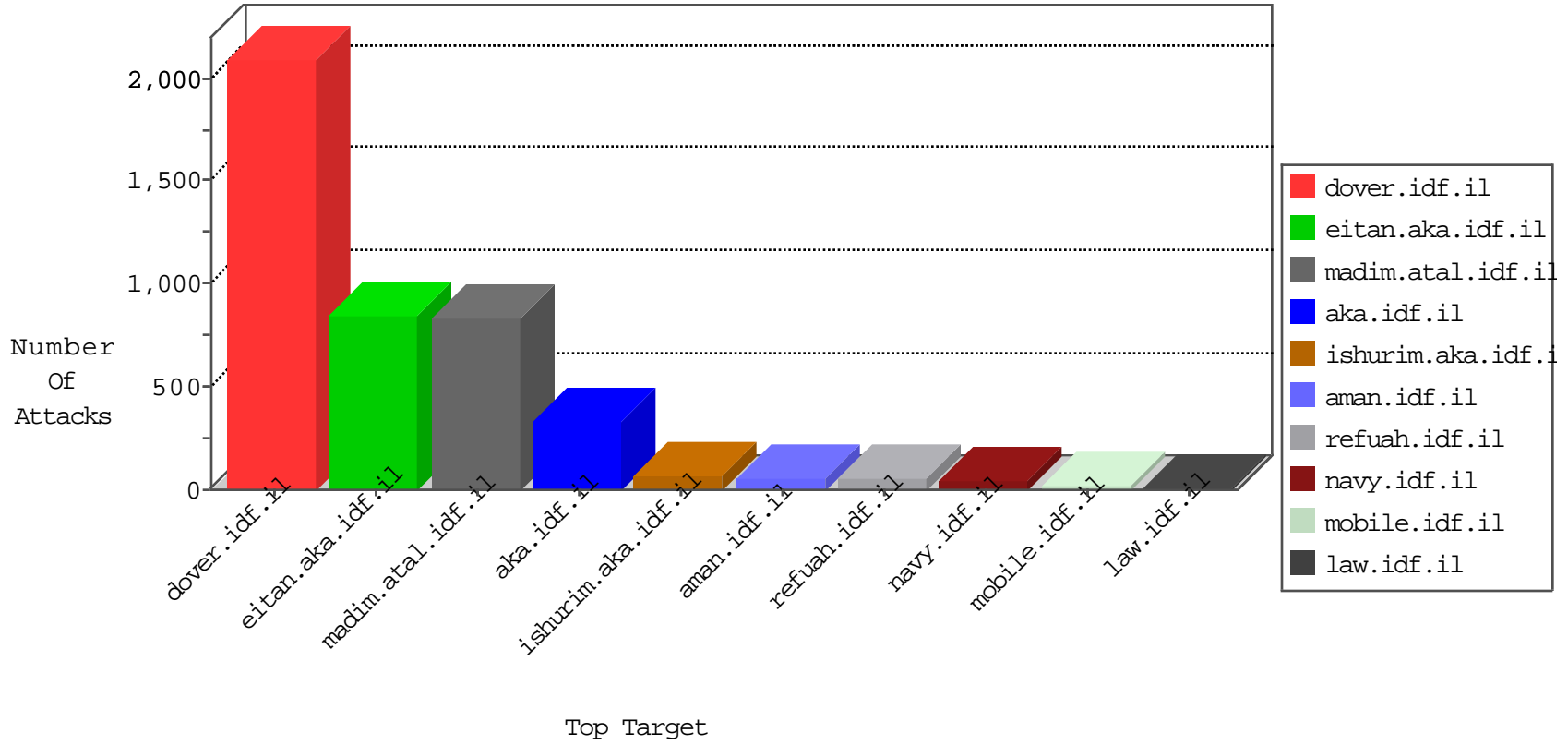


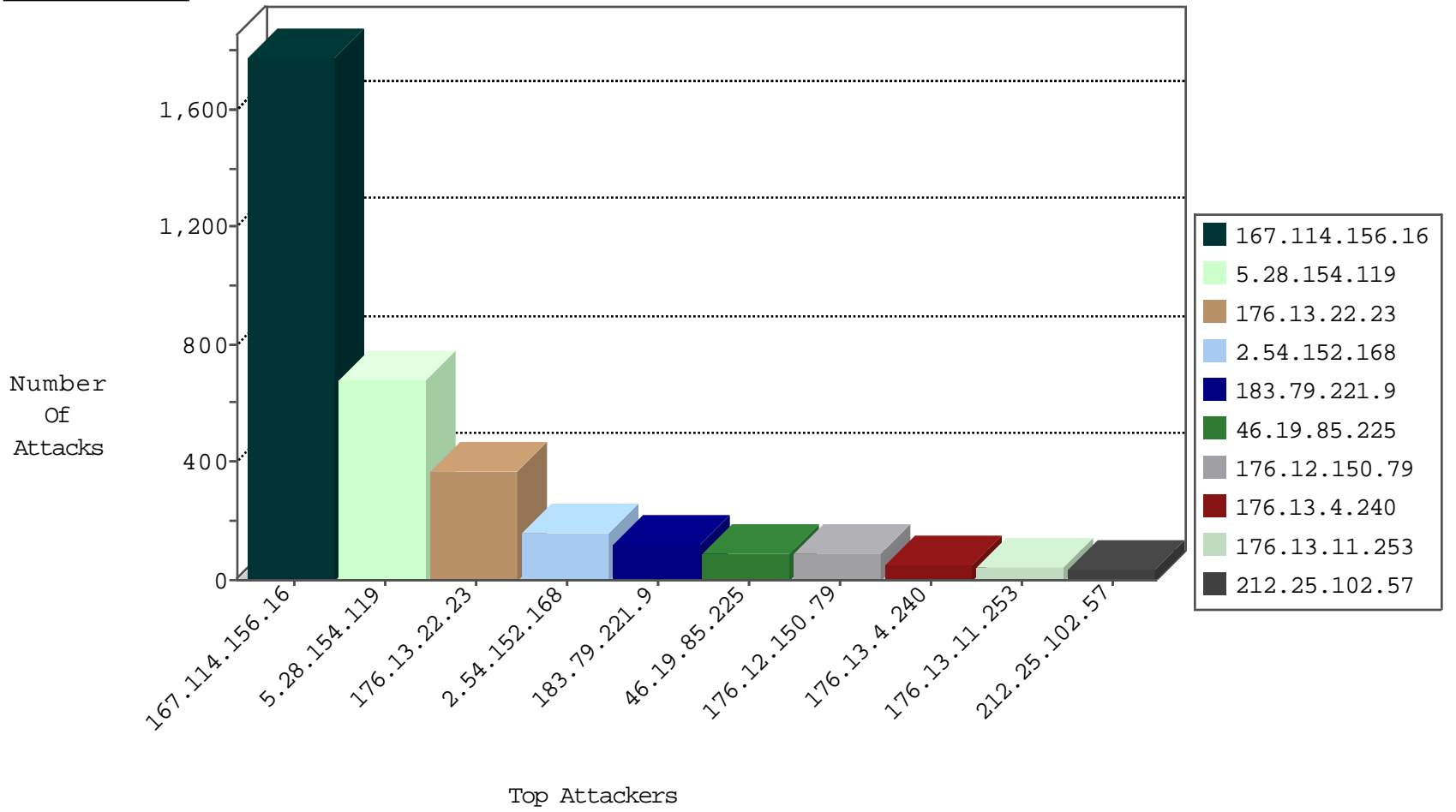
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3173
37.142.68.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
82.102.171.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
62.90.161.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
188.247.75.151	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
37.26.149.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.80.217.70	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
82.80.217.70	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
194.90.115.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
118.193.23.46	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
124.36.104.164	Japan	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
58.187.37.103	Vietnam	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

12-14-2015-09:04:04 to 12-14-2015-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.74.125.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
185.32.179.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.203.27.83	147.237.8.27	India	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.64.58.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.64.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
192.115.123.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.188.125.12	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.233.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.99.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.52.161.177	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP Setup.php access	1
37.26.146.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.12.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.28.154.119	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	591
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	81
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.54.152.168	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
81.199.122.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	24
207.241.229.110	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
46.19.85.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
5.102.254.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
2.52.176.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
80.178.189.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
37.142.148.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.54.62.147	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
213.8.159.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
185.18.206.194	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
62.90.161.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
5.102.254.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.4	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.129.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.65.230.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.163.128	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.90	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.62.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.163.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
82.102.171.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.102.171.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
40.77.167.61	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.62.147	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
77.158.88.42	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
188.120.148.185	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.10	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
