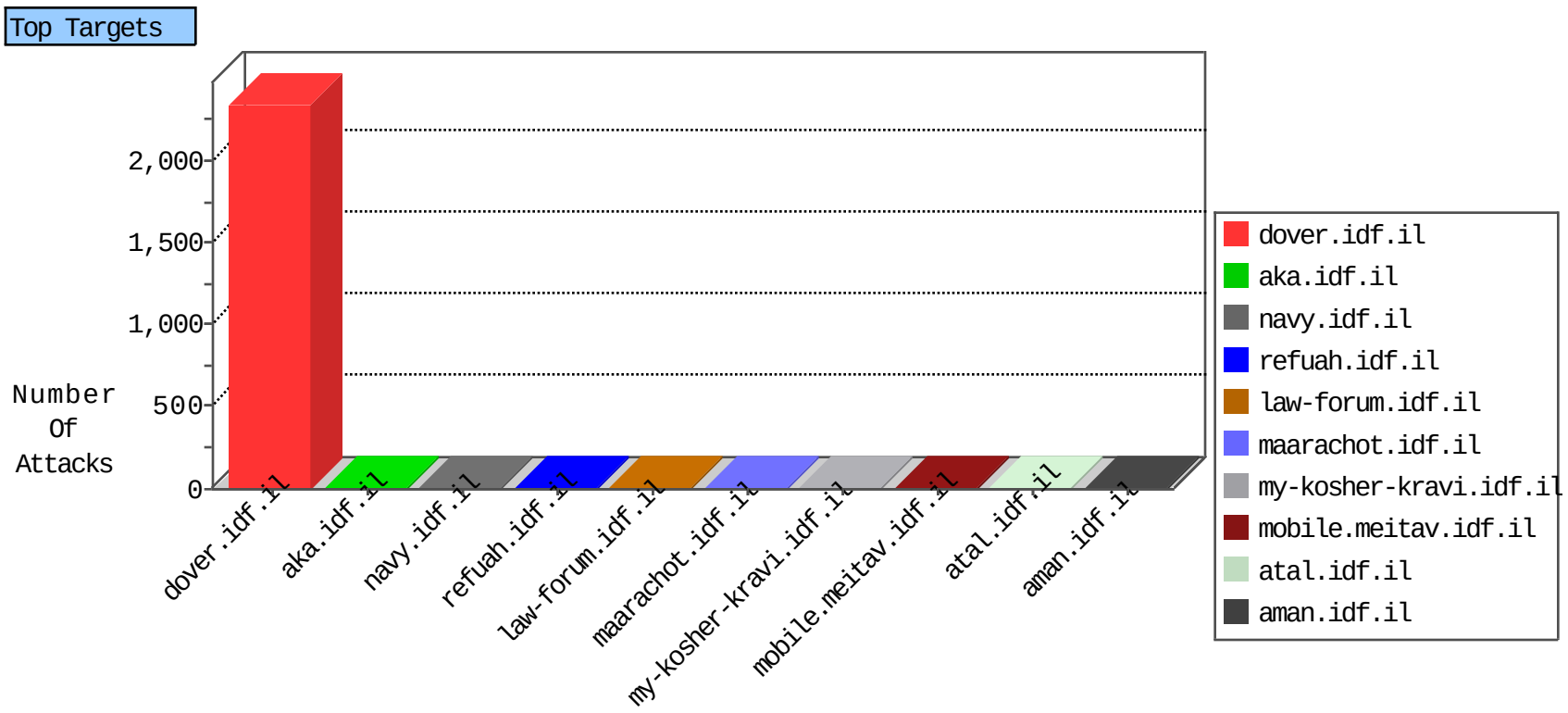
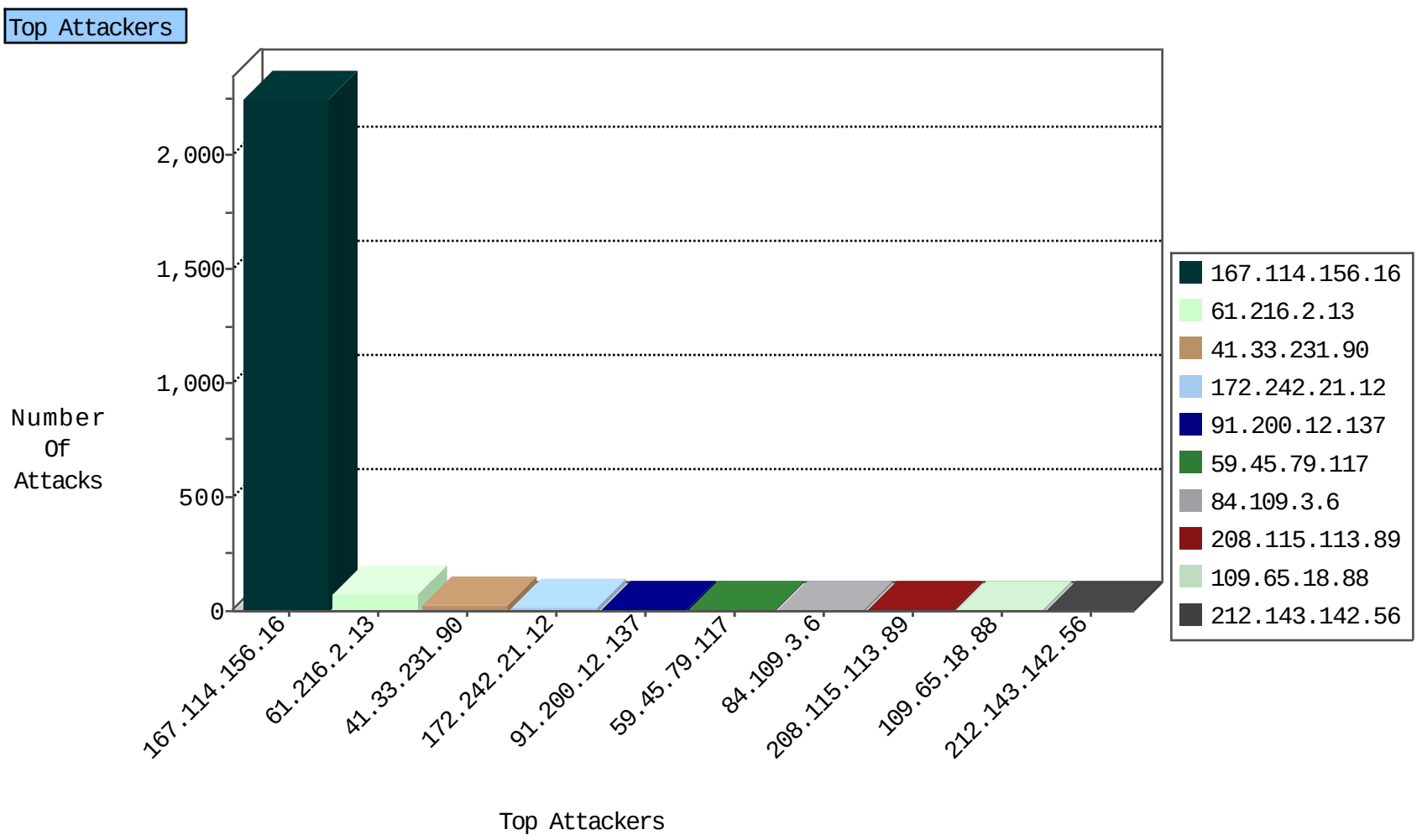
12-07-2015-03:04:00 to 12-07-2015-04:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-07-2015-03:04:00 to 12-07-2015-04:04:00

