Top Threats Oct 29, 2023

Threat ID/Name	ID	Threat/Content Type	Count
SSH User Authentication Brute Force Attempt	40015	vulnerability	428
generic:rndskittytor.com!	613873083	spyware	309
ZGrab Application Layer Scanner Detection	57955	vulnerability	72
Suspicious DNS Query (generic:astivysauran.com)	582869784	spyware	54
Suspicious DNS Query (generic:sdk.beizi.biz)	614140488	spyware	52
Suspicious DNS Query (generic:pvp-rivals.com)	614110788	spyware	49
Suspicious DNS Query (generic:soap2day.tel)	614364207	spyware	41
Suspicious DNS Query (generic:rndskittytor.com)	613873083	spyware	40
AndroxGh0st Scanning Traffic Detection	86759	spyware	35
phpunit Remote Code Execution Vulnerability	55852	vulnerability	20
Suspicious DNS Query (generic:absentlyrindbulk.com)	614139984	spyware	18
generic:track.flexlinkspro.com	611016462	spyware	16
Gh0st.Gen Command and Control Traffic	13264	spyware	14
Suspicious DNS Query (generic:gameavenue.co)	614383293	spyware	14
AndroxGh0st Scanning Traffic Detection	86760	spyware	13
ABB PB610 Panel Builder 600 IDAL HTTP Host Stack Buffer Overflow Vulnerability	56335	vulnerability	12
Suspicious DNS Query (generic:q3ww6.1antiphonon.online)	614308992	spyware	10
generic:click-v4.expdirclk.com	611200836	spyware	9
Suspicious DNS Query (generic:ww1.gameavenue.co)	614383917	spyware	6
generic:stats.itopvpn.com	603842928	spyware	6
generic:plf6.915vip19.xyz	613890714	spyware	5
Generic Router Remote Command Execution Vulnerability	93386	vulnerability	5
generic:ganeshacarrental.com	613061112	spyware	4
generic:special.beatifulllhistory.com	613819725	spyware	4
Suspicious DNS Query (generic:ww25.remote-dba.cc)	614058591	spyware	4
TP-Link Home WiFi Router Security Bypass Vulnerability	56320	vulnerability	4
Suspicious DNS Query (generic:bareelaborate.com)	614272158	spyware	4
Suspicious DNS Query (generic:pais.su)	614016423	spyware	4
Suspicious DNS Query (generic:femsoahe.com)	614294553	spyware	4
Suspicious DNS Query (generic:www.thecheyennepost.com)	614382123	spyware	4
generic:upgrader.live	605241282	spyware	3
Joomla Improper Access Control Vulnerability	93512	vulnerability	3
LB-LINK Command Injection Vulnerability	93718	vulnerability	3
Microsoft Windows HTTP.sys Remote Code Execution Vulnerability	37610	vulnerability	2
generic:securesearchnow.com	602428614	spyware	2
MVPower DVR TV Remote Command Execution Vulnerability	54553	vulnerability	2
NJRat.Gen Command and Control Traffic	11921	spyware	2
generic:api.appeasou.com	607976913	spyware	2
Microsoft Windows SMB Variable Validation Vulnerability	33367	vulnerability	2
MVPower DVR Shell Unauthenticated Command Execution Vulnerability	57566	vulnerability	2
Microsoft Vista SMB Negotiate Protocol DoS	32348	vulnerability	2
PowerDNS Recursive Out-of-Bounds Read Denial-of-Service Vulnerability	40729	vulnerability	2
Microsoft Exchange Server Remote Code Execution Vulnerability	90815	vulnerability	1
Pivotal Spring Data Commons Remote File Read XXE Vulnerability	40992	vulnerability	1
Netgear Routers Arbitrary Command Injection Vulnerability	30554	vulnerability	1