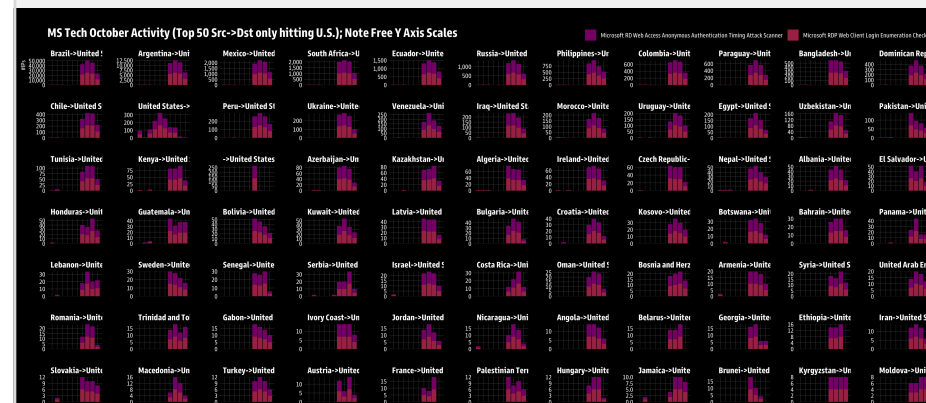


Figure 1: Coordinated attacks against U.S. RDP infrastructure since October 2025.
Source: GreyNoise Global Observation Grid (GOG).

Peak Activity:
~300,000 unique IPs

Significant spike in coordinated targeting of U.S. RDP infrastructure.