Threat Analysis Report

Probe from suspicious IP

Luke Jacobson 25.10.2025

Description

Oct 24, 2025 @ 20:06:18.357 - The following */var/log/apache2/luke.yt-access.log* log raised an alert in wazuh - *52.178.223.71 - - [24/Oct/2025:18:06:12 +0000] "GET /wp-content/plugins/hellopress/wp_filemanager.php HTTP/1.1" 404 452 "-" "-"*

A get request targets a wordpress management .php file. The targeted apache webserver returned code 404.

The IP **52.178.223.71** - Sent over *145* different get attempts to various .php files in less than one second.

This appears to be an initial reconnaissance attempt, trying to locate vulnerable files.

WhoIs

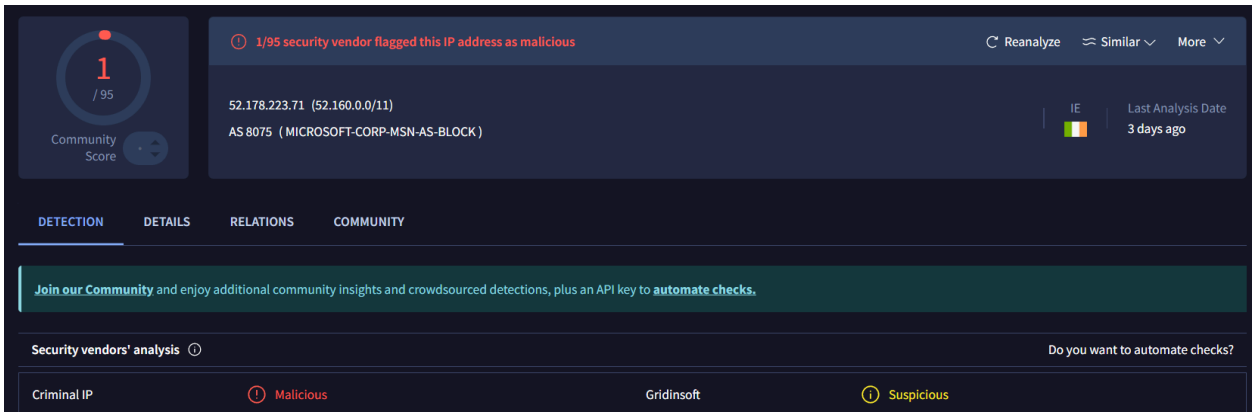
Returns **Microsoft** as the organization:

NetRange: 52.145.0.0 - 52.191.255.255
CIDR: 52.146.0.0/15, 52.152.0.0/13, 52.148.0.0/14, 52.145.0.0/16, 52.160.0.0/11
NetName: MSFT
NetHandle: NET-52-145-0-0-1
Parent: NET52 (NET-52-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Microsoft Corporation (MSFT)
RegDate: 2015-11-24
Updated: 2021-12-14
Ref: https://rdap.arin.net/registry/ip/52.145.0.0
OrgName: Microsoft Corporation
OrgId: MSFT
Address: One Microsoft Way
City: Redmond
StateProv: WA
PostalCode: 98052

Country: *US*
RegDate: *1998-07-10*
Updated: *2025-06-10*

VirusTotal

1 vendor, Criminal IP - lists this IP as malicious



AbuseIPDB

Reports 100% confidence of abuse

PHP file targets

Here are all the php files targeted in this attack:

_source.data.url
/.well-known/acme-challenge/
about.php
/030.php
/031.php
/0x.php
/0x0x.php
/1.php
/10.php
/11.php
/12.php
/123.php
/13.php
/133.php
/222.php
/2clas.php
/3.php
/33.php
/333.php
/6.php
/7.php
/a2.php
/a3.php
/aa.php
/aaa.php
/ab.php
/abcd.php
/about.php
/aghbvr.php
/aj.php
/akk.php
/alfa.php
/alpa.php
/ar.php
/article.php
/bak.php
/bless.php
/bless11.php
/bless3.php
/bolt.php
/cfile.php
/chosen.php
/classgoto24.php
/cong.php?p=
/css.php
/dlu.php
/doti.php
/ea.php
/ee.php
/en0.php
/enclas.php
/enclas.php
/error.php
/f6.php
/fe5.php
/fex.php
/ffile.php
/file1.php
/file15.php
/file18.php
/file2.php
/file21.php
/file4.php
/file8.php
/file88.php
/file9.php
/filer.php
/filesss.php
/finny.php
/fm.php
/fm.php?p=
/fns.php
/geck.php
/gi.php
/gifclass.php
/gifclass4.php
/gmo.php
/goat.php
/gt.php
/haa.php
/he.php
/hi.php
/ifm.php
/ilex.php
/inde.php
/info.php
/ini.php
/install.php
/iov.php
/ioxi-o.php
/kaza.php
/klex.php
/lala.php
/lock360.php
/lv.php
/mail.php
/max.php
/miso.php
/mlex.php
/mpxct.php
/n.php
/naxc.php
/nfile.php
/opts.php
/ouh.php
/owl.php
/pent.php
/php8.php
/plss3.php
/r79.php
/redi.php
/rrr.php
/RsR.php
/s.php
/sec.php
/shell1.php
/shellalfa.php
/size.php
/system_log.php
/taff.php
/taktak.php
/tgrs.php
/tgrs.php
/ton.php
/tor.php
/usep.php
/ut.php
/v.php
/vee.php
/wan.php
/we.php
/wfile.php
/wp-admin/maint/index.php
/wp-content/plugins/hellopres
s/wp_filemanager.php
/wp-includes/fonts/about.php
/wpo.php
/wpo.php

/wsd.php
/wsr2.php
/wsx.php
/x0.php
/x3.php
/xsox.php
/xxa.php
/yellow.php
/zde.php

Link to full wazuh logs

Suspicious_IP_Probing_24_10_2025