149.88.147.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.55.142	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.62.147	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
77.158.88.42	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.18.206.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.62.147	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.158.88.40	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
77.158.88.40	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.13.82	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
40.77.167.47	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.158.88.41	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.1.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
77.158.88.41	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
85.65.230.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
176.13.22.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
5.28.154.119	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
2.54.152.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
176.12.150.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.13.22.23	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.22.23	Block	55
176.13.4.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
176.13.11.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.54.152.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.25.102.57	Block	35
185.32.179.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.221.9	Block	19
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Illegal HTTP Version from 183.79.221.9	Block	19
176.12.150.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
176.13.22.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.22.234	Block	7
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
185.32.179.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.62.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	3
207.241.226.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	3
176.12.137.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.216	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
2.54.56.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.80.196.44	Block	2
79.177.188.41	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFirstName in www.refua.atal.idf.il/1518-he/refuah.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
176.13.6.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.116.160.49	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	2
185.32.179.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
95.86.70.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1256-he/refuah.aspx&sa=u&ved=0ahukewipj8677drjahvbhbqkxvknbyqqfggxmaw&usg=afqjcnednnsd4ekw3ac366wui0wxpegsow	Block	1
37.142.148.45	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.183.9.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.12.145.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.9.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.167.29	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
62.90.161.199	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.147.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.112.103	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19795-he/idfgdover.aspx	Block	1
183.79.223.58	Japan	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.79.223.58	Block	1
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
95.86.83.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.153.37	Israel	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