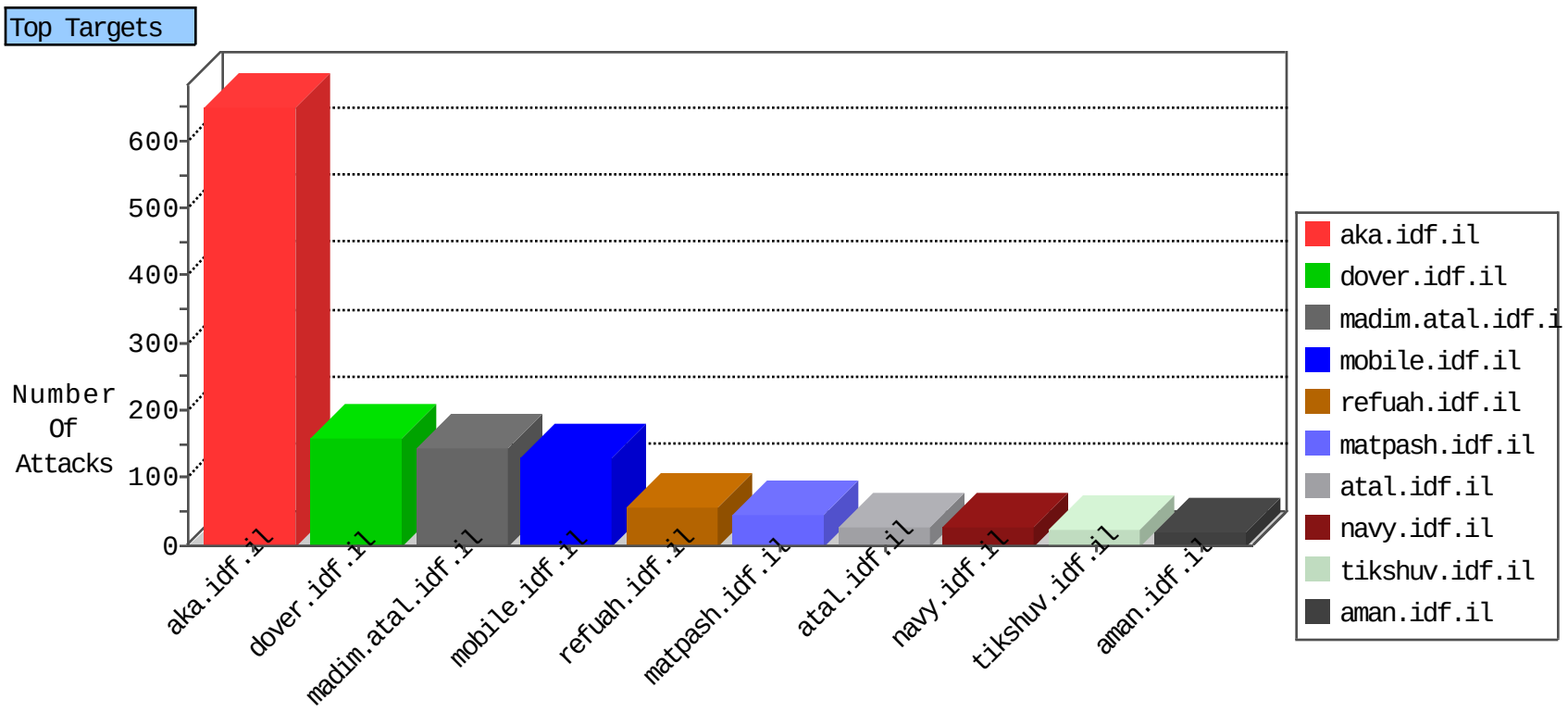
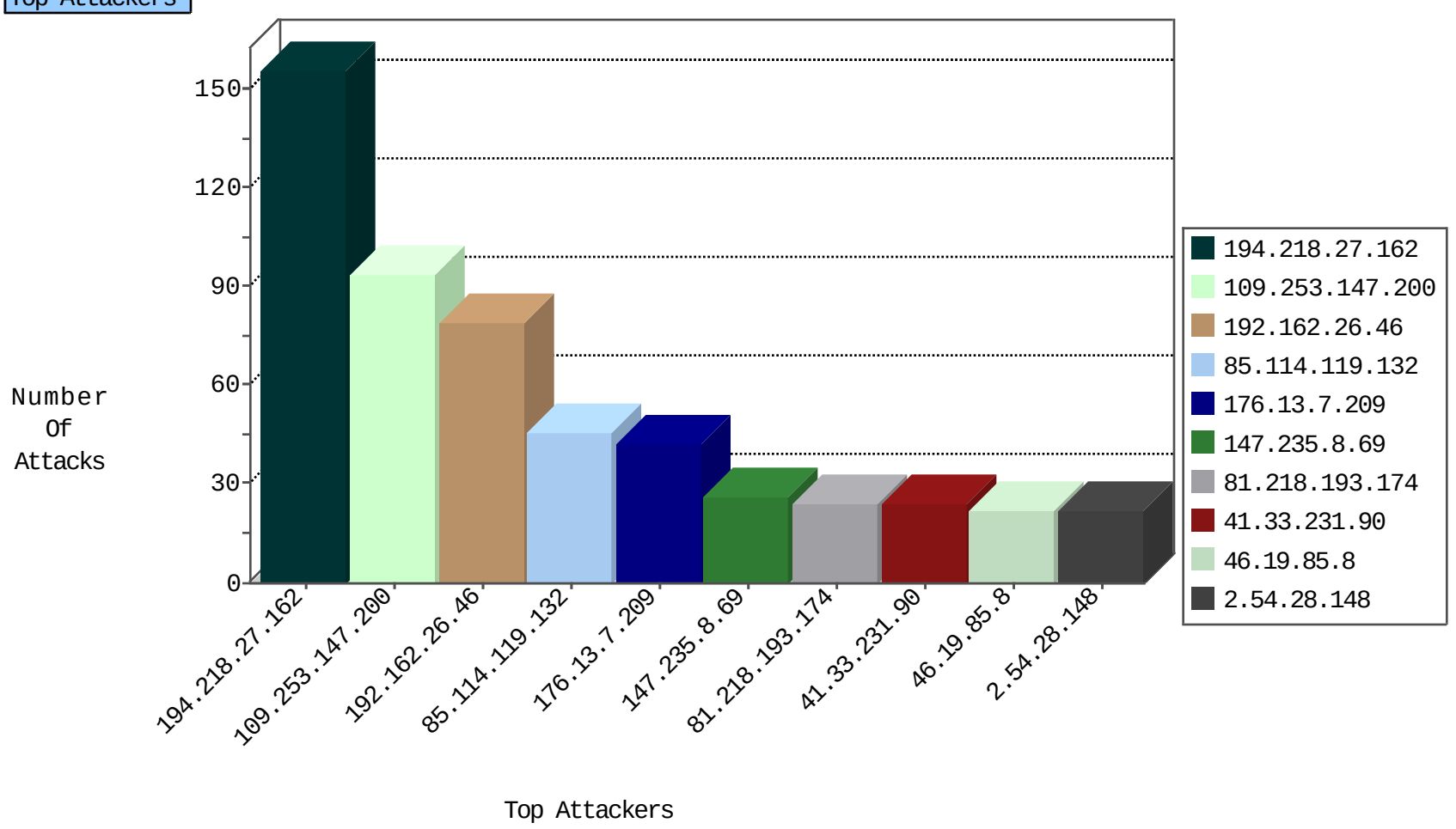
03-01-2016-16:04:01 to 03-01-2016-17:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-01-2016-16:04:01 to 03-01-2016-17:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.112.234	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
37.232.10.242	Georgia	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.i	L4 Source or Dest Port Zero	drop	1
89.248.172.207	Netherlands	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-16:04:01 to 03-01-2016-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.205.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
89.138.83.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.120.21.243	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
85.65.167.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.66.9.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

03-01-2016-16:04:01 to 03-01-2016-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.78.47.72	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
202.71.25.29	147.237.76.198	India	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
79.176.175.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.244.49.137	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
94.199.151.22	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.29.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.210.188.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.87.16.148	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.87.16.148	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.225.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
79.182.139.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.76.198	India	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
79.177.118.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
62.219.139.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.21.248.87	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.77.145.78	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.68.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.168.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.24.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.87.16.148	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.228.168.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
84.109.0.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.228.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-01-2016-16:04:01 to 03-01-2016-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	102
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	51
176.13.7.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
81.218.193.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
77.125.124.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.148.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
147.235.8.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
194.90.25.90	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
85.114.119.132	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
62.219.211.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.192.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.114.119.132	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	9
85.114.119.132	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.25.80.227	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.177.149.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
147.235.8.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
