RDP HONEYPOT / WIN-SRV01 / 2026-08-20 TO 08-26 UTC

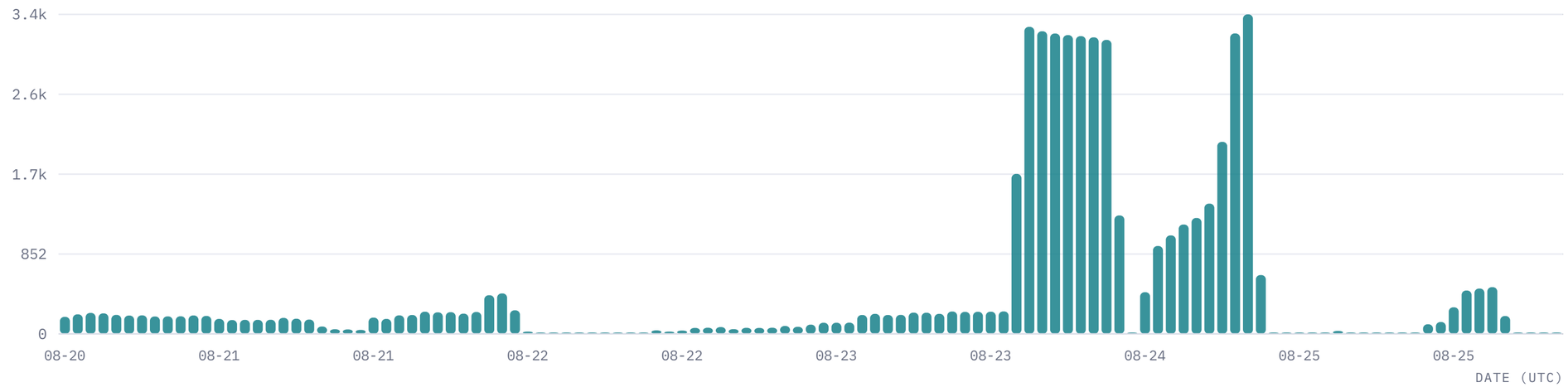
RDP attack telemetry

Every authentication attempt against one internet-facing honeypot over six days, with the password each one carried recovered where cracking succeeded.

53,839	91%	232	482	35,151	3,409
Attempts	Passwords recovered	Source IPs	Usernames tried	Distinct passwords	Peak hour

Attempts per hour

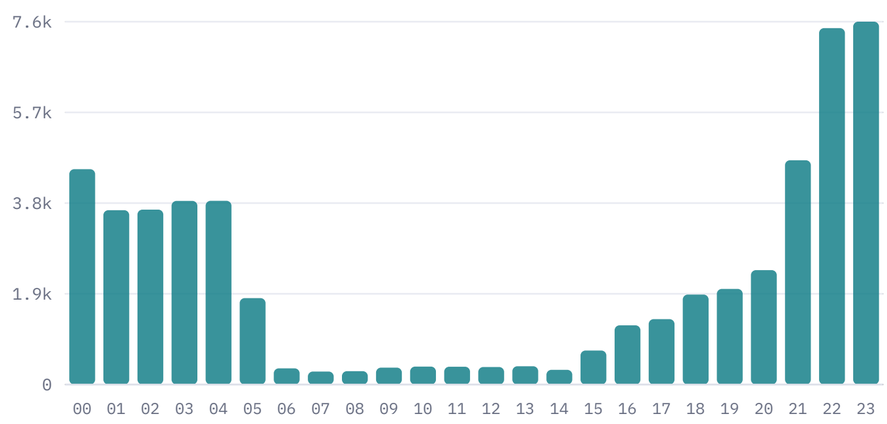
117 hourly buckets across the capture window



Traffic runs at a low baseline for three days, then steps up by an order of magnitude on 23–24 August. That is a new operator arriving, not the existing ones speeding up.

