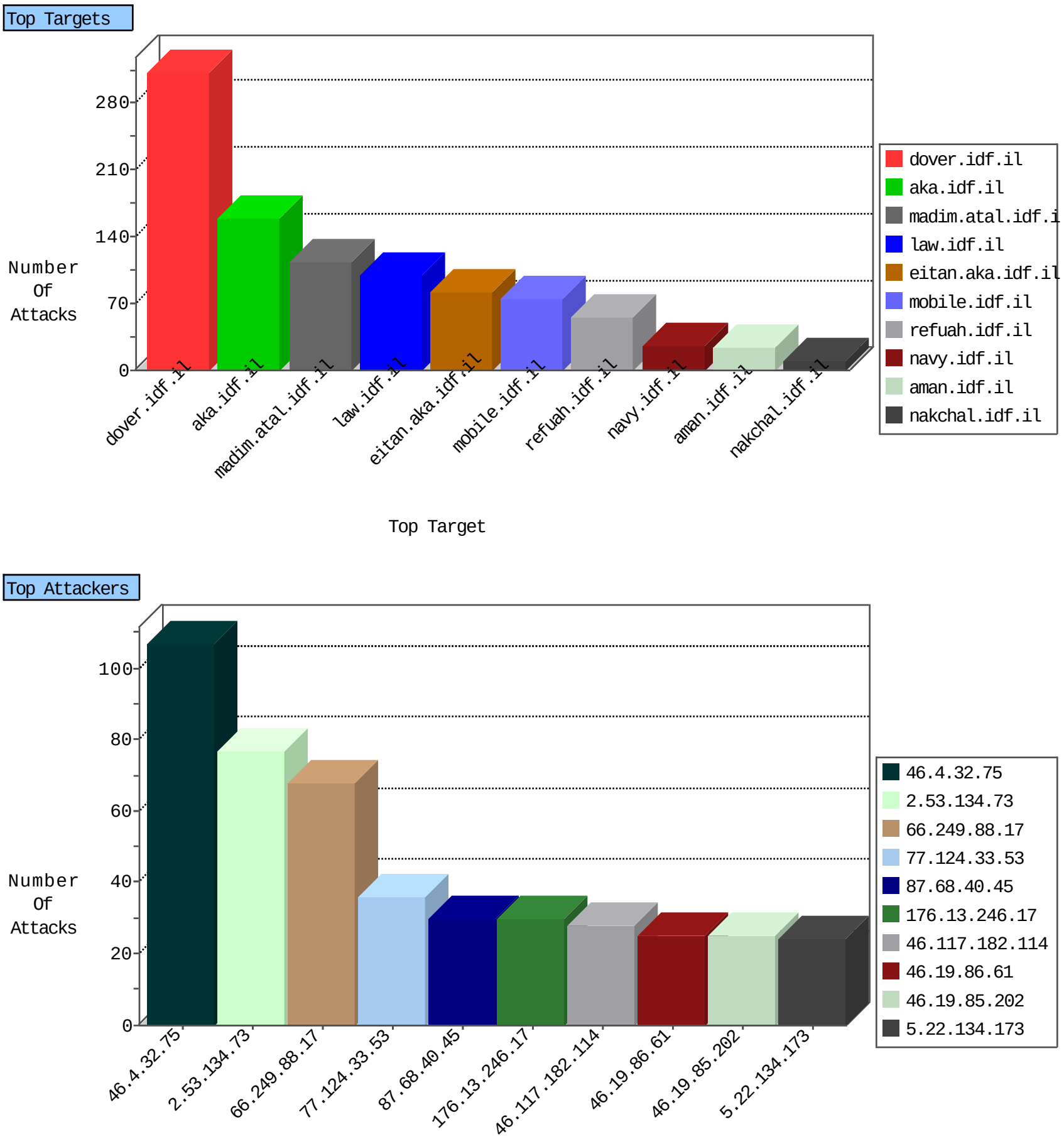
09-16-2016-16:04:09 to 09-16-2016-17:04:09

IDF Under Attack Daily Report



09-16-2016-16:04:09 to 09-16-2016-17:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
79.177.90.244	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.22.150.78	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
46.19.86.54	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1

09-16-2016-16:04:09 to 09-16-2016-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	38
46.4.32.75	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	32
46.4.32.75	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	24
46.4.32.75	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	7
46.4.32.75	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.32.75	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.32.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
182.50.130.136	Singapore	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
36.110.147.108	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-16-2016-16:04:09 to 09-16-2016-17:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.88.17	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	68
109.60.153.178	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.209.70.158	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.249.106.23	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.227.67.158	147.237.72.217	Sweden	e.idf.il	ET SCAN NMAP -sS window 1024	1
5.206.231.131	147.237.76.86	Portugal	navy.idf.il	ET SCAN Potential SSH Scan	1
159.253.38.214	147.237.76.86	Turkey	navy.idf.il	ET WEB_SERVER Poison Null Byte	1
93.158.203.147	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.86	Turkey	navy.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1

09-16-2016-16:04:09 to 09-16-2016-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.124.33.53	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.13.246.17	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
87.68.40.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.117.182.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
46.19.85.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.70.30.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.139.137	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
5.29.110.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.142.183.212	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.164.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.70.30.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
89.160.233.63	Iceland	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
83.56.31.155	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.30.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
93.173.116.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.235.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.108.26.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.3.147.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.26.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.57.141.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
14.185.246.96	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.61	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.108.33.171	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.142.6.122	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.23	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.178.173.206	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.135	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.50	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.134.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
5.22.134.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
2.53.183.42	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	5
46.19.85.92	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	4
77.138.156.59	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
80.246.136.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.126.26.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.57.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.112.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.63	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
37.142.192.138	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	NULL Character in Header Name at [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]]	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
68.180.228.171	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
185.159.36.13		147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Malformed URL ¸[[#20]]¸	Block	1
37.46.38.156	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1129-he/dover.aspx parameter SearchText	Block	1
77.138.214.205	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.117.109.75	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
40.77.167.19	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/robots.txt	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/changelog.txt	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]]	Block	1
2.55.129.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
204.79.180.255	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Multiple Illegal Byte Code Character in Method from 159.253.38.214	Block	1
37.142.9.186	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
79.178.61.223	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
46.120.8.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
40.77.167.75	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]Q7Ûù:'å[[#14]]9}@Â([[#4]][[#23]]7©“\˜™[[#0]]€[[#14]]9;ª¯[[#29]]þ[[#23]]Ø[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À in URL ¸[[#20]]¸	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
77.138.98.233	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ng in URL www.idf.ilhttp/1.1	Block	1
37.142.183.212	Israel	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Multiple Malformed URL from 159.253.38.214	Block	1
2.53.61.47	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
45.79.130.229	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
176.13.19.250	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
5.29.101.83	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.138.135.41	France	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.57.57.27	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
37.142.183.212	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il./favicon.ico	Block	1
159.253.38.214	Turkey	147.237.76.86	navy.idf.il	Multiple NULL Character in Method from 159.253.38.214	Block	1
104.129.194.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.242	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1