80.246.136.121	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.114.119.132	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.94.92.164	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
147.235.8.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
85.114.119.132	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
93.173.168.178	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.124.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.214.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.125.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.168.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.117.136.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.149.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.183.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.23	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.232.10.242	Georgia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.23	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.197.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
2.54.28.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	6
176.13.7.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
37.115.184.42	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	6
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	6
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	6
80.246.139.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	6
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	5
2.54.190.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	5
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	5
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	5
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	4
213.57.230.187	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	4
2.52.15.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Illegal HTTP Version	Block	3
85.65.97.123	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.97.123	Block	3
2.52.181.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.124.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
212.235.119.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.90.89.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.85.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.65.97.123	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
2.54.1.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.22.129.101	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
77.125.124.248	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
213.57.129.4	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.147.200	Israel	147.237.0.19	madim.atal.idf.il	Automated Vulnerability Scanning V1	Block	1
54.200.74.228	United States	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
46.19.85.170	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
173.200.193.66	United States	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
8.25.222.2	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method º–/tÇˆ]ÇÛäk'EiÐ‹XtÀ¸ž^l!§ in URL ½fm¶.	Block	1
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.246.133.173	Ireland	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
46.120.240.238	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1136-he/navy.aspxhttp:/www.search.ask.com/	Block	1
89.139.158.171	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.183.124.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
37.26.148.232	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method ß Ã‡…cž[[#11]]çTuó	Block	1