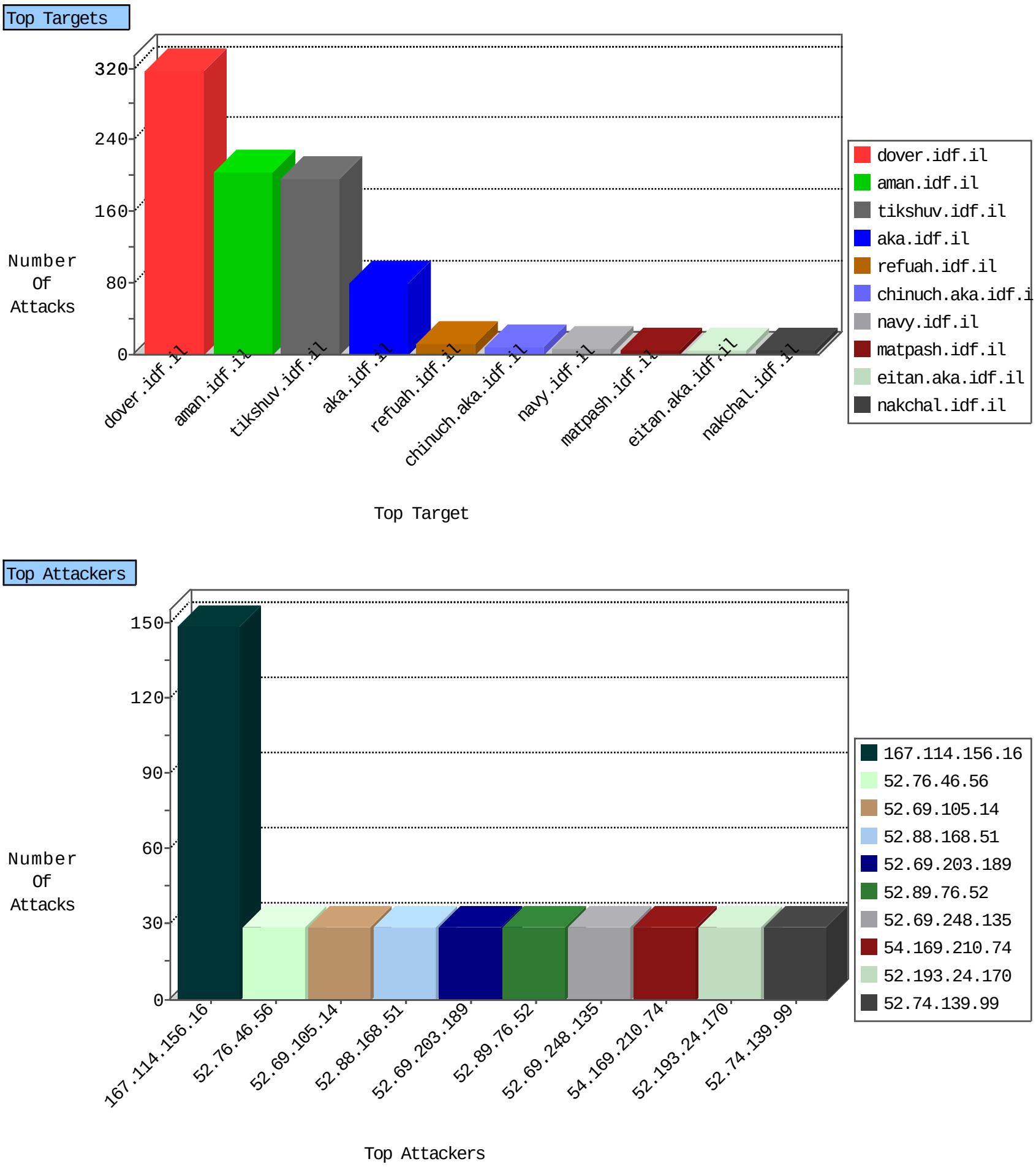
12-29-2015-01:07:21 to 12-29-2015-02:07:21