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	3702
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	449
172.242.21.12	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
172.242.21.12	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
108.232.0.17	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
172.242.21.12	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	1

12-07-2015-03:04:00 to 12-07-2015-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-07-2015-03:04:00 to 12-07-2015-04:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
61.216.2.13	147.237.76.177	Taiwan	ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.65.43	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.2	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
77.29.38.130	147.237.0.17	Macedonia, the Former Yugoslav Republic of	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.115.58.160	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.216.2.13	147.237.76.38	Taiwan	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.216.2.13	147.237.72.156	Taiwan	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.2	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
128.199.60.57	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
40.115.58.160	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
61.216.2.13	147.237.76.86	Taiwan	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.216.2.13	147.237.76.30	Taiwan	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.216.2.13	147.237.8.46	Taiwan	e.chinuch.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

12-07-2015-03:04:00 to 12-07-2015-04:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
61.216.2.13	Taiwan	147.237.77.19	law-forum.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
61.216.2.13	Taiwan	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
61.216.2.13	Taiwan	147.237.76.86	navy.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.137	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
61.216.2.13	Taiwan	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
61.216.2.13	Taiwan	147.237.76.39	mobile.meitav.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
109.65.18.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
61.216.2.13	Taiwan	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
109.236.82.50	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.8	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
61.216.2.13	Taiwan	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.3.144.13	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
61.216.2.13	Taiwan	147.237.0.35	akaws.idf.il	drop		drop	2
61.216.2.13	Taiwan	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
198.50.200.135	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
172.242.21.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
61.216.2.13	Taiwan	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
61.216.2.13	Taiwan	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.44.55.20	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.216.2.13	Taiwan	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
142.4.213.25	Canada	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.166.188.199	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
89.31.57.5	Italy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
61.216.2.13	Taiwan	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
61.216.2.13	Taiwan	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.123	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
61.216.2.13	Taiwan	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.55	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
61.216.2.13	Taiwan	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.82	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.123	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
61.216.2.13	Taiwan	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.199.60.57	Singapore	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.127.203.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
61.216.2.13	Taiwan	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
193.90.12.90	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
61.216.2.13	Taiwan	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
61.216.2.13	Taiwan	147.237.0.33	idf.il	drop		drop	1
5.52.5.57	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.124	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

12-07-2015-03:04:00 to 12-07-2015-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-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/1133-22461-he/dover.aspx.	Block	2
96.23.158.72	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
61.216.2.13	Taiwan	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /	Block	1
41.228.167.4	Tunisia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
125.212.121.172	Philippines	147.237.77.74	law.idf.il	PHP Attempt	Block	1
80.246.136.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1283-en/dover.aspx	Block	1
178.154.243.93	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
61.216.2.13	Taiwan	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1238-he/atal.aspx	Block	1
61.216.2.13	Taiwan	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
192.195.154.172	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
41.228.167.4	Tunisia	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
125.212.121.172	Philippines	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
95.108.158.173	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/1133-he/dover.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1397-en/dover.aspx	Block	1
178.154.243.96	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
61.216.2.13	Taiwan	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
5.255.253.116	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
195.62.53.168	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to /css/css	Block	1
46.117.24.227	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
130.193.50.11	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
95.108.158.191	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1438-he/dover.aspx	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
178.154.243.114	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
61.216.2.13	Taiwan	147.237.76.86	navy.idf.il	Multiple Untraceable SSL Sessions from 61.216.2.13 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
5.255.253.166	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.176.216.1	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
136.243.36.96	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×″×?×ª×¨	Block	1
61.216.2.13	Taiwan	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 61.216.2.13 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
96.23.158.72	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71652-he/maarachot.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/june/kkkkkkk=cb7c1679kkkkkkk_cb7c1679	Block	1
61.216.2.13	Taiwan	147.237.76.86	navy.idf.il	Suspicious Response Code	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.18.88	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
79.176.216.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1

12-07-2015-03:04:00 to 12-07-2015-04:04:00