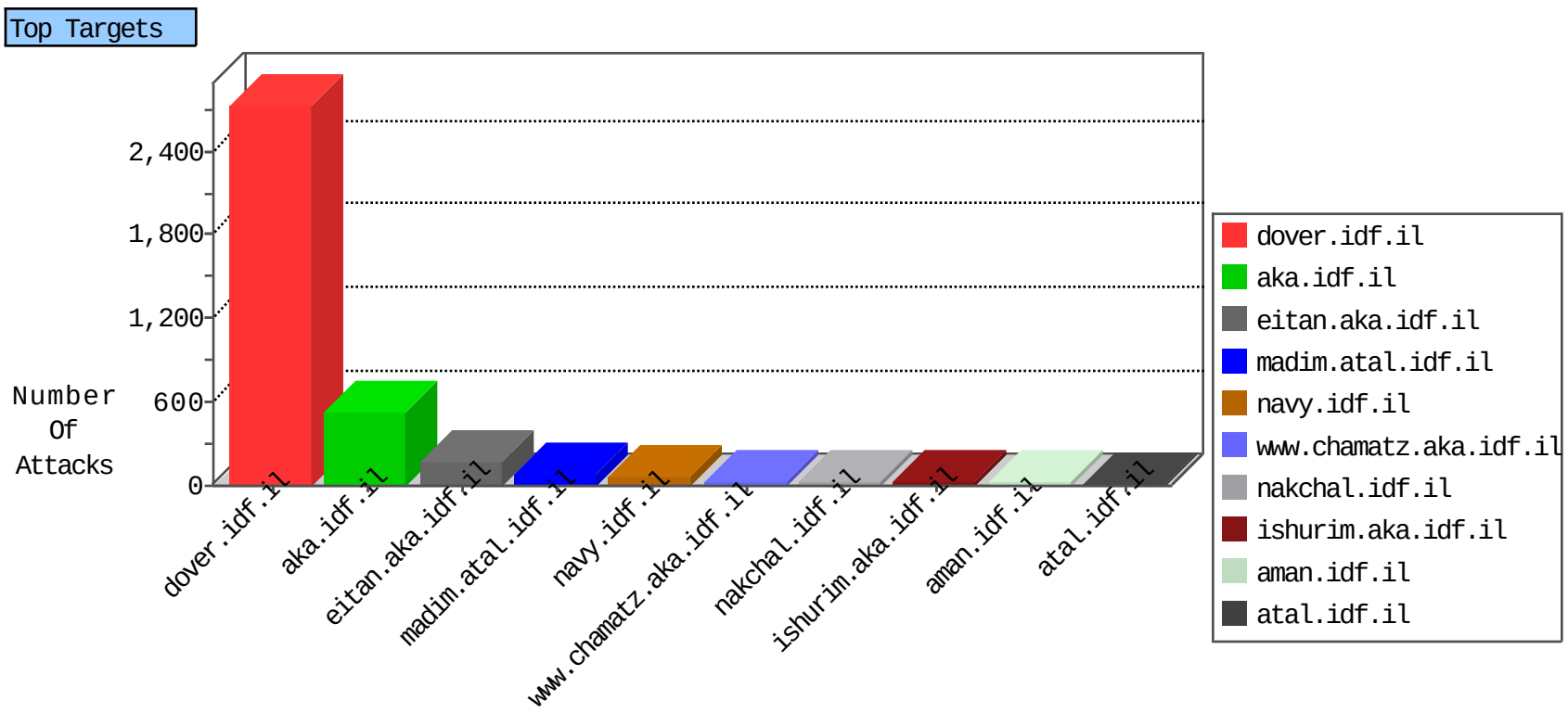
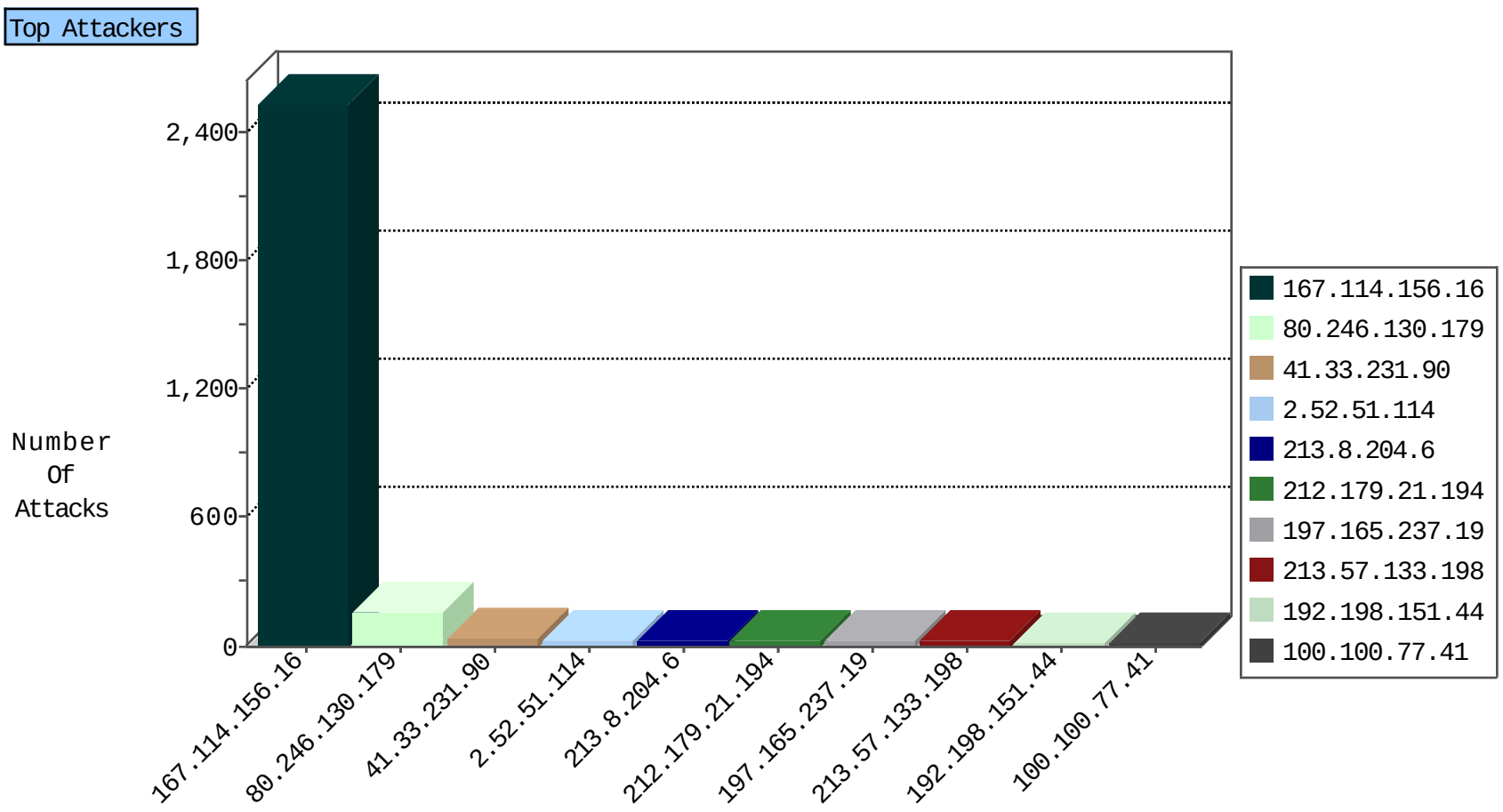
12-01-2015-16:04:09 to 12-01-2015-17:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-01-2015-16:04:09 to 12-01-2015-17:04:09

