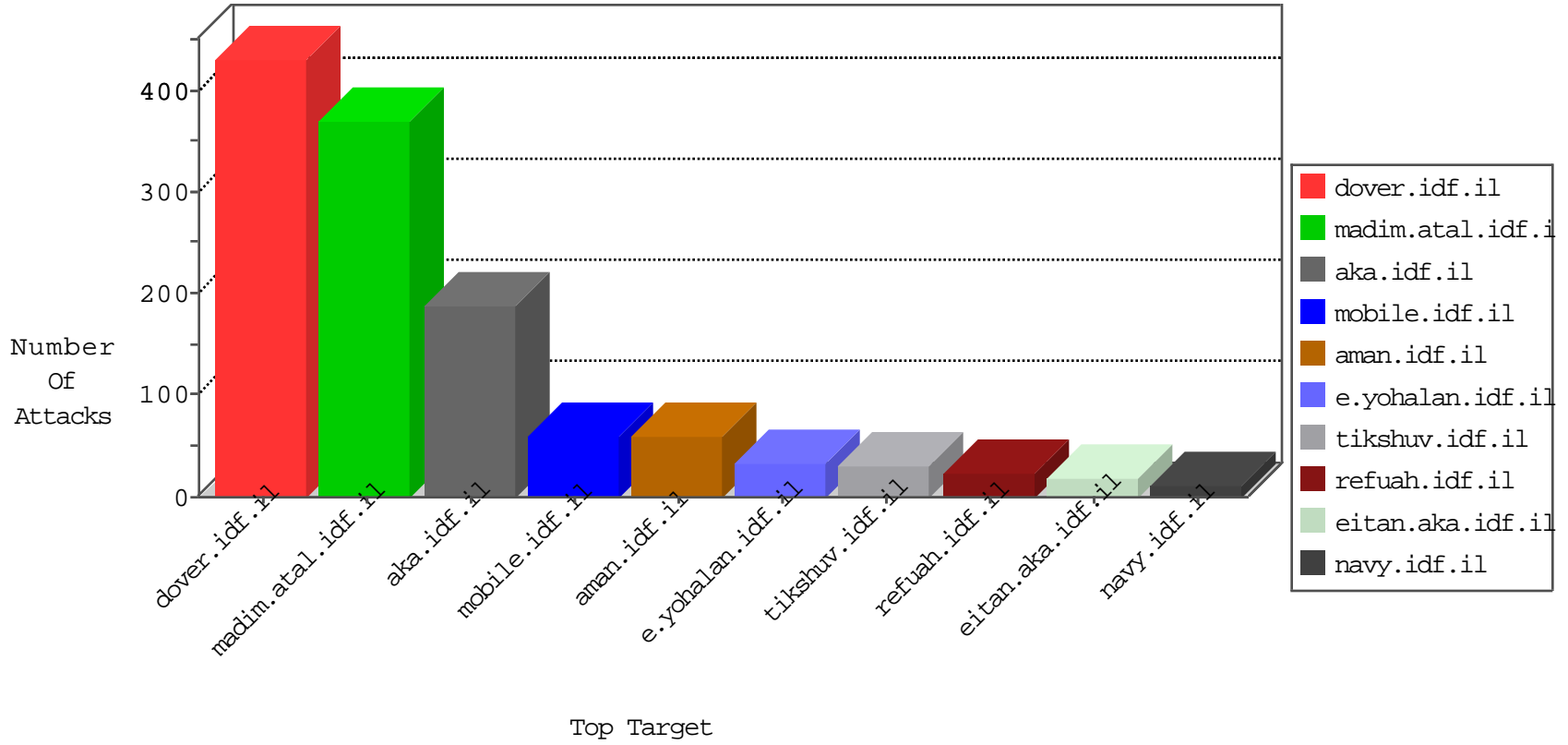


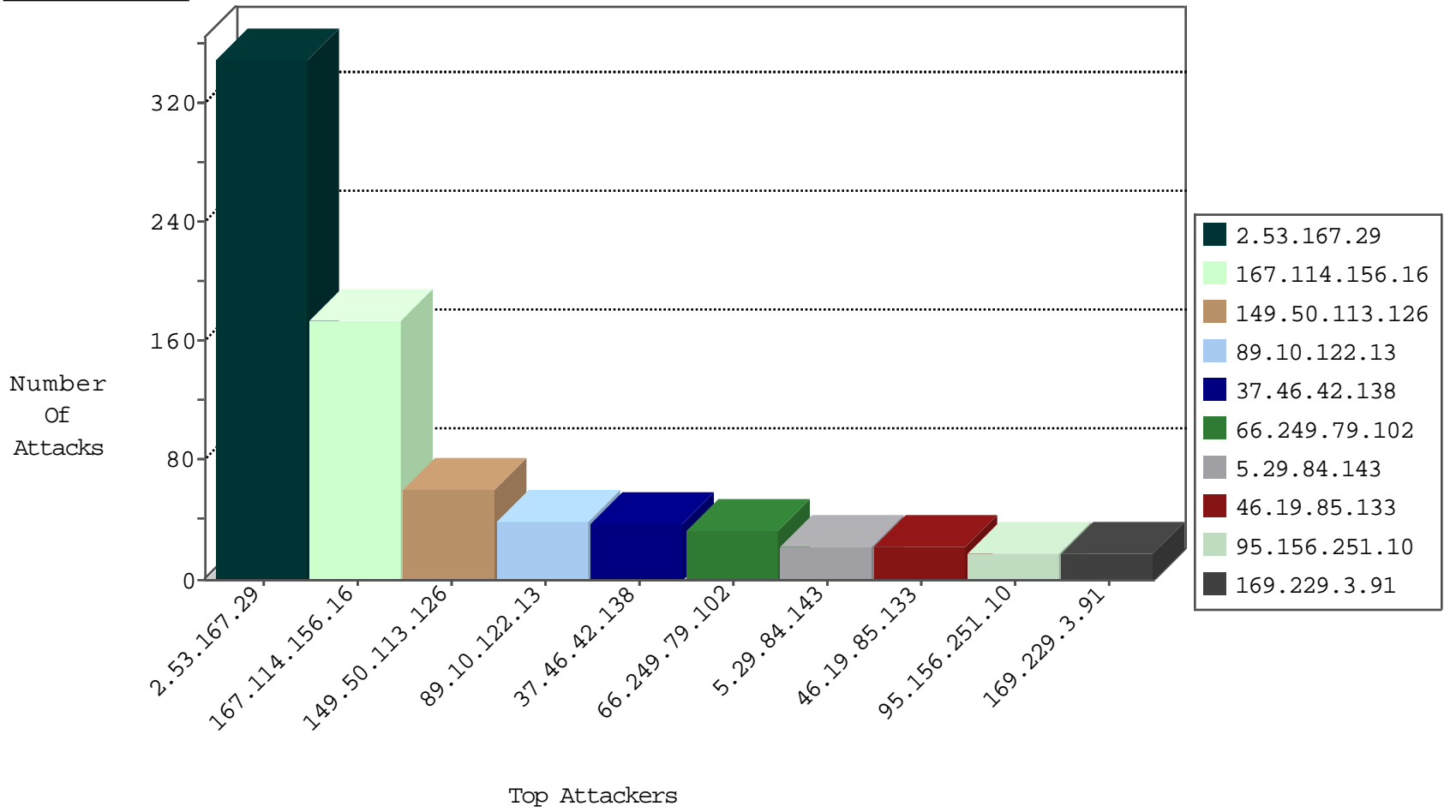
IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	6601
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	234
46.116.50.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
94.102.52.10	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
59.166.246.79	Japan	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

04-30-2016-14:04:02 to 04-30-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	4
80.246.130.133	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
120.199.111.137	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
52.16.5.197	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.100.128	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
120.199.111.137	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
95.156.251.10	147.237.77.243	Germany	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
80.74.125.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
13.92.100.128	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
13.92.100.128	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.10.122.13	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
37.46.42.138	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
5.29.84.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.50.113.126	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
149.50.113.126	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
149.50.113.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
149.50.113.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.97.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.27.105.111	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.14.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.55.47.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.133	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
69.60.111.84	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	11
69.64.48.162	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	11
46.19.85.133	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.3.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.71.62.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.46.42.138	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	8
68.64.167.142	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.220.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.23.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.121.221.15	France	147.237.77.216	dover.idf.il	drop		drop	6
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.135.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.9.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.155.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.42.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.63	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
46.120.255.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
