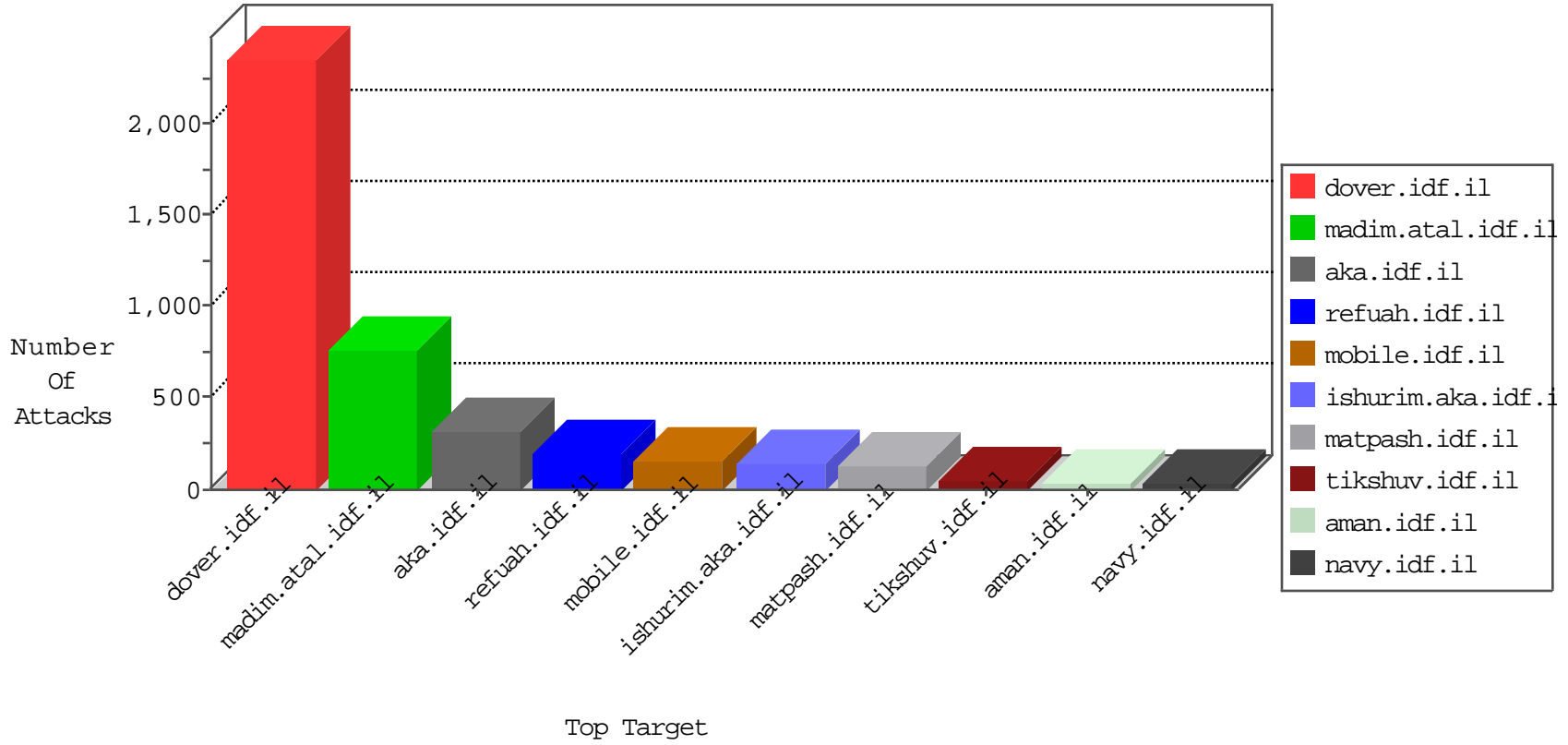


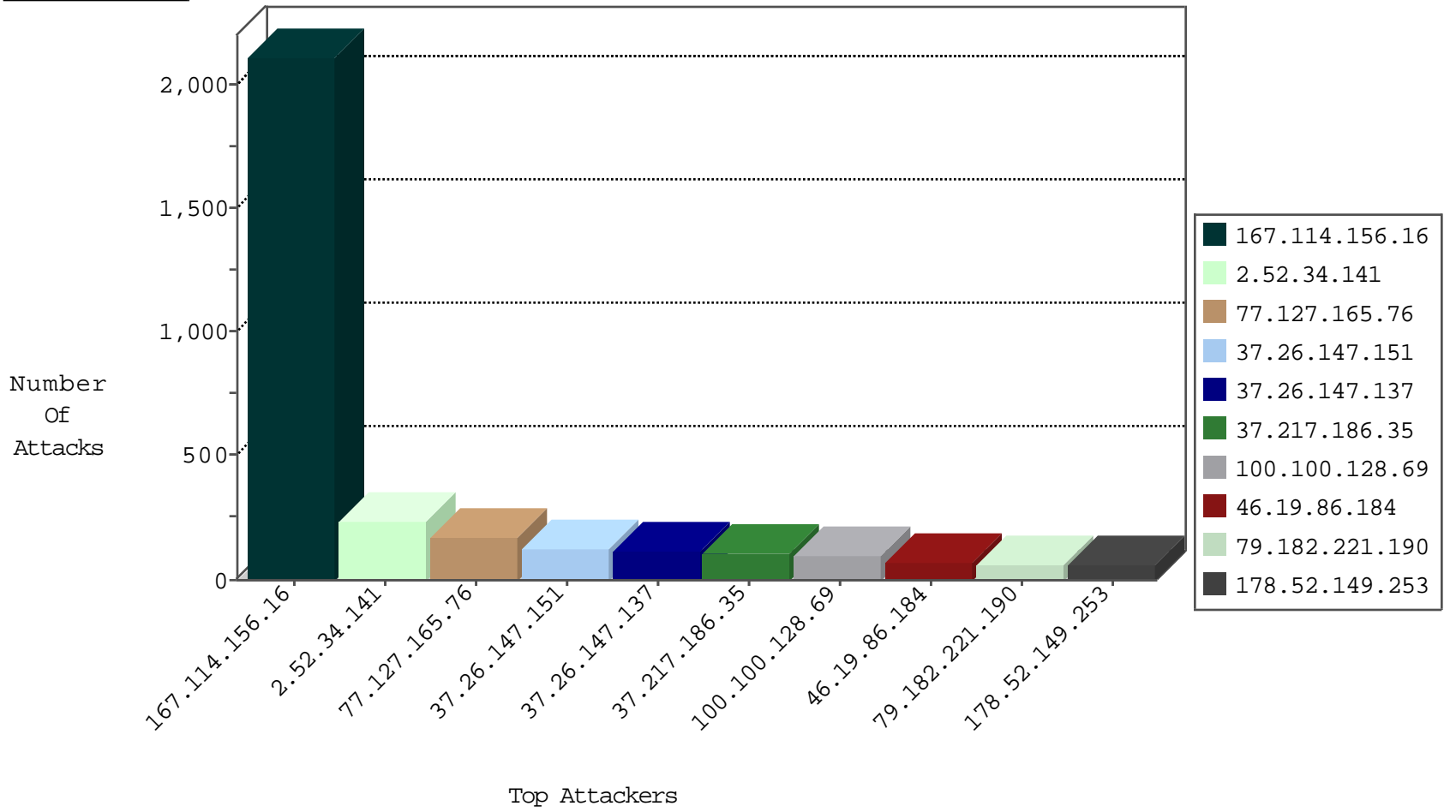
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3019
80.246.136.151	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
207.232.36.181	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
213.151.37.196	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
79.179.178.126	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.183.219.19	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.128.215	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.228.127.20		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.97.83.125	Switzerland	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	2
46.19.86.214	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
84.95.200.200	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
82.205.37.170	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
84.229.31.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.173.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.18.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.44.140.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.130.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.52.149.253	147.237.77.216	Syrian Arab Republic	dover.idf.il	portscan: TCP Distributed Portscan	1
100.38.183.54	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.12.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.49.45.47	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.171.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.181	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.165.76	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	174
37.217.186.35	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	110
100.100.128.69		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	93
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
178.52.149.253	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
107.167.109.159	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
109.253.209.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.2.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.32.179.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.216	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
80.246.139.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.34.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.180.199.182	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.177.170.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
178.52.149.253	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.189	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
82.166.240.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
62.0.200.108	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
84.108.169.101	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.225.7	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
37.46.39.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.189	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
82.80.158.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.180	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.239.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.189	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.154.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.154.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.154.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.154.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.73.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.154.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.54.140.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
149.78.248.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.108	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.52.133.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.130.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.162.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.140.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.182.107.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.183.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.30.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.34.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	206
37.26.147.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
37.26.147.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	80
46.19.86.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
79.182.221.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
37.26.147.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
2.52.34.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
37.26.147.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
80.246.136.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
109.253.221.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
80.179.141.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
149.78.47.212	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
149.78.56.32	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
176.13.20.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.200.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
176.13.14.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
79.176.55.53	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
80.246.136.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.2.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
176.13.17.79	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	5
109.253.209.205	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
82.166.240.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.222.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.78.184.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.177.170.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.139.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.66.188.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
164.138.127.192	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21570-he/idfgdover.aspx&sa=u&ved=0ahukewic6vqhcxka hujdswkhvylcvaqfeggimaa&usg=afqjcnjgkxkptobpol8pgxzxftd95sstiiw	Block	2
46.121.75.0	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
37.142.68.107	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
192.117.186.240	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
62.219.136.238	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/112260.pdf	Block	2
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
213.57.189.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.22.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.142.68.107	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	2
46.120.121.241	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
109.66.153.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.223.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct139\$ct101\$ct103\$radioQuestion in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
2.54.22.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.64.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
37.142.226.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1