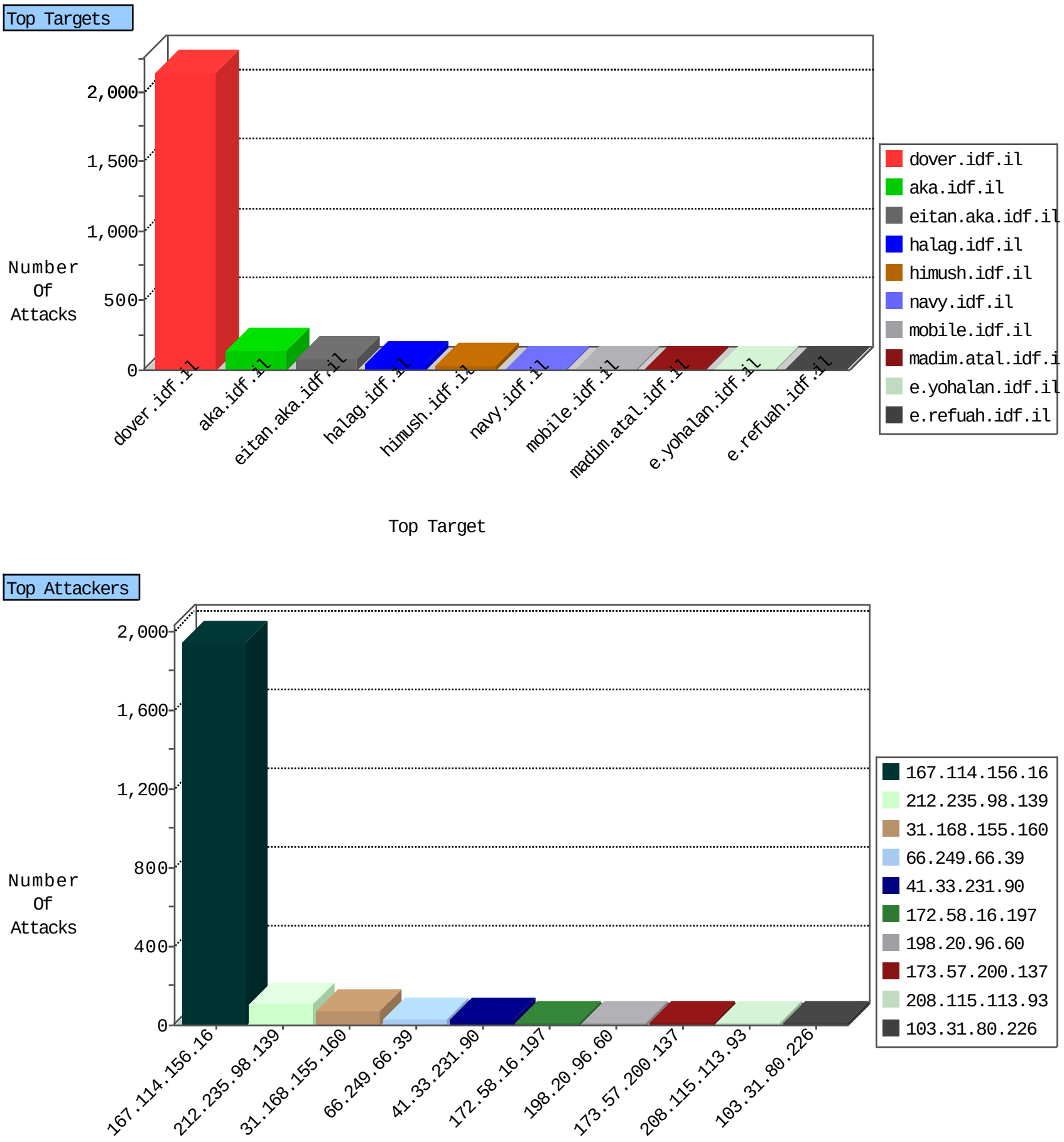
12-16-2015-06:04:02 to 12-16-2015-07:04:02

IDF Under Attack Daily Report



12-16-2015-06:04:02 to 12-16-2015-07:04:02

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	3309
198.20.96.60	Netherlands	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	11
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.93.181	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
198.20.96.60	Netherlands	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.82.64.198	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.181	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

12-16-2015-06:04:02 to 12-16-2015-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.108.62	Netherlands	147.237.77.216	dover.idf.il	3643: HTTP: Nikto HTTP Request	Block	1
198.20.96.60	Netherlands	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1

12-16-2015-06:04:02 to 12-16-2015-07:04:02

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.223	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
103.31.80.226	147.237.76.201	Pakistan	e.atal.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.8.24	Indonesia	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
103.31.80.226	147.237.76.198	Pakistan	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.176	Pakistan	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.86	Pakistan	navy.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.39	Pakistan	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.34	Pakistan	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.218.246.103	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.198	United States	e.yohalan.idf.il	ET DROP Dshield Block Listed Source	1
128.199.207.123	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
36.72.228.72	147.237.8.24	Indonesia	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
103.31.80.226	147.237.76.200	Pakistan	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.8.24	Indonesia	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
103.31.80.226	147.237.76.196	Pakistan	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.148	Pakistan	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.44	Pakistan	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.38	Pakistan	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.31	Pakistan	nakchal.idf.il	ET SCAN Potential SSH Scan	1
80.82.70.230	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

12-16-2015-06:04:02 to 12-16-2015-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	108
31.168.155.160	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
173.57.200.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
172.58.16.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
207.241.226.40	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
109.64.135.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.183.56.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
172.58.16.197	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.57.119.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.2.143	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.42.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
168.244.4.57	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
168.244.4.57	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
65.55.210.129	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.42	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
105.197.172.249	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.120.148.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.178.51.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
171.208.221.246	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.114	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
149.50.87.164	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
208.120.46.224	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
2.52.132.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.162	China	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.11	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
171.208.221.246	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.80	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.146.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
121.54.44.91	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.36	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
171.208.221.246	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.50.87.164	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.66.96.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.74	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.11	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

12-16-2015-06:04:02 to 12-16-2015-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	12
121.241.127.12	India	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.241.127.12	Block	6
176.13.2.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.250.148.225	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 80.250.148.225	Block	3
66.249.66.83	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17728.jpg	Block	2
213.8.174.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.229.27	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.77	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.152	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
198.20.96.60	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/	Block	2
208.115.111.74	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/miluim/scriptresource.axd	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
2.54.135.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.66.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/miluim/scriptresource.axd	Block	1
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	Block	1
66.249.75.15	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.15	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
121.241.127.12	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/mailthis.gif	Block	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
217.132.249.126	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.146.225	Block	1
46.19.85.176	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.189	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
69.171.228.122	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
217.132.249.126	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 217.132.249.126	None	1
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
52.53.216.61	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17923-he/dover....	Block	1
174.19.180.3	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
180.76.15.21	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
2.52.15.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Suspicious Response Code	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/8/size220x0/17728.jpg	Block	1

12-16-2015-06:04:02 to 12-16-2015-07:04:02