Firewall Events elhacker.net

Feb 23rd 2023 22:53 (UTC +01:00) → Feb 23rd 2023 23:59 (UTC +01:00)
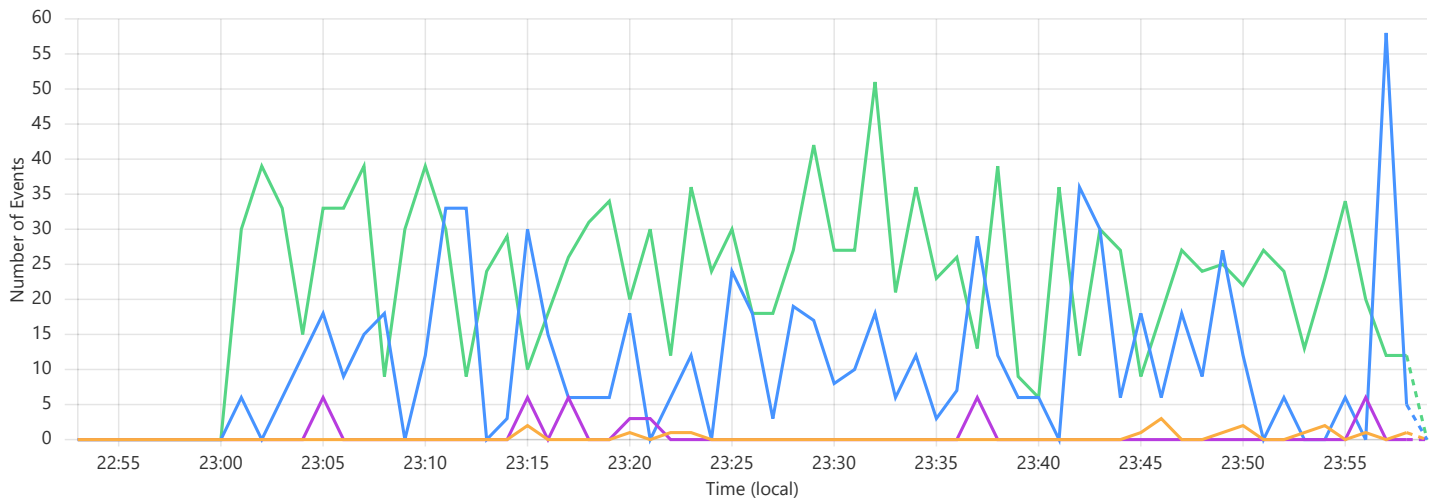
CLOUDFLARE

Filters:

IP equals 154.49.211.99

Events summary ▢ About Firewall Events

Action   Host   Country   ASN   IP   Path   •••

Total	○ Log	○ Block	○ Managed Challenge	○ Legacy CAPTCHA
2.19k	1.44k	699	36	17

Events by service

○ Managed rules (previous version)	○ Firewall rules
2.15k	41

Top events by source

IP Addresses		User Agents	
154.49.211.99	2.19k	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36	87
		Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/44.0.2403.155 Safari/537.36	85
		Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1866.237 Safari/537.36	81
		Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.47 Safari/537.36	80
		Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2820.59 Safari/537.36	80
		Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2225.0 Safari/537.36	80
		Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2226.0 Safari/537.36	77
		Mozilla/5.0 (X11; OpenBSD i386) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36	75
		Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.3319.102 Safari/537.36	74
		Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2309.372 Safari/537.36	71
		Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2225.0 Safari/537.36	71
		Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2866.71 Safari/537.36	70
		Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36	70
		Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36	69
		Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.137 Safari/4E423F	69

Paths		Countries	
/index.php	318	France	2.19k
/	96		
/index.action	36		
/wls-wsat/CoordinatorPortType	30		
/ajax.php	24		
/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp	24		
/wp-login.php	22		
/login.action	18		
/login.php	18		
/MUP/	18		
/vendor/phpfastcache/phpfastcache/docs/examples/phpinfo.php	12		
/portal/attachment_downloadByUrlAtt.action	12		
/_search	12		
/.../.../.../.../.../.../.../.../.../windows/win.ini	12		
/WealthT24/GetImage	12		

Managed rules

No data

Managed rules (previous version)

100005 - DotNetNuke - File Inclusion - CVE:CVE-2018-9126, CVE:CVE-2011-1892, CVE:CVE-2022-31474	804
100173 - XSS, HTML Injection - Script Tag	463
100016 - Version Control - Information Disclosure	96
100135A - XSS - JavaScript Events	96
WP0026 - Wordpress - Broken Access Control, File Inclusion	75
100199 - Apache Struts - Code Injection - CVE:CVE-2013-1965, CVE:CVE-2013-1966, CVE:CVE-2013-2115, CVE:CVE-2013-2134, CVE:CVE-2013-2135	54
100008B - SQLi - String Concatenation	48
100302 - SQLi - UNION in MSSQL	36
100153 - Oracle WebLogic - Command Injection - CVE:CVE-2019-2729, CVE:CVE-2019-2725, CVE:CVE-2017-10271, CVE:CVE-2017-3506	36
100524 - Java - Remote Code Execution	30
100135C - XSS - JavaScript Events	30
100026 - PHP, vBulletin, jQuery File Upload - Code Injection, Dangerous File Upload - CVE:CVE-2018-9206, CVE:CVE-2019-17132	24
100136A - XSS - JavaScript URI - Beta	24
100009 - SQLi - Conditional	24
100038 - Information Disclosure - Common Files	21

HTTP DDoS rules

No data

HTTP Methods

GET	1.8k
POST	385
PUT	6

Activity log

Date	Action taken	Country	IP address	Service
› Feb 23, 2023 11:58:51 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:50 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:50 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:50 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:49 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:49 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:43 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:42 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:42 PM	Log	France	154.49.211.99	Managed rules (previous version)
› Feb 23, 2023 11:58:42 PM	Log	France	154.49.211.99	Managed rules (previous version)

1 to 10 of **2,193** items