

PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Exchange Checked Every Other Day. Metabase Attempts Step Up.

A recurring pool of malicious IPs checked Exchange servers for ProxyNotShell in passes no more than 48 hours apart. Attempts on a known exploited Metabase flaw stepped up more than threefold. Gateway backdoor attempts widened sharply.

42–44 hours

GAP BETWEEN EXCHANGE
PROXYNOTSHELL PASSES, 05 TO 13
OCTOBER

3x+

RISE IN METABASE KEV
ATTEMPT IPS FROM 11 OCTOBER

22x

RISE IN GATEWAY BACKDOOR
IPS, 07 TO 11 OCTOBER

98%+

GATEWAY BACKDOOR IPS
ON ISP ADDRESS SPACE

WHAT'S INSIDE

Exchange checked for ProxyNotShell every 42 to 44 hours

About a thousand malicious IPs ran the [Exchange ProxyNotShell check](#) on every odd-numbered day from 05 to 13 October, against no more than 24 on even days. IPs from the same pool returned from pass to pass.

Metabase KEV flaw attempts stepped up

Attempts against [CVE-2026-72898](#), an unauthenticated Metabase flaw rated CVSS 10, rose more than threefold from 11 October. Every IP was malicious. Each Metabase instance stores credentials for the databases it queries.

Gateway telnet backdoor pool grew more than twentyfold

The number of IPs trying factory accounts on Dasan and D-Link gateways grew about 22 times in four days. Over ten days, GreyNoise tagged 1,598 IPs with the [Dasan backdoor behavior](#), all malicious.

One host drove the RDP crawling rise

[RDP Crawler](#) activity rose 74%, and a single host not named in prior briefs sent 36% of it. That activity is likely to fall when the host goes quiet.

Want the full brief?

GreyNoise customers get complete IOCs, infrastructure detail, and role-based recommendations every week.

greynoise.io/contact