IDF Under Attack
Daily Report



12-29-2015-01:07:21 to 12-29-2015-02:07:21

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	2243
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	5
86.21.240.225	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
199.30.16.163	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
66.249.66.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.99.131.107	Canada	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
192.99.131.107	Canada	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

12-29-2015-01:07:21 to 12-29-2015-02:07:21

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-29-2015-01:07:21 to 12-29-2015-02:07:21

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
151.217.178.88	147.237.77.234		halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.55.154.39	147.237.77.234	Brazil	halag.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.121		e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.55.154.39	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.55.154.39	147.237.77.178	Brazil	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.18	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
177.55.154.39	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
201.172.190.154	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.55.154.39	147.237.76.200	Brazil	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
197.45.153.74	147.237.76.196	Egypt	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
177.55.154.39	147.237.76.177	Brazil	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
177.55.154.39	147.237.76.38	Brazil	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
188.152.249.142	147.237.77.121	Italy	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
177.55.154.39	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
12.139.41.189	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
177.55.154.39	147.237.77.243	Brazil	mobile.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.178		e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.55.154.39	147.237.77.233	Brazil	atal.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.76.30		himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.55.154.39	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.55.154.39	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
177.55.154.39	147.237.77.19	Brazil	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
197.45.153.74	147.237.76.196	Egypt	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
177.55.154.39	147.237.76.198	Brazil	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
197.45.153.74	147.237.76.196	Egypt	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
177.55.154.39	147.237.76.176	Brazil	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
189.214.79.107	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
177.55.154.39	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 4096	1

12-29-2015-01:07:21 to 12-29-2015-02:07:21

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
52.74.139.99	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
54.69.147.194	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.69.203.189	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.193.24.170	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.68.74.251	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.88.168.51	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.76.32.115	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.69.248.135	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
54.65.161.147	Japan	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.69.105.14	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.89.76.52	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.76.46.56	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
54.169.210.74	Singapore	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.68.74.251	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.88.168.51	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.76.32.115	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.69.248.135	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
54.65.161.147	Japan	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.69.105.14	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.89.76.52	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.76.46.56	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
54.169.210.74	Singapore	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.74.139.99	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
54.69.147.194	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.69.203.189	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
52.193.24.170	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
37.142.208.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.80.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.174.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.36.157.155	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
171.234.164.14	Vietnam	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
93.158.36.65	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.28.168.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
107.20.171.193	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.134	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.25.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.21.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-29-2015-01:07:21 to 12-29-2015-02:07:21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.123.214	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.123.214	Block	3
2.52.41.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.28	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.6.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
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	2
37.142.68.5	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.208.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.154.194.111	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.121.129.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.237	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/home/jserror	Block	1
8.37.71.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8888-he/navy.aspx&usg=alkjrhhazlc6ggmzkn-kgwy6lmsdcglglg	Block	1
93.158.36.65	United Kingdom	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
69.163.144.125	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
213.136.70.175	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
66.249.64.169	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/homepage.aspx/scriptresource.axd	Block	1
180.76.15.7	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.185.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
46.166.137.194	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.168.80.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
180.76.15.148	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.170	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
2.52.41.154	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
86.91.231.125	Netherlands	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19915-he/dover.aspx	Block	1
46.166.190.147	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.13.21.81	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.123.214	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ahukewikxjos1__jahxkvhqkhd2zaoyqfggimaa&sig2=cgkifoepjcwzlv3zhi58yq&usg=afqjcnhcdsh5ryhkeugapxldsq7fowjwnw	Block	1
31.168.181.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.107.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.157.245.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/pricing	Block	1
66.249.64.202	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
109.201.154.197	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ana in URL	Block	1
5.29.160.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
86.91.231.125	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
207.46.13.0	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.66.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
54.162.41.178	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
177.55.96.221	Brazil	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	1
95.90.251.149	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.195.239	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
195.154.194.111	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1

12-29-2015-01:07:21 to 12-29-2015-02:07:21