Top threats

Sunday, October 06, 2024

Threat ID/Name	ID	Threat/Content Type	Count
DNS ANY Queries Brute Force DOS Attack	40033	vulnerability	9.27 M
Microsoft SQL Server User Authentication Brute Force Attempt	40010	vulnerability	16.44 k
TCP SYN with data	8723	packet	6.18 k
TCP SYN-ACK with data	8724	packet	371
UDP Flood	8502	flood	121
MAIL: User Login Brute Force Attempt	40007	vulnerability	85
ZGrab Application Layer Scanner Detection	57955	vulnerability	37
PHP DIESCAN Information Disclosure Vulnerability	55834	vulnerability	30
ICMP Flood	8503	flood	19
phpunit Remote Code Execution Vulnerability	55852	vulnerability	18
D-Link HNAP SOAPAction Header Command Execution Vulnerability	38600	vulnerability	14
AndroxGh0st Scanning Traffic Detection	86760	spyware	14
AndroxGh0st Scanning Traffic Detection	86759	spyware	14
Malformed DNS Response Detection	92406	vulnerability	10
PowerDNS Recursive Out-of-Bounds Read Denial-of-Service Vulnerability	40729	vulnerability	10
TP-Link Archer Router Command Injection Vulnerability	93749	vulnerability	9
Bash Remote Code Execution Vulnerability	36729	vulnerability	9
Apache HTTP Server Path Traversal Vulnerability	91752	vulnerability	8
D-Link Remote Code Execution Vulnerability	57934	vulnerability	4
Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability	34221	vulnerability	4
Apache Struts2 Redirect/Action Method Remote Code Execution Vulnerability	56944	vulnerability	4
Apache Struts2 OGNL Remote Code Execution Vulnerability	90336	vulnerability	4
MVPower DVR Shell Unauthenticated Command Execution Vulnerability	57566	vulnerability	3
Gh0st.Gen Command and Control Traffic	13264	spyware	2
Overlapping TCP segment mismatch	8709	packet	2
MovableTypeCMS Remote Code Execution Vulnerability	91875	vulnerability	2
Netgear DGN Device Remote Command Execution Vulnerability	40741	vulnerability	2
LB-LINK Command Injection Vulnerability	93718	vulnerability	2
Suspicious DNS Query (generic:transcm.info)	597902301	spyware	2
NJRat.Gen Command and Control Traffic	11921	spyware	1
RPC Portmapper DUMP Request Detected	32796	vulnerability	1
Pivotal Spring Data Commons Remote File Read XXE Vulnerability	40992	vulnerability	1
GPON Home Routers Remote Code Execution Vulnerability	37264	vulnerability	1
Vacron NVR Remote Command Execution Vulnerability	54537	vulnerability	1