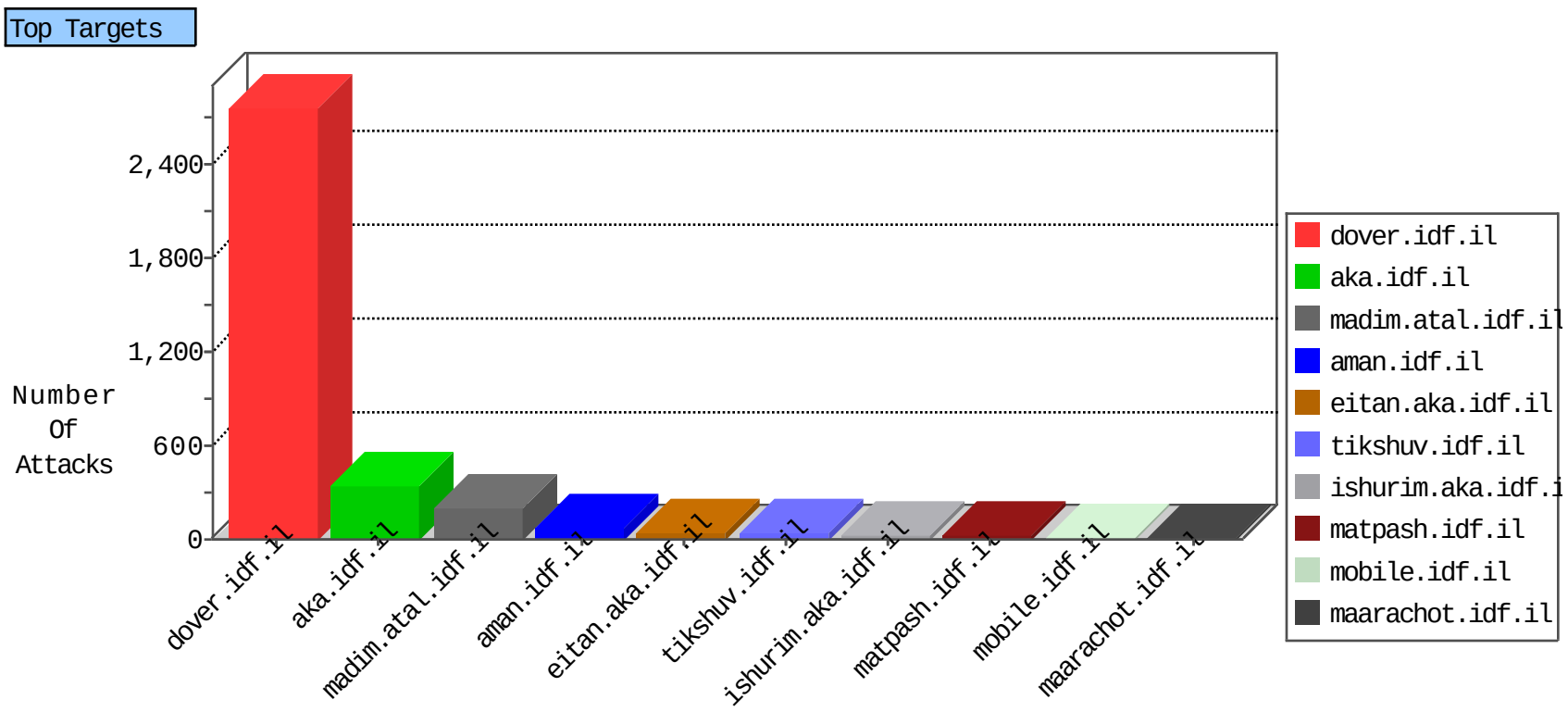
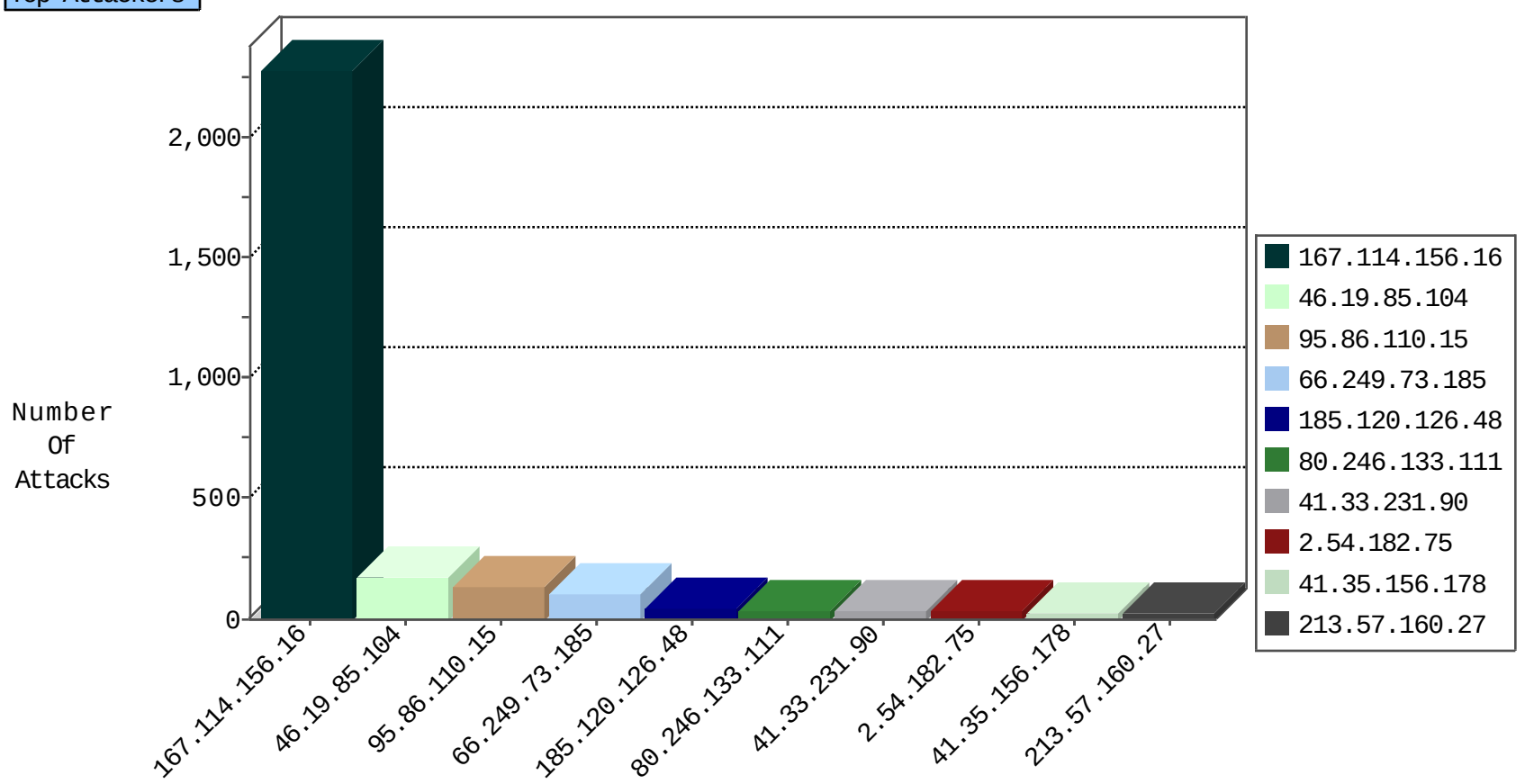
11-27-2015-09:04:05 to 11-27-2015-10:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-27-2015-09:04:05 to 11-27-2015-10:04:05

