

92.6% of the IPs behind the 21 October PHP2Shell attack burst were already known to OneFirewall. They sent 99.96% of the attempts.

A three-hour wave of automated requests against .php endpoints, the signature of the PHP2Shell web-shell campaign.

32,252

attack attempts in 3
hours, 20:00 to 23:00
UTC

27

source IPs

3

organizations hit

US · RO · CN

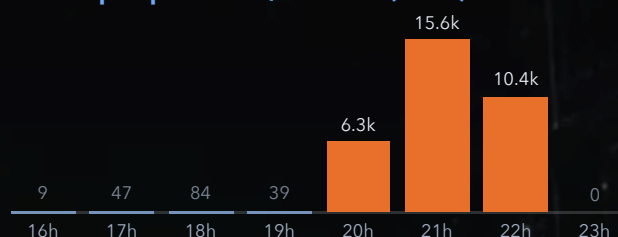
top source countries

What it is, and what it costs

Attackers scan the internet for PHP files they can abuse, such as a vulnerable upload form, an eval endpoint or a web shell left by an earlier break-in. One hit gives them remote code execution on the web server, and from there stolen data and credentials, movement into the internal network, and ransomware or botnet enrolment.

The burst was sharp: 6,284 attempts in the first hour, 15,562 in the second and 10,406 in the third, after a quiet evening of under 100 an hour.

Attempts per hour, 21 Oct (UTC)



Orange = the burst. Quiet before and after.

How well we knew the attackers

Known means a score of at least	IPs	% of IPs	% of attempts
10	25 of 27	92.6%	100.0%
30	23 of 27	85.2%	99.9%
80	20 of 27	74.1%	90.9%
150 (Critical)	17 of 27	63.0%	89.6%

Score at the time of each event. At the strictest line, 63% of IPs and 90% of traffic were already Critical.

How long we knew them

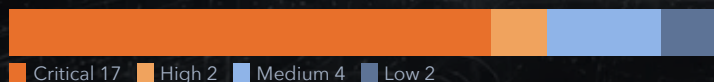
The 25 known IPs were first scored	IPs
over a year before the attack	3
1 to 12 months before	9
7 to 30 days before	8
1 to 7 days before	3
in the 24 hours before	2

Who was behind it

Share of scored events



Share of scored IPs



Critical 150+, High 90-150, Medium 40-90, Low under 40.

Top 3 attackers by events

216.36.112.159	US	5,330	score 436
171.34.139.222	CN	4,940	score 677
80.94.95.211	RO	4,685	score 444

Top 3 attackers by crime score

171.34.139.222	CN	4,940	score 677
103.160.205.37	ID	2,647	score 584
169.58.137.184	US	4,390	score 558

Where OneFirewall comes in

25 of the 27 attacking IPs were already in the OneFirewall database before the burst, so a rule pushed to the firewall would have stopped them at the first request. Intelligence moves fast across the Alliance: 5 of them had been scored only in the previous 7 days, 2 within the last 24 hours. The IPs scored High or Critical sent 90% of the burst, which makes them safe to deny automatically.

These numbers come only from Alliance members who have opted in to the research and share their traffic. They understate the real size of the attack wave across the internet.

Recommendation: re-evaluate your blocking score threshold so that it sits below 150. At 150 alone, 10 of these 27 IPs would have got through; at a threshold of 80, 20 of 27 IPs and 91% of the traffic are covered. Also patch or remove any exposed PHP upload and eval endpoints.