Hour of day

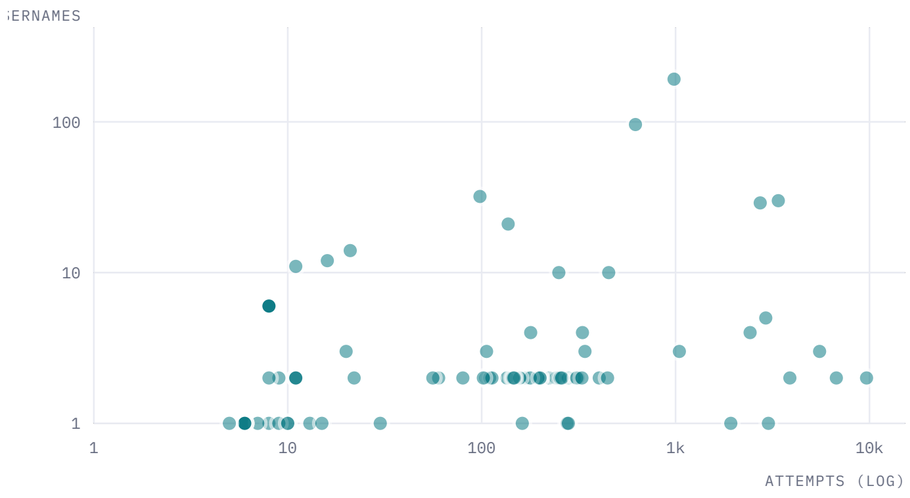
All six days aggregated, UTC



A real diurnal cycle: 22:00–04:00 UTC carries 20× the traffic of 06:00–14:00. Earlier captures on this host were flat around the clock — this population is not.

Campaign shape

Each dot is one source IP — attempts against usernames tried (log scales)



Bottom-right is a grinder — thousands of guesses at one account. Top-left is an enumerator — few guesses across many accounts. The gap between them is why one blocklist never covers both.

Busiest sources

Top 15 of 232 source addresses

SOURCE IP	ATTEMPTS	USERS
134.195.157.29	9,658	2
210.61.187.192	6,747	2
58.248.209.4	5,530	3
112.222.116.188	3,885	2
59.15.116.99	3,387	30
209.245.235.80	3,011	1
116.202.168.234	2,918	5
45.40.82.16	2,732	29
80.66.83.80	2,423	4
213.111.152.158	1,927	1
198.211.117.167	1,046	3
200.113.202.226	982	192
27.71.229.97	621	96
45.142.193.145	452	10
14.136.73.18	446	2

Most-targeted accounts

Top 12 of 482 usernames

USERNAME	ATTEMPTS
ADMINISTRATOR	39,520
ADMIN	4,984
USER	3,428
SERVER	609
Administrator	337
TEST	125
SYSTEM32	124
DELL	118
DESKTOP	112
SCANNER	111
ROOT	110
SUPPORT	110

Most-guessed passwords

Recovered cleartext, ranked by how many separate attempts carried it

PASSWORD	ATTEMPTS	PASSWORD	ATTEMPTS
1234	109	admin	61
123	101	Admin@123	59
12345	92	admin1234	58
P@ssw0rd	90	admin@1234	58
1	89	12345678	58
123456	78	123456789	54
12	73	1234567	49
admin@123	68		

> Reading these numbers. Each attempt is one credential guess captured at the NLA/CredSSP stage, so the password is recovered by cracking the NetNTLMv2 response rather than read directly. Roughly 91% resolved; the rest are shown as attempts without a password rather than dropped. Times are the honeypot's own clock in UTC.

HASH CRACKING CREW

@0xTib3rius · @apuleston · @akses_0x00 · @SwiftSecur1 · @d1wn

Thanks for helping crack the hashes.

Created by **@UK_Daniel_Card**

The honeypot mission continues.

Generated from the honeypot's attempts export joined to the cracking potfile on NTProofStr. Recovered passwords are credentials chosen by attackers, not by this host's users.