

Threat Analysis Report

Probe from suspicious IP

Luke Jacobson 25.10.2025

Description	1
Whols	1
VirusTotal	2
AbuseIPDB	2
PHP file targets	3

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.

Whols

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

The screenshot shows the VirusTotal interface for the IP address 52.178.223.71. On the left, a circular gauge displays a 'Community Score' of 1 out of 95. The main header indicates that 1/95 security vendors have flagged this IP as malicious. Below this, the IP address is shown along with its geolocation (IE) and the last analysis date (3 days ago). The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A banner encourages joining the community for more insights. A section titled 'Security vendors' analysis' shows a table with the following data:

Security vendors' analysis	Do you want to automate checks?
Criminal IP	Malicious
Gridinsoft	Suspicious

AbuseIPDB

Reports 100% confidence of abuse

The screenshot shows the AbuseIPDB interface for the IP address 52.178.223.71. A large orange banner at the top states '52.178.223.71 was found in our database!'. Below this, it reports that the IP was reported 353 times with a 100% confidence of abuse. A red progress bar visualizes the 100% confidence level. The interface includes a table with the following data:

ISP	Microsoft Corporation
Usage Type	Data Center/Web Hosting/Transit
ASN	AS8075
Domain Name	microsoft.com
Country	Ireland
City	Dublin, Leinster

PHP file targets

Here are all the php files targeted in this attack:

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