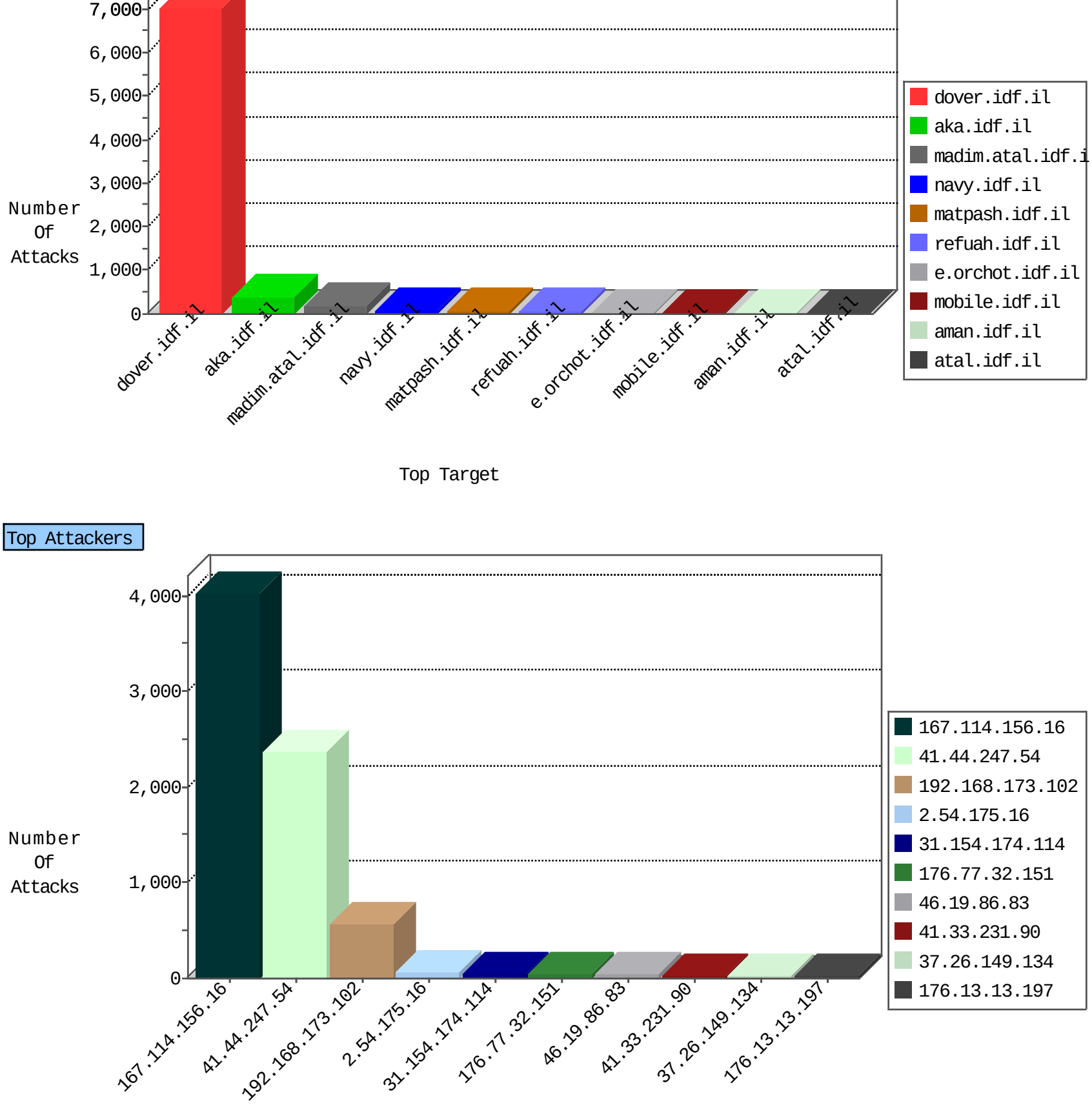
04-08-2016-14:04:04 to 04-08-2016-15:04:04

IDF Under Attack Daily Report



04-08-2016-14:04:04 to 04-08-2016-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4639
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4033
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2719
37.26.146.238	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1408
41.44.247.54	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	56
41.44.247.54	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	12
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.145.218.175	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
204.42.253.2	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	2
87.69.209.108	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
204.42.253.2	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	2
209.126.127.17	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
209.126.127.17	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
209.126.127.17	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
209.126.127.17	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1

04-08-2016-14:04:04 to 04-08-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.249.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-14:04:04 to 04-08-2016-15:04:04

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
66.102.8.243	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.114	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
67.211.217.131	147.237.76.198	United States	e.yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
180.76.170.207	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
42.112.203.241	147.237.77.227	Vietnam	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.226	Indonesia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.167.131	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
31.154.174.114	147.237.0.34	Israel	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
89.248.167.131	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
67.211.217.131	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
67.211.217.131	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
195.16.127.148	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
42.112.203.241	147.237.77.227	Vietnam	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.167.131	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.226	Indonesia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.167.131	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.226	Indonesia	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
67.211.217.131	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
195.16.127.148	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

04-08-2016-14:04:04 to 04-08-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.44.247.54	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2129
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	370
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	192
41.44.247.54	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	159
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
31.154.174.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
176.77.32.151	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
176.13.13.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.77.32.151	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
68.64.167.142	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
69.64.48.162	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	13
46.116.60.76	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
185.3.147.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.174.114	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
69.60.111.84	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.177.88.199	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.94.67.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.64.51.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
173.195.9.157	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.194.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.48.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.57	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
90.148.158.26	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.217.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.57	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.191.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.44.247.54	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.179.88.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.15	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.44.247.54	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.82.76.95	Senegal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.160.237.226	South Africa	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
87.71.47.63	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.241.229.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.148.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.217.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.64.51.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
149.78.105.80	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.117.46.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.252	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.76.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
46.19.86.149	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4

04-08-2016-14:04:04 to 04-08-2016-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.175.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
46.19.86.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
37.26.149.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
164.138.118.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.12.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
37.46.38.22	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	5
131.253.25.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
84.108.104.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.21.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.13.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.132.63.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.142.246.74	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	2
109.253.220.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.25.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method ÑH[[#22]]/.·éÐ‘,^¢ínôu•´[[#2]]ž—ŽWK]#012™ in URL	Block	1
31.154.174.114	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
149.88.60.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
84.94.67.206	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.20.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
109.253.195.244	Israel	147.237.76.86	navy.idf.il	Distributed Cookie Tampering on token: __atrfs	None	1
66.249.93.82	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1
37.8.52.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/recruitlane.aspx	Block	1
66.102.8.238	United States	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	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Name	Block	1
41.44.247.54	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.19.86.226	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
84.109.9.75	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
207.46.13.1	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method ÑH[[#22]]/.·éÐ‘,^¢ínôu•´[[#2]]ž—ŽWK]#012™	Block	1
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
80.246.133.79	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
46.116.60.76	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Abnormally Long Request method	Block	1
37.46.38.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
85.64.78.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Malformed URL	Block	1
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
84.94.67.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.117.45.159	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1

04-08-2016-14:04:04 to 04-08-2016-15:04:04