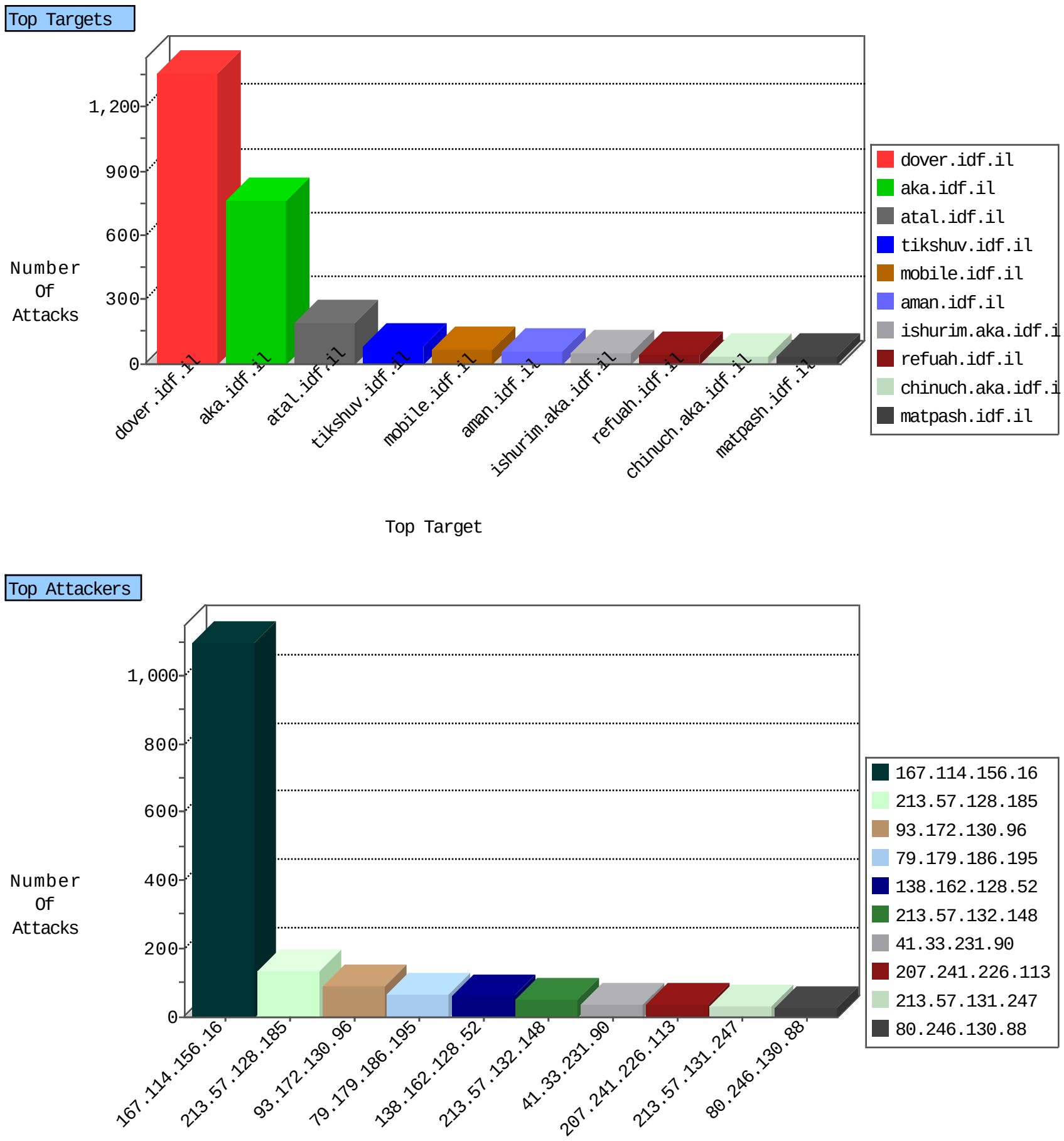
12-30-2015-19:04:08 to 12-30-2015-20:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers

12-30-2015-19:04:08 to 12-30-2015-20:04:08

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	3036
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
92.221.32.95	Norway	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

12-30-2015-19:04:08 to 12-30-2015-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-30-2015-19:04:08 to 12-30-2015-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.88	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
77.127.86.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.17.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.84.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.108.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.171.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.142.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.11.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.56.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.154.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.195.211.233	147.237.8.27	Malaysia	e.madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
193.105.134.220	147.237.8.24	Sweden	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.166.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.153.104.125	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.91.170.107	147.237.0.34	India	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.240.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.94.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.226.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.120.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.113.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.217.98.133	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.94.54.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.24.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.153.104.125	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1

12-30-2015-19:04:08 to 12-30-2015-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.128.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	67
213.57.128.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	66
138.162.128.52	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	59
213.57.132.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.178.203.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
213.57.132.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
46.19.86.115	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.85.53	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
207.241.226.113	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
207.241.226.113	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
138.162.128.54	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	17
138.162.128.53	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	16
5.22.131.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.58.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.159	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
46.19.85.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
5.102.254.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
75.147.232.121	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.28.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	11
213.57.28.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
80.246.130.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.162.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.65.48.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.131.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
37.26.146.220	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.177.98.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
80.246.130.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.54.148.174	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.146.178	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.109.214.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.99.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.10.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
46.19.85.11	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.214.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.99.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.207.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.135.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

12-30-2015-19:04:08 to 12-30-2015-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.186.195	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.179.186.195	Block	60
66.249.66.52	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	13
109.253.213.25	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	4
46.19.86.38	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	4
176.13.3.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.61	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	4
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 93.172.130.96	Block	3
109.253.213.25	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	3
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 93.172.130.96	Block	3
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 93.172.130.96	Block	3
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 93.172.130.96	Block	3
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 93.172.130.96	Block	3
178.62.48.159	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 178.62.48.159	Block	3
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 93.172.130.96	Block	3
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 93.172.130.96	Block	3
128.127.107.80	Netherlands	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.86.205	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 93.172.130.96	Block	3
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 93.172.130.96	Block	3
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 93.172.130.96	Block	3
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 93.172.130.96	Block	3
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 93.172.130.96	Block	2
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 93.172.130.96	Block	2
109.253.199.146	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
79.180.230.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.130.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 93.172.130.96	Block	2
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 93.172.130.96	Block	2
109.67.21.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.204.157	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.230.37	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	2
66.249.66.55	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 93.172.130.96	Block	2
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 93.172.130.96	Block	2
2.52.161.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 93.172.130.96	Block	2
93.172.130.96	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 93.172.130.96	Block	2
109.253.197.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.16.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/69037.pdf	Block	1
93.172.130.96	Israel	147.237.72.156	aman.idf.il	NULL Character in Method [[#17]]Ã 4Â·RÂª?Ã°[[#0]]6"'Â±Ã©ÂŸ Ã¼Âª[[#22]]_	Block	1
173.252.89.56	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.18.245	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
93.172.130.96	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 93.172.130.96	Block	1
213.57.28.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
5.175.0.137	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1

12-30-2015-19:04:08 to 12-30-2015-20:04:08