8.37.227.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.8.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.199.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.209.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.167.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	349
79.177.0.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.121.113.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 46.121.113.20	Block	6
5.29.84.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	4
42.200.35.17	Hong Kong	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
176.13.3.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
202.151.171.213	Vietnam	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.252.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/mmmmmmm=d5079062mmmmmmm_d5079062	Block	1
66.249.79.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
46.19.86.28	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.86.28	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
157.55.39.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.65.230	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
42.200.35.17	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 42.200.35.17	Block	1
84.110.34.246	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
188.68.0.46	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.82.88	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dover.aspx ⋅ ½ ε - ε £ ½ ε - ½	Block	1
79.183.155.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 6žãðĕa[#26] in URL	Block	1
66.249.66.5	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/_layouts/authenticate.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
109.65.224.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4466.jpg	Block	1
192.115.99.130	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/112994.pdf	Block	1
66.249.82.91	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.121.113.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	NULL Character in Method	Block	1
157.55.39.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
5.29.109.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.183.220.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 169.229.3.91	Block	1
42.200.35.17	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
109.67.154.100	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.161.61.19	Iceland	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in www.tikshuv.idf.il/site/general.aspx	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	1
157.55.39.251	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.251	Block	1
80.153.42.47	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
176.228.172.229	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/112981.pdf	Block	1
46.19.86.28	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
2.53.167.29	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ***** Observed *****	None	1
109.253.135.82	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1