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	3396
185.56.82.38	Netherlands	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.151	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-01-2015-16:04:09 to 12-01-2015-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.165.237.19	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	3
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-01-2015-16:04:09 to 12-01-2015-17:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
197.165.237.19	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	3
197.165.237.19	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
185.32.179.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.8.151.156	147.237.76.31	India	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
223.71.218.38	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
89.138.174.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.71.218.38	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
84.228.0.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.98.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.68.111.242	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
36.72.228.72	147.237.8.28	Indonesia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
185.32.179.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.218.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.167.88	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
223.71.218.38	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
87.69.227.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.133.168.99	147.237.77.216	Korea, Republic of	dover.idf.il	portscan: TCP Distributed Portscan	1
79.106.109.231	147.237.77.216	Albania	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-01-2015-16:04:09 to 12-01-2015-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.51.114	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
100.100.77.41		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
192.198.151.44	Europe	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
213.57.133.198	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
80.21.83.242	Italy	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
31.168.28.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.138.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
213.57.138.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
213.57.129.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
213.57.129.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.114.23.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.13.165.71	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.93.234	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.244	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.178.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.28.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.144.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.139.144.182	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.64.28.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.144.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.13.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.38	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.163.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.17.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.101.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.28.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.201.17	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
95.225.68.205	Italy	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
109.160.244.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.168.29.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
195.160.240.11	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.65	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.115.67.55	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.13	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
40.77.167.14	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

12-01-2015-16:04:09 to 12-01-2015-17:04:09

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.13	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
100.100.25.247		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.116.98.44	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4

12-01-2015-16:04:09 to 12-01-2015-17:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.179	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
213.8.204.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
197.165.237.19	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.165.237.19	Block	14
85.64.36.107	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.36.107	Block	11
80.246.130.179	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 80.246.130.179	Block	8
31.168.28.177	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	7
176.13.10.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.168.28.177	Israel	147.237.76.31	nakchal.idf.il	Post Request - Missing Content Type from 31.168.28.177	Block	5
2.54.35.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.35.65	Block	4
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.168.28.177	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	3
31.168.28.177	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.168.28.177	Block	3
176.13.4.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.226	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.85.226	None	3
216.180.241.106	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.11.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.3.66	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	2
31.168.28.177	Israel	147.237.76.31	nakchal.idf.il	Post Request - Missing Content Type	Block	2
2.54.163.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.174.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
45.55.36.68		147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.105.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
45.55.36.68		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
216.180.241.106	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	2
46.120.145.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
185.13.193.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.136.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.180.241.106	United States	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
176.13.4.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.133.246	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/1133-22638-he/dover.aspx.	Block	1
45.55.36.68		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.55.36.68	Block	1
109.67.217.139	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
95.86.107.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.121.94.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.41.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.74.169	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
46.19.85.226	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
176.12.138.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.215.94	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
79.176.146.98	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
197.45.173.51	Egypt	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
40.77.167.14	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-01-2015-16:04:09 to 12-01-2015-17:04:09