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	3460
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
115.231.222.40	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
93.174.93.151	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.37	China	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.161	China	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.161	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.36	China	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

11-27-2015-09:04:05 to 11-27-2015-10:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.218.29.20	Ukraine	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	1
159.253.145.150	United States	147.237.77.233	atal.idf.il	C095: Suspicious Addresses MFA	Permit	1

11-27-2015-09:04:05 to 11-27-2015-10:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
91.218.29.20	147.237.77.176	Ukraine	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
209.126.230.71	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.71	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.212	United States	e.dover.idf.il	ET DROP Dshield Block Listed Source	1
176.209.222.35	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
210.50.197.154	147.237.0.34	Australia	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.230.71	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
200.113.127.147	147.237.0.200	Chile	m4u.idf.il	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
176.209.222.35	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

11-27-2015-09:04:05 to 11-27-2015-10:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	104
95.86.110.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.126.48		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	30
41.35.156.178	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
41.35.142.34	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.53.233		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
100.100.103.55		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
95.86.110.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
185.120.126.48		147.237.72.156	aman.idf.il	drop	SAM rule	drop	14
95.86.110.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
95.86.110.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
2.52.168.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
95.86.110.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
100.100.102.20		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
197.231.70.64	Gabon	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	11
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
100.100.72.50		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
80.246.137.49	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
185.32.179.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.39	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.182.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.182.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.182.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.182.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.182.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.187	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.128.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.128.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
149.88.221.182	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
100.100.48.212		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.133.234	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.64.162		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.173	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.183.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.31	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.137.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.102.254.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.28.146.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
149.88.221.182	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.52.6.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.57.129.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
185.3.146.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.103	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
197.231.70.64	Gabon	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

11-27-2015-09:04:05 to 11-27-2015-10:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
80.246.133.111	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.133.111	Block	31
78.156.118.38	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.19.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.177.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
84.228.22.125	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.228.22.125	Block	3
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	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.85.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.172	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
185.32.179.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.137	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
84.228.30.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.91	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.182.133.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
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
5.102.246.130	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
93.173.243.179	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.0.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.18.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method m.facebook.katana in URL	Block	1
116.75.0.141	India	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
79.178.144.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 112 cookies	Block	1
37.26.149.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
2.54.19.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
92.98.41.188	United Arab Emirates	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.154.168.82	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
85.65.104.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.208.242.133	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
40.77.167.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
116.68.101.43	India	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
79.183.33.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.245.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
209.126.230.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
5.102.246.130	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
93.173.243.179	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
89.139.180.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	1
80.246.139.103	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
121.122.172.61	Malaysia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
79.179.99.94	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
213.151.38.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyuss	Block	1

11-27-2015-09:04:05 to 11-27-2015-10:04:05